СБОРНИК НАУЧНЫХ ТРУДОВ

4-го Международного радиоэлектронного форума

«Прикладная радиоэлектроника.

Состояние и перспективы развития»

(МРФ'2011)

4th International Radio Electronic Forum

(IREF'2011)

PROCEEDINGS

Том II

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

«ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

(МКТСТ'2011)

Volume II

INTERNATIONAL CONFERENCE

«TELECOMMUNICATION SYSTEMS AND TECHNOLOGIES »

(ICTST'2011)

18-21 октября 2011г.

Харьков, Украина

October 18-21, 2011

Kharkov, Ukraine

Харьков
2011

УДК 621.37/.39

4-й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития» МРФ-2011. Сборник научных трудов. Том II. Международная конференция «Телекоммуникационные системы и технологии». – Харьков: АНПРЭ, ХНУРЭ. 2011. – 448 с.

В сборник включены научные доклады участников Международной конференции «Телекоммуникационные системы и технологии» (МКТСТ) 4-го Международного радиоэлектронного форума «Прикладная радиоэлектроника. Состояние и перспективы развития» МРФ-2011.

Издание подготовлено инновационно-маркетинговым отделом
Харьковского национального университета радиоэлектроники
и редакцией журнала «Проблемы телекоммуникаций»
http://pt.journal.kh.ua

61166, Украина, Харьков, просп. Ленина, 14.
Тел.: (057) 7021-397, 7021-515, 7021-735
Факс: (057) 7021-113
E-mail: innov@kture.kharkov.ua
akad@kture.kharkov.ua

© Академия наук прикладной радиоэлектроники, 2011
© Харьковский национальный университет радиоэлектроники, 2011

Программный комитет
конференции
«ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»
МКТСТ-2011

Аджемов А.С.	д.т.н.,проф., ректор Московского технического университета связи и информатики, Москва, Россия.
Бабкин В.П.	генеральный директор ЗАО Научно-производственного предприятия спецрадио (ЗАО НПП спецрадио), г. Белгород, Россия.
Бачевский С. В	д.т.н., проф., ректор Санкт-Петербургского государственного университета телекоммуникаций им. Проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия.
Борисов В. И.	д.т.н, генеральный директор Воронежского НИИ связи, г. Воронеж, Россия.
Бутенко В.В.	д.т.н., проф., генеральный директор Федерального государственного унитарного предприятие научно-исследовательского института радио, г. Москва, Россия.
Воробиенко П.П.	д.т.н., проф. ректор Одесской национальной академии связи им. А.С. Попова, г. Одесса, Украина.
Ильченко М.Е.	д.т.н., проф., директор учебно-науного института телекоммуникационных систем национального технического университета Украины «Киевский политехнический институт», г. Киев, Украина.
Имандосова М.Б.	д.т.н., проф., проректор по учебной и научной работе Казахской академии транспорта и коммуникации им. М.Тынышпаева г. Алматы, Казахстан.
Клымаш М.Н.	д.т.н., проф., зав. каф. телекоммуникации Национального университета «Львовская политехника», г. Львов, Украина.
Кривуца В.Г.	д.т.н., проф., ректор Государственного университета информационно-коммуникационных технологий, г. Киев, Украина.
Крикун В.С.	директор Харьковской филии ОАО «Укртелеком», г. Харьков, Украина.
Кузнецов А.П.	д.т.н., проф. проректор по научной работе Белорусского государственного университета информатики и радиоэлектроники, г.Минск, Белоруссия.
Певцов Г.В.	д.т.н., проф., зам. начальника университета по научной работе Харьковского университета воздушных сил, г. Харьков, Украина.
Петровский В.Н.	директор Закрытого акционерного общества «Украинская мобильная связь» (МТС-Украины), харьковского филиала, г. Харьков, Украина.
Пономарев Л.И.	д.т.н., проф. кафедры 406 Московского технического университета (МАИ), г. Москва, Россия.
Сапрыкин С.Д.	к.т.н., проф., генеральный конструктор НПК «НИИДАР», г. Москва, Россия.
Сарычев В.А.	д.т.н., проф., генеральный директор по научной работе и технической политике, зав. каф. радиоэлектронных систем Академии гражданской авиации НПО «Радар», г. Санкт-Петербург, Россия.
Скрыник А.П.	заместитель руководителя Государственной службы специальной связи и защиты информации, г. Киев, Украина

Слободянюк П.В.	к.т.н., доц., начальник Украинского государственного центра радиочастот, г. Киев, Украина
Стрелковская И.В.	д.т.н., проф., декан факультета «Информационные сети» Одесской национальной академии связи им. А.С. Попова, г. Одесса, Украина.
Татарчук С.И.	к.т.н., заместитель генерального директора ОАО «Укртелеком», г.Харьков, Украина.
Тепнадзе С.А.	д.т.н., проф., ректор Авиационного института Грузинского технического университета, г. Тбилиси, Грузия
Хорошко В.А.	д.т.н., проф. Государственного университета информационно-коммуникационных технологий, г. Киев, Украина. .
Шахтарин Б.И.	д.т.н., проф. Московского государственного технического университета имени Н.Э.Баумана, г. Москва, Россия
Юдин А.К.	д.т.н., проф., зав. каф., директор Института новейших технологий Национального авиационного университета, г. Киев, Украина

ОБЗОР МАТЕРИАЛОВ ФОРУМА

Конференция
«ИНТЕГРИРОВАННЫЕ ИНФОРМАЦИОННЫЕ РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (ИИРЭСТ–2011) ..... том 1

Конференция
«ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (ТСТ-2011) ..... том 2

Конференция
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ БИОМЕДИНЖЕНЕРИИ» (АПБ-2011) ..... том 3

ПЛЕНАРНОЕ ЗАСЕДАНИЕ КОНФЕРЕНЦИИ

ПИТАННЯ ДОСЛІДЖЕННЯ МЕРЕЖ МАЙБУТНЬОГО FN (Future Networks)

Кривуца В.Г., Беркман Л.Н.
Державний університет інформаційно-комунікаційних технологій
03110, м.Київ, вул. Солом'янська, 7

We consider a principled approach to the formulation and solution using the mathematical models under actual problem with the choice of research methods of quality networks FN, which define the main time and probability characteristics of provided services.

Донедавна щоразу, коли йшлося про створення глобальної інформаційної інфраструктури (ГІІ), ми неодмінно спиралися на концепцію NGN, яка передбачає досягнення головної мети - можливості надання будь-якої телекомунікаційної послуги кожному абонентові в будь-який час і в будь-якому місці за прийнятну плату.

З появою конкретних публікацій, що подавали опис NGN,а згодом і Рекомендації МСЕ Y.3001, де визначено, зокрема, характерні властивості FN, напрошується такий висновок: саме FN – це та мережа, яка дає змогу повною мірою реалізувати концепцію ГІІ.

У зазначеній Рекомендації доволі докладно висвітлюються принципи побудови мережі FN, її особливості з погляду технічних вирішень, якості й ефективності впровадження послуг для операторів і користувачів.

Нині ефективним є вибір методів, що дозволяють одночасно дістати доволі прості алгоритми для оцінювання основних параметрів мережі в нормальному і критичному режимах, а також алгоритмів, які уможливлюють оцінювання цих параметрів із високою точністю (похибка менша від припустимих значень для нормального функціонування).

Цілком природно, що у процесі основного дослідження FN необхідно реалізувати оптимальне проектування, тобто метод багатокритеріальної оптимізації (векторного синтезу). Це дасть змогу визначити найкращі параметри мережі за результуючим критерієм.

Як відомо, у процесі оптимізації параметрів системи S варіюють сукупність (вектор) $x = x_1, \dots, x_n$ цих параметрів, маючи на меті вибрати таке значення x цієї сукупності, при якому вектор якості системи $K = (k_1, k_2, \dots, k_m)$ має найкраще (у сенсі вибраного критерію переваги) значення.

У загальному випадку кожний із частинних показників якості може залежати від усіх *n* параметрів:

$$\begin{cases} k_1 = F_1(x_1, \dots, x_n), \\ k_m = F_m(x_1, \dots, x_n). \end{cases}$$

Ці залежності зазвичай називають цільовими функціями.

Згідно з накладеними обмеженнями O_S параметри $x_1, \dots, x_n$ мають задовольняти деякі обмеження типу рівностей, нерівностей і дискретності, причому в загальному випадку обмеження типу рівностей чи нерівностей накладаються не лише на значення кожного з параметрів зокрема, а й на зв’язки між ними.

Зауважимо, що задача оптимізації параметрів складається, як відомо, із двох основних етапів. На першому (попередньому) етапі, відштовхуючись від сукупності умов і обмежень вихідних даних, відшукують вигляд цільових функцій і функцій зв’язку. При цьому, вочевидь, бажано мати вихідні дані про структуру системи, котрі можна розглядати як частину умов чи обмежень.

На другому (основному) етапі здійснюють оптимізацію параметрів системи, тобто визначають таке значення сукупності параметрів системи, яке, задовольняючи задані обмеження, забезпечує найкраще значення вектора

$K' = < k_1, k_2, \dots, k_m >$ показників якості.

Для дослідження інфокомунікаційної мережі FN найдоцільніше при оптимізації параметрів звести задачу до дослідження поводження цільових функцій, тобто функцій скі-

нченної кількості змінних $x_1, \dots, x_n$, з урахуванням обмежень, що накладаються на ці змінні.

Розглянемо формулювання задачі оптимізації параметрів у *m*-вимірному просторі R^m показників якості.

При оптимізації параметрів можна окрім простору R^m показників якості $k_1, \dots, k_m$ розглядати також простір варійованих параметрів мережі R^n і простір R^q обмежень.

Проте у процесі оптимізації розгляд у просторах R^n і R^q має лише допоміжний (проміжний) характер, оскільки остаточне рішення про вибір системи можна ухвалити лише після розгляду всіх можливих значень вектора $K = \langle k_1, \dots, k_m \rangle$ у просторі R^m.

Варто зазначити, що ситуація у просторі R^m має багато спільного для всіх трьох випадків оптимізації: дискретного вибору, оптимізації параметрів і синтезу структури. Що ж до розгляду у просторах R^n і R^q, то він характерний лише для оптимізації параметрів.

У процесі оптимізації параметрів кожний варіант S побудови системи (або кожна система S) повністю визначається сукупністю $x = \langle x_1, \dots, x_n \rangle$ значень своїх параметрів, тобто

$$S = S(x_1, \dots, x_n).$$

У свою чергу, кожній системі S відповідає певне значення вектора $K = \langle k_1, \dots, k_m \rangle$ показників якості.

Вважатимемо, що залежність між S і K взаємно однозначна, позначивши її так:

$$K = K'(S).$$

Тоді у просторі показників якості кожній системі відповідатиме одна і тільки одна точка $A(S)$, в якій вектор визначає оптимальні параметри мережі.

Загалом при синтезі FN мереж доводиться враховувати, що відповідна система зазнає багатьох збурень, які являють собою випадкові процеси або випадкові величини. Для кожної реалізації ξ зазначених збурень можна ввести умовний показник якості k_ξ, котрий залежить не лише від параметрів $x_1, \dots, x_n$ системи, а й від випадкової величини (або випадкового процесу) ξ, тобто

$$k_\xi = F_\xi(x_1, \dots, x_n; \xi).$$

Наприклад, оцінюючи якість відтворення повідомлення x, можна вважати

$$k_\xi = \varepsilon^\xi = (y - x)^2,$$

де y - результат відтворення системою повідомлення x ; ε — похибка відтворення повідомлення.

А оскільки якість системи не можна характеризувати випадковою величиною, то за показник якості часто беруть математичне сподівання величини k_ξ, тобто вважають, що

$$k = Mk_\xi.$$

Якщо ξ — неперервна випадкова величина зі щільністю ймовірності $\omega(\xi)$, то

$$k = \int_{A\xi} \omega(\xi) F_\xi(x_1, \dots, x_n; \xi) d\xi.$$

У разі, коли закон розподілу $\omega(\xi)$ відомий, у результаті інтегрування дістаємо

$$k = F(x_1, \dots, x_n),$$

тобто показник якості являє собою відому функцію параметрів $x_1, \dots x_n$ системи, і задача оптимізації параметрів $x_1, \dots x_n$ зводиться до відомих, уже розв'язаних задач.

Утім у ряді випадків вид розподілу $\omega(\xi)$ апріорі (тобто до початку синтезу) не відомий, а якщо й відомий, то вираз виявляється надто складним, так що дістати в явному вигляді шукану залежність не вдається або процедура її відшукання надто складна. У таких випадках може бути доцільним застосування процедури так званої стохастичної апроксимації. Цю процедуру можна розглядати як поширення градієнтних методів на ситуації, в яких необхідно враховувати наявність випадкових збурень ξ. При цьому оптимальне значення вектора параметрів $x = < x_1, \dots, x_n >$ можна шукати, наприклад, за таким дискретним алгоритмом:

$$x[k] = x[k-1] - \Gamma[k]\nabla F_\xi(x[k-1], \xi[k]).$$

Тут $\nabla F_\xi = \{\partial F_\xi / \partial x_1, \dots, \partial F_\xi / \partial x_n\}$ - градієнт функції F_ξ.

Поданий алгоритм відрізняється від звичайної процедури градієнтного методу лише тим, що в цьому разі функція F_ξ, а отже, її градієнт ∇F_ξ має випадкові реалізації. Проте в теорії стохастичної апроксимації доводиться, що за належного вибору вагової матриці $\Gamma[k]$ (або вагового коефіцієнта $\gamma[k]$), а також у разі виконання деяких додаткових (які зазвичай справджуються) умов забезпечується збіжність(із імовірністю одиниця) величини $x[k]$ до значення, що відповідає екстремуму(у загальному випадку — локальному) показника якості. (При цьому вважається, що коли збурення ξ є випадковим процесом, то цей процес стаціонарний, а $\xi[k]$ — послідовні (у часі) вибіркові значення цього процесу).

Якщо заздалегідь обчислити градієнт ∇F_ξ не вдається (наприклад, через недиференційовність за x функції $F_\xi(x, \xi)$), то його можна знайти наближено з вимірювань на макеті системи(якщо такий існує) або на її електронній моделі. Як і тоді, коли йдеться про звичайні градієнтні методи, замість дискретного алгоритму можна застосовувати також аналоговий алгоритм, наприклад такого виду:

$$dx/dt = -a(t)\nabla F_\xi(x, \xi),$$

де вагова функція $a(t)$ відіграє ту саму роль, що й в алгоритмах, які визначають результуючу суб'єктивну цільову функцію.

Література:

1. Кривуца В. Г. Імітаційне моделювання та прогнозування: підручник для ВНЗ/Кривуца В. Г.—К., 1999.— 150 с.

2. Кривуца В. Г. Математичне моделювання телекомунікаційних систем: навч. посібник/Кривуца В. Г., Барковський В. В., Беркман Л. Н.— К.: Зв'язок, 2007.— 270 с.

3. Система управління сучасними телекомунікаційними мережами: монографія: у 2 ч./[Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.].—К.: ДУІКТ, 2009.— 268 с.

4. Кривуца В. Г. Сучасні цифрові системи комутації: підручник / Кривуца В.Г., Беркман Л.Н., Стеклов В.К. – К.: ДУІКТ, 201.- 389 с.9. Сайко В.Г. Методика оцінки впливу глибини замирання сигналу на перешкодостійкість OFDM-систем радіозв'язку / В.Г. Сайко, А.П.Полоневич / / Зб.тез V Міжнар. наук. техн. конф. «Сучасні інформаційно-комутаційні технології» COM-INFO'2010 р.,Livadia.- С. 41-42.

5. Корн Г. Справочник по математике: для научных работников и инженеров / Г.Корн, Т.Корн; пер. с англ. – М:Наука, 1973.

6. Дэйвид Г. Порядковые статистики / Дэйвид Г.; пер. с англ. – М.:Наука,1979.

МУЛЬТИАГЕНТНІ ТЕХНОЛОГІЇ, МОДЕЛІ Й МЕТОДИ УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПРОВАЙДЕРІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ПОСЛУГ

С.Ф. Теленик, О.І. Ролік, О.О. Покотило, Т.Ю.Разруцький
Національний технічний університет України «Київський політехнічний інститут»
проспект Перемоги, 37 корп.18, м. Київ, 03056, e-mail: telenik@auts.ntu-kpi.kiev.ua

The problem of information technologies infrastructure management is examined in the report. The complex of models of infrastructure management on the example of the problems of resource allocation and workload control and construction of information technology infrastructure measurement and evaluation metrics are proposed. General approach to the implementation of infrastructure management with the use of the multi-agent technology is proposed. The specificities of the agents' operations automation development – the monitoring data receiving, the calculating formulas setting, the parameters between the monitoring and control objects sending and subroutines loading are considered. The structure and the description of the information technologies infrastructure management system are given.

Вступ. Внутрішньо обумовлені розвитком потреб суспільства інтеграційні процеси призвели до появи інформаційно-комунікаційних технологій (ІКТ). Сьогодні розвиток галузі ІКТ визначає низка основоположних тенденцій, серед яких домінують: розвиток глобальних і національних ІТ-інфраструктур; перехід до обміну даними на основі протоколу IP; побудова програмних систем на основі Service-Oriented Architecture (SOA) і WEB-Oriented Architecture (WOA); консолідація ресурсів у центрах оброблення даних (ЦОД); віртуалізація платформ і ресурсів; розвиток хмарних обчислень (Cloud Computing); формування компонентно-базованого підходу до створення АСУ та АІС і розроблення композитних корпоративних застосувань на базі WEB 2.0 і WEB 3.0; захист WEB-застосувань на основі концепції Data Centric Security; перетворення систем управління базами даних у платформи для створення застосувань; об'єднання технологій Network Attached Storage (NAS) і Storage Area Network (SAN) на основі взаємодії із застосуваннями по IP-протоколу.

Злиття інформаційно-обчислювальних і телекомунікаційних мереж призвело до формування уявлень про інфраструктуру інформаційних технологій (ІТ-інфраструктуру), яка об'єднує мережі, обладнання користувачів, застосування різних рівнів і уможливлює використання самої інфраструктури та її компонентів, насамперед, серверів, систем збереження даних (СЗД), комунікаційного обладнання, а також засобів розроблення застосувань і самих застосувань у якості сервісів. Складовими глобальної та національної ІТ-інфраструктур виступають ІТ-інфраструктури органів державної влади, корпорацій, великих провайдерів інформаційно-комунікаційних послуг (ІКП). Віртуалізовані ресурси ЦОД дозволяють середнім і невеликим компаніям отримувати в якості сервісів ІТ-інфраструктуру та її компоненти, програмне забезпечення та платформи для його розроблення. Компанії можуть підібрати найвигіднішим чином (за ціною, надійністю та іншими критеріями) набір сервісів для підтримки усіх своїх бізнес-процесів. Суттєве зменшення капітальних і операційних витрат забезпечило доступність інформаційних, комунікаційних, обчислювальних та інших ресурсів високої якості більш широкому колу компаній, що стимулює розвиток виробництва і зростання конкуренції. З іншого боку, провайдери ІКП теж суттєво виграють, оскільки нові ресурси надаються за рахунок більш раціонального використання існуючих потужностей ЦОД без їх подальшого нагромадження. До того ж зменшення вартості послуг стрімко розширило коло клієнтів провайдерів ІКП. Але для того, щоб збільшити коефіцієнт використання потужностей ЦОД, ефективно розподіляти ресурси, забезпечувати обумовлений зі споживачами рівень якості сервісів, провайдерам необхідно розробляти і впроваджувати сучасні системи управління ІТ-інфраструктурою (СУІ) [1].

1 Сутність управління ІТ-інфраструктурою. У галузі ІКТ утворився і швидко розвивається новий науково-практичний напрямок – управління ІТ-інфраструктурою, у

якому аналітики виділяють таких 15 категорій програмних рішень [2]: управління мережами; управління серверами; управління БД; управління подіями; управління збереженням; управління кінцевими користувачами; управління застосуваннями; служба підтримки; управління рівнем обслуговування і сервісами для бізнесу; управління ресурсами; управління змінами і конфігураціями; управління потужностями; планування робіт; фінансове управління ІТ; автоматизація ІТ-процесів.

Складність ІТ-інфраструктури, становлення ринку ІКП як ринку користувачів призводить до необхідності комплексного врахування усіх чинників впливу у процесах прийняття рішень щодо розвитку ІТ-інфраструктури і управління власне самими ІТ-інфраструктурами.

Відповідно виникає потреба у комплексі моделей, здатних адекватно пов'язати параметри управління бізнесом і ІТ-інфраструктурами з параметрами ринку, структурними, технологічними параметрами ІТ-інфраструктур, ІКТ та іншими параметрами. Не менш важливою проблемою є вибір і, за необхідності, розроблення відповідних методів прийняття рішень і побудови управління на цих моделях. Насамкінець, постає проблема реалізації в реальних умовах їх функціонування, з урахуванням комплексного характеру взаємодії та взаємопроникнення згаданих вище тенденцій.

У доповіді розглянуто комплекс проблем, пов'язаних із створенням СУІ великого провайдера ІКП. Подано комплекс моделей і методів управління ІТ-інфраструктурою, покладений в основу функціонування СУІ. Масштабний характер зазначеного комплексу моделей і методів демонструється на моделях розподілу ресурсів, управління навантаженням та зведення метрик, які використовуються для вимірювання і оцінювання ІТ-інфраструктури та її компонентів. Описано підхід до реалізації СУІ з використанням мультиагентних технологій. Наведено структуру і принципи функціонування СУІ, результати виконаних експериментів.

Враховуючи новітні тенденції у сфері надання ІКП, насамперед поширення нових видів сервісів (Internet, програмні застосування, контент), появу нових технологій забезпечення сервісів, необхідність у тіснішій взаємодії мереж окремих провайдерів, міжнародний консорціум провайдерів комунікаційних сервісів Telecommunication Management Forum запропонував enhanced Telecommunication Operating Model (eTOM), у якій виклав нову парадигму управління бізнесом та операціями провайдерів ІКП. В Operation Support System (OSS) системи управління провайдера розглядається управління підтримкою операцій і готовністю, наданням послуг, забезпеченням якості та надійності, білінгом на рівнях споживачів, сервісів, ресурсів і мереж.

Якщо врахувати ще й Management Support System (MSS) з її управлінням розвитком, життєвими циклами ІТ-інфраструктури і продуктів на тих же рівнях споживачів, сервісів, ресурсів і мереж, то вимальовується дійсно масштабний комплекс моделей. Цю обставину підкреслює ще й той факт, що жоден з розробників СУІ не має єдиного комплексного рішення, яке б забезпечувало весь спектр функціональних потреб провайдерів ІКП.

2 Загальна характеристика комплексу моделей і методів СУІ. Складність загальної проблеми управління ІТ-інфраструктурою робить виправданою її декомпозицію. Враховуючи взаємодію ЦОД, їх зонування, для реалізації підходу необхідно вирішити щонайменше такі задачі:

1) планування ЦОД і зон, розподіл навантаження між ними;
2) управління ресурсами і навантаженням зон;
3) балансування навантаження зон;
4) диспетчерування навантаження зон.

Продемонструємо масштабність проблеми розроблення моделей на задачах управління ресурсами і навантаженням зон. Оскільки зазначенні моделі повинні враховувати багато чинників, в доповіді запропонована наведена на рис. 1 класифікація потрібних для вирішення цих задач моделей і алгоритмів з урахуванням зазначених чинників як ознак класифікації.

Основна мета, задачі	Надання IT-послуг, забезпечення якості сервісів		Управління власною IT-інфраструктурою, підтримка бізнес-процесів	
Технології	Виділені сервери	Віртуальний хостинг	Серверна віртуалізація	Кластерні системи
Етапи життєвого циклу	Узгодження задач бізнесу та IT	Планування IT-сервісів	Впровадження IT-сервісів	Управління IT-сервісами
Рівень абстракції ресурсів	Абстрактні		Конкретні	
Забезпечення ресурсами	Цілком або ніяк		Допускається часткове забезпечення ресурсами	

Рис.1 Параметри визначення класів моделей управління ресурсами і навантаженням

Перша ознака передбачає відмінність моделей в залежності від цілей ведення бізнесу – управління IT-інфраструктурою для підтримки власних бізнес-процесів чи надання IT-послуг зовнішнім споживачам. Такий поділ впливає на вигляд критерію у відповідних моделях. Другою ознакою є технології, покладені в основу IT-інфраструктури. Ці чинники впливають на всі елементи моделей: критерій, обмеження, тип змінної. В залежності від етапу життєвого циклу IT-сервісу (третя ознака) виникають ті чи інші задачі. При цьому на етапі планування крім технологічних і ресурсних обмежень можуть використовуватись також і інші види обмежень, наприклад вартісні обмеження чи обмеження на показники надійності. Рівень абстракції ресурсів (четверта ознака) визначає багаторівневість математичних моделей: на першому етапі здійснювати розподіл абстрактних (узагальнених) ресурсів кожного типу без прив'язки до їх конкретного місцезнаходження, з уточненням отриманих результатів на другому етапі. Також суттєво впливає на вид моделей остання ознака – забезпечення ресурсами, тобто, чи дозволяється часткова підтримка сервісів, чи вони мають бути підтримані у повному обсязі або не підтримані зовсім.

Потрібні моделі визначаються комбінаціями зазначених параметрів. Можна сформулювати 2*4*4*2*2=128 класів моделей, для кожного з яких визначається критерій, ресурсні, технологічні та інші обмеження. У доповіді наведено модель для управління ресурсами і навантаженням зони Internet традиційного ЦОД. Сформульована задача розподілу ресурсів серверного пулу між віртуальними машинами користувачів, при якому досягається критерій (1) за умов (2) – (7):

$$\min \sum_{j=1}^{m} S_j Y_j \,, \tag{1}$$

$$\sum_{i=1}^{n} \varpi_j x_{ij} \le \Omega_j, j = 1,\ldots,m, \tag{2}$$

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \varphi_j x_{ij} \le \Phi, \tag{3}$$

$$\sum_{i=1}^{n} \beta_j x_{ij} \le B_j \,, \tag{4}$$

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_j x_{ij} \le \Lambda, \tag{5}$$

$$\sum_{j=1}^{m} \mathrm{X}_{ij} \le 1, i = 1,\ldots,n, \tag{6}$$

$$y_j = x_{1j} \vee \ldots \vee x_{nj} \,, \tag{7}$$

Тут прийняті такі позначення:

S_j – вартість обслуговування сервера j;

$$x_{ij} = \begin{cases} 1, & \text{якщо віртуальна машина } i \text{ базується на фізичному сервері } j; \\ 0, & \text{в іншому випадку.} \end{cases}$$

ϖ_i, β_i, φ_i, λ_i – відповідно процесорна місткість, оперативна пам'ять, пропускна здатність обміну даними і місткість логічного пристрою СЗД віртуальної машини *i* (визначаються на основі вимог користувача до відповідних параметрів серверів);

Ω_j, B_j - процесорна місткість і оперативна пам'ять фізичного сервера *j*;

Ф, Λ - сумарні ємність СЗД і пропускна здатність Λ обміну даними серверного пулу.

Наведена модель належить до класу задач булевого програмування, для вирішення яких можна використовувати евристичний та керований генетичний алгоритми із праці [3]. Інші моделі належать до різних класів задач математичного програмування. Ці моделі і відповідні методи наведені в низці праць авторів, насамперед [3 – 7].

Ще однією з проблем, які розглядаються в доповіді, є проблема агрегування метрик одного рівня аналізу ІТ-інфраструктури у метрики вищого рівня, коли застосовуються нечіткі метрики. Формальна постановка проблеми подана у термінах теорії нечітких множин і нечіткої логіки. Нехай маємо дворівневу систему показників функціонування мереж (сервісів, технологій), причому на нижньому рівні n показників K_1, K_2,…,K_n, які повинні бути зведені у один показник Q верхнього рівня. Показник Q є лінгвістичною змінною значення якої належать множині S. Показники K_1, K_2,…,K_n також є лінгвістичними змінними, які набувають значень із множин значень A_1, A_2,…,A_n. У нечіткій логіці з n входами і одним виходом міркування здійснюються за правилами (нечіткими правилами), які мають вигляд

$$R_j \text{ Якщо } K_1 \in A_{1,j} \wedge K_2 \in A_{2,j} \wedge \ldots \wedge K_n \in A_{n,j}, \text{ то } Q \in S_j, \qquad (8)$$

де $A_{i,j}$ і S_j – нечіткі множини вхідної і вихідної лінгвістичних змінних, R_j – нечітке правило.

Необхідно розробити метод агрегування показників оцінювання якості сервісів, заданих у вигляді нечітких множин.

Запропонований у доповіді метод побудови функції належності та нечітких правил базується на основі використання навчальних вибірок даних. Розроблений відповідний алгоритм навчання, який дозволяє будувати функції належності вхідних нечітких змінних і формувати нечіткі правила зведення показників оцінювання якості сервісів [8,9].

3 Реалізація СУІ. Не менш складні проблеми пов'язані з реалізацією СУІ. Сьогодні СУІ поєднують переваги і недоліки централізованого і децентралізованого підходів на основі широкого застосування мультиагентних технологій. Мобільні і стаціонарні агенти, мета-агенти територіально розподіленої СУІ взаємодіють в процесі реалізації функцій моніторингу, аналізу і управління елементами ІТ-інфраструктури, її компонентами та ІТ-інфраструктурою в цілому, планують і виконують спільну роботу для вирішення поставлених задач, використовуючи надані їм ресурси. При цьому вони організовують канали взаємного зв'язку, синтезують функції оброблення даних на своєму рівні, в рамках спільної задачі. Агенти мають бути достатньо гнучкими, щоб закріпитися в виділеному їм середовищі. Необхідно розробити моделі і відповідні методи для організації взаємодії агентів в СУІ, які б забезпечували зв'язок між окремими агентами і координацію їх зусиль для управління ІТ-інфраструктурою та її компонентами, синхронізацію, накопичення інформації, уніфікацію алгоритмів оброблення даних моніторингу.

СУІ будується за ієрархічним принципом, з центральним сервером на верхньому рівні, периферійними серверами на нижніх рівнях, та підключеними до них агентами. З нижніх рівнів на верхні надходять узагальнені дані моніторингу та інформація про функ-

ціонування ІТ-інфраструктури, у зворотному напрямі розповсюджуються політики управління, задачі та цілі СУІ.

Програмне забезпечення СУІ складається з серверного, агентських та клієнтських програмних модулів. Серверний модуль (сервер) забезпечує взаємодію між модулями системи, надає доступ до даних та забезпечує їх цілісність та захист, здійснює планування моніторингу, аналіз та управління елементами ІТ-інфраструктури, розподіл ресурсів між агентами та застосуваннями і задач між агентами. Збір даних моніторингу та управління елементами сервер здійснює через відповідні агентські модулі. Сервер синхронізує і оброблює дані, інформує підключених агентів і клієнтів про зміни. Клієнтський модуль (клієнт) реалізує інтерфейс адміністратора для налаштування СУІ, відстеження працездатності і продуктивності елементів ІТ-інфраструктури, контролю стану її складових і ІТ-інфраструктури в цілому, а також для введення команд управління при реконфігурації чи проведенні відновлювальних заходів.Агентський модуль (агент) контролює елементи ІТ-інфраструктури, аналізує їх стан і поведінку. Виконаний у вигляді окремого сервісу, він реалізує індивідуальний набір функцій моніторингу і управління, визначений в залежності від завдань, вирішуваних агентом, і обслуговуваних ним об'єктів. Зібрані агентом дані оброблюються ним і іншими агентами, і разом з результатами оброблення зберігаються в локальній базі даних (БД) або відправляються на сервер.

Для вирішення проблеми організації роботи агентів СУІ необхідно насамперед створити узагальнену модель представлення всіх елементів та складових ІТ-інфраструктури, описати всі матеріальні (маршрутизатори, сервери, а також їх складові – процесори, накопичувачі) та віртуальні (процеси, служби, потоки) об’єкти моніторингу та управління. Вводяться необхідні поняття:

- об’єкт моніторингу та управління (ОМУ) – логічний об’єкт, який представляє елемент ІТ-інфраструктури, його складову частину або процес, що ним виконується;
- шаблон ОМУ – абстрактний об’єкт, який об’єднує ОМУ, що відображають однотипні елементи ІТ-інфраструктури, за спільними ознаками, декларує структуру цих елементів, взаємозв’язки між ними, доступний їм функціонал та логіку визначення стану;
- параметр, шаблон параметра ОМУ – об’єкт, який характеризує ОМУ. Оскільки усі ОМУ, що належать до одного шаблону, мають однаковий набір параметрів, то загальна інформація стосовно параметра зберігається в його шаблоні, а значення самих параметрів пов’язуються з конкретними ОМУ і можуть змінюватися в часі;
- зв’язки між ОМУ, їх параметрами та шаблонами відображають функціональні зв’язки та залежності між відповідними елементами ІТ-інфраструктури. Вага зв’язку відображає ступінь взаємного впливу зв’язаних елементів.

Всі ці сутності утворюють реляційну модель даних, що дозволяє ефективно зберігати пов’язану з ними інформацію про ІТ-інфраструктуру, а використання механізму шаблонів значно спрощує програмування логіки оброблення даних агентами за рахунок повторного використання алгоритмів для різних ОМУ, які використовують цей шаблон.

ІТ-інфраструктура зображується у вигляді зв’язаного графа ОМУ – ярусно-паралельної форми. Граф шаблонів ОМУ описує її узагальнену структуру. На першому ярусі знаходяться ОМУ, значення параметрів яких можуть бути отримані за допомогою лічильників, а значення параметрів ОМУ верхніх рівнів є функціями від параметрів ОМУ, що знаходяться рівнем нижче.

Для розподілу задач між агентами СУІ необхідно розбити задачі на підзадачі, які, в свою чергу, ототожнити з ОМУ, що відображають реальні елементи ІТ-інфраструктури, або з віртуальними ОМУ, що відображатимуть дану підзадачу. Оскільки агент СУІ може отримувати значення лише тих параметрів ОМУ, до яких має доступ, необхідно визначити ОМУ, що прив’язані до конкретних агентів (відповідно, підзадач, що можуть виконуються на конкретних обчислювальних машинах), після чого можна розподілити ОМУ (підзадачі) між агентами. ОМУ, що не прив’язані до конкретних агентів можна перерозподіляти і під час роботи системи.

Оскільки при цьому пов'язані логікою оброблення інформації ОМУ можуть бути закріпленими за різними агентами, реалізація описаного підходу можлива за умови надання агентам здатності до взаємодії і планування роботи. У доповіді пропонуються моделі визначення поведінки агентів і планування взаємодії при вирішенні задач моніторингу, аналізу і управління.

Для вирішення кожної підзадачі уточнюються значимі параметри ОМУ, алгоритми визначення значень параметрів та станів ОМУ. Для спрощення налаштування агентів та програмування алгоритмів визначення значень параметрів та станів ОМУ всіх рівнів, забезпечення оперативної передачі змін стану ОМУ по ієрархії та необхідної швидкості реакції на події в IT-інфраструктурі, виникає потреба у використанні таких засобів автоматизації операцій з розроблення агентів: отримання даних моніторингу; задання розрахунків формулами; пересилка значень параметрів між ОМУ; підключення підпрограм. У доповіді розглянуто особливості реалізації кожного з зазначених засобів автоматизації.

Отримання даних моніторингу. Отримання актуальних значень параметрів ОМУ нижніх рівнів ініціює планувальник, який запускає виконання моніторингових функцій згідно заданих налаштувань. Для реалізації моніторингових функцій використовуються як стандартні методи Windows Management Instrumentation, так і розширювані методи, орієнтовані на вирішення конкретних задач за допомогою створеної для СУІ технології DALLF (Dynamic Auto Link Library Function), що дозволяє реалізовувати та динамічно завантажувати необхідні функції.

Задання розрахунків формулами. Для обчислення метрик, визначення станів та значень параметрів ОМУ використовуються стандартизовані або розширювані алгоритми. До перших належать порогові, нечіткі, та статистичні алгоритми, основними перевагами використання яких є проста в налаштуванні та чіткий алгоритм їх роботи. Логіка правил, як розширюваний алгоритм, дозволяє задавати власні алгоритми оброблення даних та оцінювання стану з використанням стандартних функцій і завантажених DALL-функцій. Ці алгоритми можна задавати у шаблону ОМУ, після чого наслідувати, перевизначити, задавати власні для конкретних ОМУ або їх параметрів. Порогові алгоритми простіші у налаштуванні і менш вимогливі до ресурсів. При налаштуванні алгоритму визначаються числові діапазони, яким у відповідність ставиться певний логічний стан. Визначення стану зводиться до визначення відповідного діапазону. Використання нечітких методів продемонстровано вище на задачах зведення метрик.

Статистичні алгоритми дозволяють визначити стан чи значення параметра, використовуючи стани або значення параметрів, від яких він залежить. Визначення стану можливе лише за умови, що всі параметри-залежності мають однаковий набір порівнюваних станів. Значення параметра можна обчислити як зважену суму, або як зважене середнє (арифметичне, геометричне, гармонічне). Стан визначається за допомогою порогових алгоритмів, причому спектр станів можна копіювати із параметрів-залежностей, або перевизначити.

Логіка правил дозволяє реалізувати будь-який користувацький алгоритм обчислення, використовуючи математичні та логічні операції та функції. Для реалізації логіки правил створена проста скриптова мова програмування, яка підтримує унарні та бінарні операції, операції різних пріоритетів, а також функції. Логіка може використовуватись для обчислення як значень параметрів ОМУ, так і метрик та станів (в тому числі нечітких), причому в якості вихідних даних можна використовувати як значення параметрів, так і стани будь-яких зв'язаних ОМУ.

Реалізація користувацького алгоритму може бути «зібрана» двома способами: за допомогою динамічної композиції об'єктів-операцій і створення синтаксичного дерева, або ж за допомогою програмної генерації коду і створення нової бібліотеки. Множину операцій та функцій, які підтримує логіка, можна розширювати, розташовуючи їх реалізації в DALLF-бібліотеці.

Використання шаблонів дозволяє агрегувати значення декількох параметрів ОМУ певного шаблону. Це дозволяє використовувати узагальнений алгоритм для усіх реаліза-

цій даного фрагменту графа шаблонів, за рахунок чого зникає необхідність робити окрему реалізацію даної функції в місцях, де можлива наявність декількох ОМУ одного шаблону, а також переробляти алгоритм при зміні кількості ОМУ чи параметрів даного шаблону.

Пересилка значень параметрів між ОМУ. Для своєчасного оновлення станів ОМУ всіх рівнів ієрархії, необхідно вчасно оповіщати їх про оновлення стану або значень параметрів ОМУ, від яких вони залежать. У доповіді розглянуто різні способи передачі повідомлень про зміну стану об'єкту та запуску оновлення стану залежного від нього об'єкту. Найпростішим способом є передача оновлених значень до БД, з наступним їх зчитуванням залежними ОМУ за сигналами планувальника. Недоліком цього способу є низька швидкість реакції на зміни, а при підвищенні частоти оновлення з метою підвищення швидкості реакції значно зростає потреба у ресурсах. При використанні реактивного оновлення ОМУ відбувається оповіщення одразу всіх залежних від нього ОМУ верхнього ярусу, які, в свою чергу, одразу оновлюють свій стан. Цим забезпечується швидке поширення інформації про зміни та швидка реакція на них, проте можливе перенавантаження агента або надто часте оновлення стану ОМУ, який залежить від інших часто оновлюваних ОМУ. Для нейтралізації останнього недоліку використовується черга задач, що обмежує кількість одночасно виконуваних задач. Задачі оновлення стану ОМУ і подібні їм позначаються як такі, що ставляться в чергу лише один раз. Тоді при повторному виклику задачі, яка вже є в черзі, буде підвищено її пріоритет. Крім того, для усунення розсилання повідомлень при незначній зміні стану ОМУ чи значень його параметрів встановлюється коридор, в межах якого коливання змінних не вважаються за їх зміну.

Підключення підпрограм. Для отримання значень лічильників та виконання певних операцій у логіці правил можна використовувати користувацькі функції за допомогою згаданої вище технології DALLF. Користувачі можуть розробляти і використовувати власні бібліотеки, динамічно їх завантажувати, використовуючи рефлексію типів. При реалізації функцій набори вхідних і вихідних параметрів вказуються у метаданих.

Висновки. Для перевірки запропонованого підходу був проведений комплексний експеримент, який підтвердив його працездатність, дозволив порівняти ефективність запропонованих методів, вплив підходу на ефективність функціонування системи управління ІТ-інфраструктурою. У доповіді наводяться результати експериментальних досліджень.

Література:

1. SLA Management Handbook. Vol.1. Executive Overview, Member Reviewed Version 2, TeleManagement Forum, Morristown, NJ, January 2005. Vol.2. Concepts and Principles, Release 2.5, TeleManagement Forum, Morristown, NJ, July 2005.

2. Дубова Н. ИТ-«управленцы» на марше // Открытые системы. –2009. –№ 5.–С.12 – 16.

Теленик С.Ф Генетичні алгоритми вирішення задач управління ресурсами і навантаженням ЦОД / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, С.А.Андросов // Автоматика. Автоматизація. Електротехнічні комплекси та системи. – 2010. – №1 (25). – С.106 – 120.

3. Теленик С.Ф. Управління навантаженням і ресурсами ЦОД при виділених серверах / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, Р.В. Римар, К.О. Ролік // Автоматика. Автоматизація. Електротехнічні комплекси та системи. – 2009. – №2 (24). – С. 122 – 136.

4. Теленик С.Ф. Управління ресурсами ЦОД / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, К.О. Крижова // Вісник ЛНУ імені Івана Франка. – 2009. – №11. – С. 103 – 119.

5. Теленик С.Ф. Управління навантаженням і ресурсами ЦОД при віртуальному хостингу / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, Р.В. Римар, С.А. Андросов // Вісник Тернопільського Державного технічного університету. Том 14. – №4. – 2009. – С. 198 – 210.

6. Теленик С.Ф. Моделі управління віртуальними машинами при серверній віртуалізації / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, А.Ю. Лабунський // Вісник НТУУ

«КПІ»: 7. Інформатика, управління та обчислювальна техніка. – К.: «Век+».– 2009. – Вип. 51. – 2009. – С. 147 – 152.

8. Теленик С.Ф Нечітке оцінювання в задачах управління рівнем обслуговування / С.Ф. Теленик, О.І. Ролік, М. В. Ясочка, О.М. Моргаль // Наукові записки Українського науково-дослідного інституту зв'язку. – №2. –2011. – С.29 – 42.

9. Теленик С.Ф Зведення метрик рівня обслуговування користувачів на основі експертних висновків методів / С.Ф. Теленик, О.І. Ролік, О.М. Моргаль, О.С.Квітко // Вісник Вінницького політехнічного інституту. – 2011. – №1. – С.112 – 123.

К РАЗВИТИЮ ТЕОРИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Поповский В.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр.Ленина, каф. телекоммуникационных систем, тел. (057)702-13-20
E-mail: tkc@kture.kharkov.ua; факс (057)702-13-20

It is asserted that mathematical models of complex systems, including telecommunication ones, should be built using multidimensional representations. It is interrelation among the components (elements) of the system that assure its super-integral integrity and emergency properties.

Two types of stochastic systems representations are analyzed: through probabilistic characteristics (of density or of probability distribution function) and through state equations. It is concluded that variable states method is more general and enables to represent all the set of random objects: values, processes and fields.

Общие вопросы

Нынешний этап развития и совершенствования информационных и телекоммуникационных систем осуществляется за счет технологических решений и потребительского спроса на услуги. Телекоммуникации - это едва ли не единственная отрасль, к развитию которой наука имеет лишь опосредствованное отношение и привлекается большей частью при разработке отдельных элементов сетей или фрагментов. Уместная в данном случае наука — теория систем пока что декларируется в концепции ПСП — правилах системной политики и до сих пор не обрела базисного характера.

Причин неактивного использования результатов теории в развитии отрасли несколько. Во-первых, сама теория систем, начиная со второй половины прошлого столетия, притормозила в развитии из-за отсутствия явных запросов со стороны прикладных задач.

Во-вторых, при стремительном расширении телекоммуникационных систем весьма удовлетворительные результаты дают все более новые технологии и острой необходимости в привлечении современной системной науки пока что не было. Наконец, многочисленные разработчики и производители нового сетевого оборудования, а соответственно и технологий, не заинтересованы в системности и унификации разработок. Их основной интерес в том, чтобы «застолбить» ту или иную нишу рынка телекоммуникаций.

Несмотря на все эти объективные и субъективные причины, возникает потребность и необходимость использования системных теорий, в частности кибернетики, в свое время давшей теории систем «второе дыхание». Вместе с тем, в уже существующих технологиях все больше используются различные кибернетические решение, где телекоммуникационная система, или ее часть, рассматривается как динамичная, управляемая система, где реализуются формализованные дифференциальные модели, функционирующие в соответствии с принятыми критериями (в том числе стохастическими), методы преодоления априорной неопределенности, процедуры принятия решений, оценок, экстраполяции, интерполяции и управления.

Мощный аппарат кибернетических решений удачно используется в одномерном варианте. Достаточно детально исследованы различные одномерные методы и процедуры. Вместе с тем, при переходе к многомерным представлениям и моделям возникают определенные сложности, которые часто аккуратно обходятся авторами. Здесь проблема не только в необходимости обоснования марковских свойств многомерной модели, но и в самих алгоритмических решениях, в интерпретации выигрышей или потерь, вызванных наличием и учетом взаимных связей между компонентами многомерной системы. В то же время именно эти взаимные связи систему делают системной, ибо при независимых компонентах она распадается на отдельные элементы, а благодаря этим взаимным связям система приобретает сверхинтегральные свойства, не являющиеся простой суммой свойств отдельных составляющих ее элементов, и обретает характеристики эмерджентности.

Таким образом, с одной стороны, возникает необходимость использования результатов теории систем и кибернетики в существующих инфокоммуникационных технологиях (а в дальнейшем и в том, чтобы в создаваемых на основе строгих математических предпосылок и критериев телекоммуникационных системах, использовать передовые технологии), с другой стороны — при проецировании теории систем на инфокоммуникационные системы возникает необходимость в конкретизации теории применительно к свойствам инфокоммуникаций.

В связи с потребностью теоретического обоснования многих алгоритмов обработки сигналов, управления и адаптации, которые уже внедрены в существующие технологии или ожидается их внедрение. Возникла необходимость включения в учебный план специальност дисциплин «Теория систем» и «Методы управления и адаптации в ТКС». Кроме того, сама инфокоммуникационная система, которая все больше становится похожей на систему управляемых автоматов, уже сейчас требует конструктивной теории, поясняющей работу субсистем управления, являющуюся аналогом нервной системы человека.

Отраслевая наука — теория телекоммуникационных систем, очевидно, должна излагаться на основе статистического, вероятностного подхода. На наш взгляд, это принципиально важно, поскольку в отличие от детерминистского подхода, где задача приводит к конкретному решению, решение вероятностных задач обычно охватывает целый класс ситуаций. Это, помимо общности, приводит к более устойчивым решениям в условиях случайных и нестационарных процессов, трафика, сигналов и помех.

Необходимость разработки теории телекоммуникационных систем состоит также и в том что до сих пор отсутствуют методики построения адекватных многомерных математических динамических моделей и разработки набора математических приемов и методов анализа и синтеза, в необходимости создания методологии системных исследований, позволяющих проектировать и эксплуатировать данные системы с принципами самоорганизации и самовосстановления, устойчивые на микро и макроуровнях к зависаниям и катастрофическим исходам. Уже сегодня потребности практики актуализируют разработку теории телекоммуникационных систем.

Математические модели телекоммуникационных систем

В любой теории одним из главных положений является выбор математических моделей, определяющих данную предметную область. Вариант комплекта математических моделей, необходимый для построения указанной теории, можно представить в виде таблицы №1. В верхней части таблицы сосредоточены общие характеристики систем. Сосредоточимся на нижней более конкретной части.

В общем случае любой физический объект можно рассматривать как случайный. При этом случайная часть может быть сосредоточена как в самом объекте, так и в тех инструментах, с помощью которых отображают данный объект и формируют наблюдения об этом объекте.

Поскольку любая модель лишь приближенно соответствует моделируемому объекту, то часто допустимыми считаются отклонения параметров модели до 20%. Поэтому, если объект характеризуется незначительным уровнем случайной компоненты, то модель такого объекта часто считают детерминированной, что облегчает решение задачи.

В тех случаях, когда не удается задачу свести к чисто детерминированной приходится ее решать как стохастическую. Имеется два основных приема решений, каждый из которых основывается на своих математических моделях.

1. Метод моделирования и решений стохастических задач с использованием результатов теории вероятностей. В данном методе рассматривается не сам случайный объект ξ, а его вероятностные характеристики: функция распределения вероятностей $F(x) = P\{\xi \le x\}$, где x - неслучайная переменная величина, определяющая вероятность непревышения ее случайной величиной ξ.

Таблица 1. Типы математических моделей систем

<table>
<tr><td colspan="2">Простые
одна модель</td><td colspan="2">Сложные
множество моделей</td></tr>
<tr><td colspan="4">Свойства систем</td></tr>
<tr><td>Структурные
(состав, связность, сложность, иерархичность)

- теория графов
- теория симплексов</td><td colspan="2">Общесистемные
(целостность, устойчивость, инвариантность, открытость, надежность)
- теория тензоров
- теория устойчивости
- теория автоматов
- теория систем</td><td>Функциональные
(инерционность, производительность, точность, результативность)
- дифференциальные уравнения
- разностные уравнения</td></tr>
<tr><td colspan="2">Локальные</td><td colspan="2">Распределенные
- по времени
- по пространству</td></tr>
<tr><td colspan="2">Линейные
$y = A(t)x(t)$</td><td colspan="2">Нелинейные
$y = A(x,t)$</td></tr>
<tr><td colspan="4">Область представлений параметров
- частотная
- временная
- пространственная
- общая</td></tr>
<tr><td colspan="4">Стохастические = детерминистские + случайные</td></tr>
<tr><td>Случайные события

$P(A)$</td><td>Случайные величины
$p(x)$</td><td>Случайные процессы

$p(x_n, t_n)$</td><td>Случайные поля

$p(\vec{x}_n, \vec{t}_n)$</td></tr>
<tr><td colspan="2">Статические</td><td colspan="2">Динамические</td></tr>
</table>

Другая часто используемая вероятностная характеристика – распределение вероятностей этой переменной

$$p(x) = \frac{dF(x)}{dx}, \text{ где } F(x) = \int_{-\infty}^{x} p(x)dx. \qquad (1)$$

Данный метод моделирования нашел широкое применение в практике, в том числе в радиотехнике и связи, где задачи сводятся к получению параметров различных объектов, обеспечивающих желаемое значение вероятности. Важным достоинством данного метода является то, что все преобразования переменной x и ее вероятностей $p(x)$ могут осуществляться с помощью обычных интегро-дифференциальных операторов.

Метод отлично зарекомендовал себя в тех задачах, где случайные объекты обладают свойствами случайных величин. Поэтому при использовании обсуждаемого метода моделирования важно априори определить к какому типу относится анализируемый случайный объект: событию, величине, процессу или случайному полю. Если же возникает необходимость отображения динамических свойств случайных объектов, то модель случайных величин уже не работает. Необходимый при этом переход к вероятностям случайных процессов и полей при представлениях $F(\vec{x})$ и $p(\vec{x})$ оказывается громоздким n-мерным, где n-число сечений, в которых представлены эти процессы или поля.

Случайный процесс $x(t)$ - это математический объект, представляющий собой множество случайных функций времени и (или) пространства, в каждом сечении которых определена плотность распределения вероятностей:

$$p(x_1, x_2, \ldots, x_n; t_1, t_2, \ldots, t_n) = \frac{\partial^n F(x_n, t_n)}{\partial^n x_n}, \qquad (2)$$

где $F(x_n, t_n)$ - функция распределения процесса $x(t)$ в n - сечениях.

С представлениями (2), в силу громоздкости, работать достаточно сложно, поэтому существует ряд частных представлений, среди которых: предположение о диффузности процесса $x(t)$, о стационарности и эргодичности. Существует также ряд аппроксимаций известными функциями.

Использование предположения об эргодичности процессов имеет ограниченное практическое применение в силу невозможности решений динамических и нестационарных задач, являющихся основными в телекоммуникациях. Вместе с тем, следует отметить, что несмотря на свою ограниченность данный метод продолжает широко использоваться в теории связи и других прикладных науках.

2. Метод моделирования и решения стохастических задач, использующий представления о самих случайных объектах: случайных величинах, случайных процессах или случайных полях. Среди наиболее конструктивных таких моделей являются модели диффузионного типа, в частности модели марковских процессов. Такой процесс, включающий случайную и детерминированную компоненты, представим в виде:

$$x(t) = x(0) + \int_T \theta(t)dt + \int_T \Phi(t)dW(t), \qquad (3)$$

где $x(0)$ - регулярная постоянная составляющая,

$\int_T \theta(t)dt$ - регулярно изменяемая компонента, описываемая обычным интегралом Лебега,

$\int_T \Phi(t)dW(t)$ - случайно изменяемая компонента, порожденная винеровским процессом $W(t)$, описываемая интегралами Ито или Стратоновича.

Кроме такого интегрального, часто используется и представление дифференциальным управлением состояния:

$$dx(t)/dt = F(t)x(t) + G(t)\xi(t), \qquad (4)$$

где $F(t) = \alpha$ - коэффициент состояния процесса $x(t)$ численно равный обратной величине интервала корреляции этого процесса $\alpha = \tau_{кор}^{-1}(x)$;

$G(t)$- коэффициент генерации, $G(t) = \sigma_x^2 / 2\alpha$, определяющий уровень случайно изменяющейся компоненты;

$\xi(t)$ - гауссов белый шум (порождающий процесс).

Для случайного поля состояние $x(t)$ становится вектором, а коэффициенты $F(t)$ и $G(t)$ - матрицами, недиагональные элементы которых определяют уровни взаимных связей между компонентами системы $x_i(t)$.

В рассматриваемом втором методе, называемом методом переменных состояния, не исключается, наоборот - широко используются также результаты теории вероятностей и математической статистики. Так, два состояния марковского процесса $x(t_1)$ и $x(t_2)$ связаны между собой переходной вероятностью:

$$x(t_2) = p(t_2 / t_1) \cdot x(t_1),$$

где $p(t_2 / t_1) = \exp\{-\Delta t / \tau_{кор}\}$ - вероятность перехода из состояния в момент времени t_1, в состояние момента t_2, $\Delta t = t_2 - t_1$.

В соответствии с теоремой Дуба случайный процесс, представимый уравнением состояния (4), относится к классу марковских. Часто уравнение (4) называют уравнением формирующего фильтра.

Важным достоинством марковских моделей (3) и (4) является возможность получения адекватных моделей для динамических, в том числе нестационарных, случайных объектов. Достаточно хорошо разработанная прикладная математика для марковских процессов позволяет получать оптимальные оценки $\hat{x}(t)$, используя фильтры Калмана или Стратоновича, находить оптимальные алгоритмы управления, используя принцип двойственности с алгоритмами оценки и теорему о разделении алгоритмов стохастического управления, синтезировать различные процедуры обработки случайных сигналов, аппроксимируемых широким спектром моделей: случайных величин, процессов или полей. Так, для случайной величины x уравнение состояния (4) вырождается:

$$dx(t)/dt = 0. \qquad (5)$$

Очевидно состояние системы, определяемой уравнением (5) постоянно во времени. Случайность такой системы состоит в неизвестном значении самого состояния и наличии шумов наблюдения (измерения) $v(t)$, входящих в уравнение наблюдения:

$$y(t) = H(t)x(t) + v(t), \qquad (6)$$

где $H(t)$ - матричный коэффициент, элементы которого h_{kl} определяют величину сдвига и масштаба наблюдаемой величины $x(t)$.

Уравнение наблюдения (6) можно интерпретировать как самостоятельную модель типа «вход/выход» или «черный ящик». Что же касается модели состояния (4), то она уже не укладывается в рамки черного ящика из-за конкретизации внутренней структуры, возможной нелинейности, нестационарности, распределенности. Алгоритм оценки системы (4), построенные по методу Калмана-Бьюси преобразовывается в процедуру стохастической аппроксимации или процедуру Роббинса-Монро [5]. Следует заметить, что адекватной моделью ТКС может быть только n-мерное случайное поле $\vec{x}(t)$, где взаимные связи, определяют главные свойства (целостность, эмерджентность) этой сложной организационно-технической системы. При этом указанные взаимные связи в этой системе могут носить как вероятностный (за счет корреляции), так и регулярный, функциональный характер. Взаимная связь между компонентами x_i и x_j может образоваться в силу зависимых измерений, например при наличии переходных влияний, которые учитываются недиагональными элементами h_{kl}.

Выводы

1. Математические модели сложных систем, в том числе телекоммуникационных, должны быть построены с использованием многомерных представлений. Именно взаимные связи между компонентами (элементами) системы обеспечивают ей сверхитегральные свойства целостности и эмерджентности.

2. Учитывая то, что ТКС представляет собой сложную организационно-техническую систему, для нее не удается подобрать какой-либо одной общей математической модели. Множество моделей отображает различные функциональные свойства на уровне элементов, сети, предоставления услуг, бизнес-процессов. Целенаправленность ТКС определяется управлениями на каждом из уровней в соответствии с принятыми критериями оптимальности или же критериями достижимости (например, достижимости уровня качества обслуживания).

3. На практике редко когда встречаются чисто детерминированные или чисто случайные системы. В зависимости от соотношения этих составляющих используют детерминированные или стохастические модели систем. Детерминированные модели весьма удобные для анализа и синтеза: здесь широко разработанный и относительно простой математический аппарат, имеется возможность представлений во временной области и в частотной для линейных моделей. При использовании стохастических моделей – иная процедура дифференциальных и интегральных преобразований, кроме

того необходимо четко определиться: какой конкретно моделью следует аппроксимировать данную систему – случайным процессом или случайной величиной.

4. Наиболее распространенными являются два метода представления математических стохастических моделей: с помощью вероятностных характеристик (функции, плотности распределения вероятностей) или в пространстве состояний, где моделируется непосредственно динамика состояния самой системы. Представление вероятностными характеристиками, являющиеся предметом рассмотрения в теории вероятностей, характеризуют множество случайных величин. Описание этими характеристиками случайных процессов приводит к громоздким многомерным функциям и на практике обычно не используется. Более конструктивными являются предположения об эргодичности случайных процессов, что позволяет использовать аппарат случайных величин. Одновременно с этим исключается возможность моделирования динамики системы. Динамика, в том числе нестационарная, адекватно моделируется дифференциальными или разностными уравнениями в пространстве состояний. Перечисленные и многие другие представления оказываются полезными тех или иных стохастических систем. В тоже время модели в пространстве состояний несомненно являются более общими, полными и адекватными представлениями, поскольку отображают состояние всей системы, а не только ее части в виде вероятностных характеристик и позволяет получать адекватные конструктивные модели не только случайных величин, но и процессов и полей.

Секция № 1

ОСНОВЫ ТЕОРИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

ГЛОБАЛЬНАЯ СИСТЕМА РАСПРЕДЕЛЕНИЯ СИГНАЛОВ ТОЧНОГО ВРЕМЕНИ НА ОСНОВЕ СПУТНИКОВОЙ НАВИГАЦИОНОЙ СИСТЕМЫ ГЛОНАСС

Аджемов А.С., Мишенков С.Л., Смирнов Н.И., Антонников Д.О.,
Московский технический университет связи и информатики, Россия

Substantiated the possibility of the modernized Global Navigation Satellite System (GNSS) GLONASS as the main source of synchronization of telecommunication networks Russia CIS countries over time; lists the required parameters for the use of GLONASS in metrological purposes, the expediency of using GLONASS for transmission of information as a key segment of the mobile core network communication in places where you can not use fiber-optic or microwave connectivity of base stations.

В последние 5 лет в мире развиваются технологии синхронизации сетей связи по частоте и времени. В качестве основного источника для синхронизации по времени используется глобальная навигационная спутниковая система (ГНСС) GPS, которая имеет привязку к шкале Всемирного точного времени. На территории России, согласно требованиям Федерального закона от 07 июля 2003 г. №126-ФЗ «О связи», привязка сетей связи должна осуществляться к шкале Московского времени. Расхождение шкал времени Всемирного, которое получают с помощью ГНСС GPS, и Московского, - допускается в пределах 9 секунд, что значительно превосходит технически необходимое время. Таким образом, для временной синхронизации сетей электросвязи России необходимо использовать другие источники, основным из которых должна стать модернизируемая ГНСС ГЛОНАСС, которая была разработана более 30 лет назад и, несмотря на проведенные в последний год усовершенствования, требует дальнейшей модернизации [1]. Работы должны вестись в рамках новой ФЦП «Поддержание развития и использование системы ГЛОНАСС на 2012-2020 гг.».

Проведенные расчеты позволяют обосновать целесообразность использования ГНСС ГЛОНАСС так же и в качестве источника синхронизации сетей электросвязи по частоте.

Ввиду наличия на борту ГНСС ГЛОНАСС высокостабильных источников частоты и времени, подстраиваемых от Государственного эталона, в перспективе эту систему можно будет использовать также в метрологических целях.

В перспективе ГНСС ГЛОНАСС можно будет использовать и для передачи информации в качестве основного сегмента опорной сети мобильной связи в местах, где невозможно подключение базовых станций с использование кабелей, ВОЛС или радиорелейных линий связи.

В соответствии с постановлением Правительства Российской Федерации от 25 августа 2008 г. № 641 "Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS" в целях обеспечения национальной безопасности, проведения независимой политики в области спутниковой навигации, повышения эффективности управления движением транспорта, уровня безопасности перевозок пассажиров, специальных и опасных грузов оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS подлежат: космические средства; воздушные, морские и речные суда; автомобильные и железнодорожные транспортные средства; приборы и оборудование, используемые при проведении геодезических и кадастровых работ; средства, обеспечивающие синхронизацию времени.

Федеральным органам исполнительной власти поручено провести работы по поэтапному оснащению аппаратурой ГНСС ГЛОНАСС или ГЛОНАСС/GPS транспортных и технических средств и систем радиосвязи. С этой целью руководителями соответствующих федеральных органов исполнительной власти должны быть определены перечни транспортных и технических средств и систем, подлежащих оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS,

В соответствии подпунктом «в» пункта 5 Плана мероприятий по реализации постановления Правительства Российской Федерации от 25 августа 2008 г. № 641, разработанным и утвержденным Минтрансом России (поручение Правительства Российской Федерации от 4 августа 2009 г. № П7-26369), Минкомсвязи России поручено определить виды технических средств, обеспечивающих синхронизацию шкал времени и подлежащих оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS.

Анализ этой задачи показал, что для ее решения требуется проведение научных исследований. Для разработки требований к использованию ГНСС необходимо учитывать и накопленный международный опыт.

Доля производства продукции в валовом внутреннем продукте США за 2009 г. составила 12%, а доля, приходящаяся на оказание услуг, 88%. Таким образом, бывший крупнейший производитель продукции в процессе своего развития превратился в крупнейшего производителя услуг.

Роль информации в современном обществе неуклонно возрастает, поэтому в числе услуг важнейшими являются услуги получения, обработки и распределения знаний и информации.

Развитие процессов получения, обработки и распределения знаний и информации приводит современные структуры к созданию информационного общества. Под информационным обществом понимается постиндустриальное общество, - историческая фаза возможного развития цивилизации, - в которой главными продуктами производства становятся информация и знания. Отличительные черты информационного общества состоят в следующем: 1) увеличение роли информации, знаний и информационных технологий в жизни оператора электросвязи; 2) возрастание количества людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг в валовом внутреннем продукте; 3) нарастающая информатизация оператора электросвязи с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и электронных СМИ; 4) создание глобального информационного пространства, обеспечивающего: эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам, а также и удовлетворение их потребностей в информационных продуктах и услугах.

На создание информационного общества направлено и развитие России, что отражено в ряде программных документов последнего времени. На необходимость скорейшего развития информационного общества в России и перевода информационных технологий в прикладное русло указал Президент Российской Федерации Д.А. Медведев в своем выступлении на VII социально-экономическом форуме «Информационное общество» в Твери 8 июля 2010 г.

Одним из примеров при реализации такого подхода является проект «Электронное правительство», в рамках которого предусмотрено оказание государственных услуг при помощи информационных технологий.

Технологическая реализация данного проекта невозможна без обеспечения единой шкалы координированного времени Российской Федерации UTC(SU) (Московского времени). Кроме того, обеспечение единой шкалы координированного времени РФ UTC(SU) необходимо для реализации целого ряда технологий, среди которых: определение местоположения космических аппаратов (КА), воздушных объектов, морских и речных судов, автомобильных и железнодорожных транспортных средств, местоположение геодезических и кадастровых работ, а также предоставление услуг для современной радиосвязи.

Одним из наиболее перспективных путей решения этой задачи является использование возможностей ГНСС ГЛОНАСС.

Многие современные сети электросвязи нуждаются не только в частотной, но и во временной синхронизации. В недалеком прошлом сети требующие синхронизацию по времени ограничивались узко специальным применением, например, банковской транзакцией. Сегодня любая распределенная сеть связи оказывающая дополнительные услуги нуждается в привязке к шкале точного времени. Этого требует оказание определенных

услуг по расписанию (введение льготных тарифов в определенное время суток); приложения сетей цифрового телевидения (доступ к видео ресурсам по расписанию); системы с цифровой подписью; распределенное использование информационных порталов (например, оказание Государственных услуг в электронном виде); балансировка нагрузки в распределенных сетях с коммутацией пакетов информации и многое другое.

Анализ международного опыта временной синхронизации сетей связи

Международный Союз Электросвязи (ITU) разрабатывает новый стандарт частотной и временной синхронизации лишь на основе возможностей ГНСС GPS. С появлением данного стандарта ВСЕ сети связи будут использовать сигналы ГНСС GPS в качестве основных источников синхронизации, как это уже предусмотрено и осуществляется в сетях связи стандартов CDMA 2000; UMTS; Wi-MAX; LTE, а также в новом поколении оборудования стандарта GSM.

Для сохранения независимой политики страны Европейского Союза используют передачу синхросигналов по волоконно-оптическим линиям связи и готовятся к использованию европейского ГНСС ГАЛЛИЛЕО.

Возможности модернизируемой ГНСС ГЛОНАСС для синхронизации времени

В соответствии с требованиями интерфейсного контрольного документа системы ГЛОНАСС (редакция 5.0) «погрешность привязки шкалы системного времени ГЛОНАСС к шкале UTC(SU) не должна превышать 1 мкс». Данная погрешность относится к погрешности, присущей непосредственно системе ГЛОНАСС (погрешность выдаваемой поправки τ_c).

Таким образом, потребитель, оснащенный спутниковой навигационной аппаратурой, даже не учитывая аппаратурную погрешность, а также погрешности возникающие из за нестабильности среды распространения навигационного сигнала по трассе, не имеет права формировать шкалу времени, синхронизированную со шкалой времени UTC(SU) с погрешностью превышающую 1 мкс.

Аппаратурная погрешность (остаточная погрешность при калибровке группового времени запаздывания радиосигналов в спутниковой навигационной аппаратуре потребителей) и погрешности возникающие на трассе распространения навигационного сигнала (погрешности ионосферы, тропосферы) по сравнению с погрешностью, присущей системе ГЛОНАСС (1мкс), вносят незначительный вклад (в основном на уровне не превышающем 10 наносекунд).

Обработка информации, предоставляемой Международным бюро мер и весов (BIPM) в открытом доступе, в частности протоколов CIRCULAR T, за 2010 год (cirt 265 – cirt 271) свидетельствует о том, что погрешность существующей ГЛОНАСС в части привязки его шкалы времени к шкале времени UTC(SU) существенно меньше установленной в интерфейсном контрольном документе и составляет (150 – 200) нс.

Однако, аналогичная характеристика ГНСС GPS составляет лишь (10 – 30) нс, что позволяет использовать сигнал ГНСС GPS не только в качестве временной, но и в качестве частотной синхронизации сетей связи.

Литература:

Аджемов А.С., Мишенков С.Л., Смирнов Н.И., Кусков В.Д., Новикова Е.Л., Караваев Ю.А. Перспективы создания системы распределения сигналов точного времени на основе космической навигационной системы ГЛОНАСС //T.Comm. Телекоммуникации и транспорт. №5, - 2010 г.

ПРИНЦИПИ ПОБУДОВИ ІНВАРІАНТНИХ П'ЄЗОРЕЗОНАНСНИХ КОЛИВАЛЬНИХ СИСТЕМ

Зеленський О.О.[1], Підченко С.К.[2]
[1]Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
61070, Харків-70, вул. Чкалова, 17, каф. прийому, передачі та обробки сигналів
E-mail: azelens@mail.ru, тел. (057)-788-45-04, факс (057) 315-11-86
[2]Хмельницький національний університет
29016, м. Хмельницький, вул. Інститутська, 11, каф. радіоелектронних апаратів і телекомунікацій
E-mail: sergpchn@ya.ru, тел. (03822) 2-20-43, факс (03822) 2-32-65

The considered principles of the building invariant piezoelectric device on base multifrequency oscillatory systems, where is used joining main function to stabilizations of the frequency of the fluctuations with the current identification of destabilizing factors. An ideological basis of the given approach is the A. Harkevich's concept of the multilateral converter and the B. Petrov's principle of multi-channel systems.

Вступ

Анізотропія кристалічного п'єзоэлемента обумовлює виникнення різних видів пружних зв'язків напруг і деформацій, які викликають появу побічних резонансів у п'єзоколивальних системах (ПКС). Зазвичай багаточастотність розглядається як небажана властивість п'єзорезонансного пристрою (ПРП), і з нею, як і з чутливістю до факторів впливу (ФВ), намагаються боротися індивідуальними конструктивно-технологічними методами. Однак, в умовах масового використання ПКС, безупинного підвищення вимог до їх метрологічних характеристик під час дії цілого ансамблю факторів (температури, вібрації, електричного і магнітного поля і т. п.) ці методи малоефективні у вирішенні головної проблеми – інваріантності п'єзорезонансних пристроїв до факторів впливу.

З 1972 р. сформований і знайшов своє удосконалення принципово новий підхід до вирішення цієї проблеми, який базується на представленні ПКС у вигляді динамічного об'єкта з природною надмірністю у частотному базисі (багаточастотністю) і поточною ідентифікацією домінуючих зворотно діючих на його ФВ за допомогою алгоритмів обробки багаточастотних сигналів (з цієї причини методи реалізації такого підходу названі алгоритмічними). Оцінки величин ФВ використовуються для цілей компенсації, статування або як результат рішення самостійної задачі одночасного виміру m фізичних величин у локальному об'ємі вимірювального поля [1].

Матеріальною основою алгоритмічного підходу є бурхливий розвиток мікроелектронної і мікропроцесорної техніки, застосування якої в поєднанні з багаточастотним збудженням ПКС є «революційним напрямком» у прецизійній радіоелектроніці. Ідеологічною основою алгоритмічного підходу є фундаментальні результати теорії інваріантності та її застосувань в області вимірювальної техніки і автоматики.

1. ПРП як багатобічний перетворювач О. О. Харкевича

В рамках теорії багатобічного перетворювача О. О. Харкевича [2], яка базується на двох основних принципах – законі збереження енергії і принципі взаємності, багатобічний перетворювач (ББП) розглядається як перетворювач одного виду енергії в інший. Система характеризується узагальненими силами y_i, переміщеннями x_i та швидкостями $\dot{x}_i$, а також узагальненими константами. Її внутрішня енергія

$$W_\Sigma = W_K + W_{\Pi} + W_P, \qquad (1)$$

де $W_K(\dot{x}_j)$, $W_{\Pi}(x_j)$ – кінетична і потенційна енергія, $W_P(\dot{x}_j) = 2\int \Phi dt$ – енергія розсіювання; $\Phi(\dot{x}_j)$ – функція розсіювання, яка як і $W_K(\dot{x}_j)$ є квадратичною формою узагальнених

швидкостей. Повна зовнішня сила y_i обумовлена реакціями системи

$$y_i = \frac{d}{dt}\left(\frac{dW_K}{d\dot{x}_j}\right) + \frac{d\Phi}{d\dot{x}_j} + \frac{dW_П}{dx_j} \quad \text{або} \quad y_i = \sum_{j=1}^{m} \xi_{ij} x_j \,, \tag{2}$$

де $\xi_{ij} = p^2 m_{ij} + p r_{ij} + c_{ij}$, $p = d/dt$ – константи m_{ij}, r_{ij}, c_{ij} мають розмірності маси, механічного опору і пружності відповідно.

Переходячи до m потоків енергії, які втікають (витікають) з m сторін, одержимо

$$y_i = \sum_{j=1}^{m} z_{ij} \dot{x}_{ij}, \tag{3}$$

де $z_{ij} = 1/p\xi_{ij}$ – узагальнений опір. Тоді лінійна модель ББП буде мати вигляд

$$\mathrm{Y} = \mathrm{Z}\dot{\mathrm{X}}, \tag{4}$$

де $\mathrm{Y} = \left\{ y_i \right\}_{i=1}^{m}$, $\dot{\mathrm{X}} = \left\{ \dot{x}_j \right\}_{j=1}^{m}$, $\mathrm{Z} = \left\{ z_{ij} \right\}_{i,\,j=1}^{m}$ – симетрична матриця перетворення, елементи якої $z_{ij} = z_{ji}$, $i \neq j$ (реверсивність перетворення) – коефіцієнти перетворення, а $z_{ii} = y_i / \dot{x}_i \big|_{\dot{x}_k = 0}$, ($k = \overline{1,m}$; $k \neq i$) – власні опори. Використовуючи аналогію «сила – напруга», будь - який ББП приводиться до його лінійного $2m$ - полюсного аналога.

Для нелінійного ББП замість z_{ij} вводиться функція чутливості $S_{ij} = dy_i / dx_j \Big|_{\substack{x_k = const \\ \dot{x}_j = \dot{x}_{j0}}}$, причому в силу взаємності $S_{ij} = S_{ji}$, та відповідним вибором початкових значень x_{j0} система може бути приведена до лінеаризованої форми

$$\delta\mathrm{Y} = \mathrm{S}\delta\mathrm{X}. \tag{5}$$

Концепція ББП дозволяє трактувати ПРП як багатомірний об'єкт керування, у моделі якого явно фігурують контрольовані збурення:

$$y_i(p) = y_{з_i}(p) + \Delta y_{к_i}(p) + \Delta y_{нк_i}(p) = W_{ii}(p) x_{з_i}(p) + \\ + \sum_{j=1,\, j\neq i}^{m} W_{ij}(p) x_{з_j}(p) + \sum_{k=1}^{n} A_{i_k}(p) x_{к_k}(p) + \Delta y_{нк_i}(p), \tag{6}$$

де $\mathrm{X}_з(p) = \left\{ x_{з_i} \right\}_{j=1}^{m}$ – вектор заданого керування; $\mathrm{X}_к(p) = \left\{ x_{к_k} \right\}_{k=1}^{n}$ – вектор контрольованого збурення; $\mathrm{W}(p)$, $\mathrm{A}(p)$ – передатні функції каналів керування і каналів збурення відповідно; $\Delta y_{нк_i}(p)$ – додатковий рух за рахунок неконтрольованих збурень [3].

Відомо [4], що для абсолютної інваріантності координати y_i від збурення x_j

$$y_i(p) = \Phi(p) x_j(p); \; i = \overline{1,n}; \; j = \overline{1,m} \tag{7}$$

необхідно, щоб

$$\Phi_{ij}(p) \equiv 0. \tag{8}$$

Оскільки $\Phi_{ij}(p) = (C_{ij0} p^r + C_{ij1} p^{r-1} + \ldots + C_{ijr}) G_{ij}^{-1}(p) \equiv 0$, то з (8) випливає

$$C_{ijl} \equiv 0 \quad \forall l = \overline{0,r}. \tag{9}$$

Представляючи $C_{ijl} = a_l + b_l$ (принцип двоканальності) і, поклавши $a_l = -b_l$, можна задовольнити (8) у пасивній диференціальній (безідентифікаційній) системі шляхом підбору параметрів каналів, наприклад, використовуючи дві ПКС із протилежними за знаком температурними коефіцієнтами частоти (ТКЧ). У ідеальному випадку $y_i(t) \equiv g_i(t)$, тобто реальний рух системи точно відповідає бажаному.

На практиці, однак, завжди $y_i(t) - g_i(t) = \varepsilon$, тому скрізь надалі ми будемо мати інваріантний до ε ПРП. Крім того, оскільки $j > 1$, мова буде йти про його поліінваріантість.

Слід відзначити, що поділ усіх $m+n$ каналів керування ББП (6) на керуючі і дестабілізуючі є умовним. Наприклад, інваріантність кварцового генератора означає виконання (8) для всіх $m+n$ каналів, інваріантність же п'єзорезонансного датчика однієї фізичної величини вимагає виконання цієї умови для $m+n-1$ каналів. Такий вибір моделі дозволяє з єдиних позицій вирішувати проблему інваріантності усіх існуючих ПРП.

2. Аксіоматика багаточастотного підходу до інваріантості ПРП

Аксіоматика багаточастотного підходу до інваріантності ПРП як система основних його положень з урахуванням викладеного формулюється в такий спосіб.

1. Інваріантність до зворотно діючих ФВ досяжна для всіх типів фізично реалізованих ПРП незалежно від їхнього функціонального призначення, так як базується на їх найбільш загальних властивостях – багаторезонансності і стаціонарності характеристик чутливості до ФВ:

$$\mathrm{M} = \left\{ \tilde{\mathrm{A}} : \mathrm{X}_p(t) \times \mathrm{Y}(t^*),\ \mathrm{M} = \mathrm{Y} \in \Omega \subset \Re^n,\ \mathrm{X}_p \in G_x \subset \Re^m, \right.$$

$$\left. \mathrm{X}_p = \mathrm{X}_3 \cup \mathrm{X} \cup \theta \right\},\ \mathrm{M} = \bigcup_{i=1}^{L} \mathrm{M}_i,\ \tilde{\mathrm{A}}(t) = \tilde{\mathrm{A}}(t-\tau), \qquad (10)$$

де X_p – розширений вектор впливів на ПРП, L – число функціональних класів ПРП.

2. В інваріантних ПРП здійснюється поточна ідентифікація ФВ завдяки сполученню їх основних функцій з вимірювальними шляхом багаточастотного збудження. У загальному випадку ПРП розглядається як нелінійний багатоканальний об'єкт керування з оператором перетворення $\tilde{\mathrm{A}}$:

$$\tilde{\mathrm{A}} = comb(\mathrm{w}, \mathrm{A}), \qquad (11)$$

де **w** – оператор перетворення задаючих впливів.

3. Нелінійний динамічний БОК задовольняє вимогам спостереження (у метрологічному змісті), керованості, стійкості, тобто задача

$$\Delta\mathrm{Y} = \mathrm{A}\mathrm{X} \qquad (12)$$

коректна по Адамару на парі метричних просторів (G_x, Ω).

4. Комбіноване керування відповідає найбільш раціональній структурі інваріантного ПРП, є основою побудови безпошукових адаптивних пристроїв, які істотно розширюють можливості підходу. Задачі синтезу розімкнутого і замкнутого контурів комбінованої системи покладаються незалежними:

$$\mathrm{Q}_{зк} \neq \Phi(\mathrm{Q}_{рк}). \qquad (13)$$

5. Оптимізація розімкнутого контуру керування інваріантного ПРП полягає в підвищенні точності і вірогідності ідентифікації ФВ:

$$\mathrm{u}_{\mathrm{opt}} = \arg\min_{\mathrm{u}\in\mathrm{U}} \Re(\mathrm{u}),\ P_{\hat{X}} = \max_{\mathrm{u}\in\mathrm{U}} P\left\{ \mathrm{X}_0 \in G_x^0 \right\}, \qquad (14)$$

де $\Re(\mathrm{u})$ – похибка ідентифікації, U – множина керувань, G_x^0 – область ідентифікації X_0 із заданою похибкою.

6. Резонансні частотні канали БОК можуть комплексуватися амплітудними, фазовими і нерезонансними (потенційними, оптичними й ін.). У число останніх можуть входити конструктивно-технологічні «канали», які характеризують у нормованій моделі похибки виробництва ПРП:

$$\Delta\mathrm{Y} = \bigcup_{k=1}^{H} \Delta\mathrm{Y}_k;\ \Delta\mathrm{Y}_1 = (\omega_1, \omega_2, ..., \omega_{h1})^T;\ \Delta\mathrm{Y}_2 = (A_1, A_2, ..., A_{k2})^T, ...,\ \Delta\mathrm{Y}_H = (B_1, B_2, ..., B_H)^T. \qquad (15)$$

7. Багатомірний цифровий або аналоговий ідентифікатор ФВ представляє собою новий клас ПРП – багатопараметрових вимірювачів з одним чутливим елементом. Даний класу вимірювачів має самостійне значення у вимірювальній техніці [5].

Окреслимо основні механізми, які визначають динамічні властивості багаточастотних п'єзорезонансних коливальних систем.

1. Висока добротність прецизійних КР обумовлює великі значення постійних часу кіл БПКС ($0{,}01 - 0{,}05\,\text{с}$), що значно затягує процеси встановлення стаціонарної амплітуди коливань у порівнянні з LC - системами. За наявності механізмів амплітудно-фазової інверсії це призводить і до збільшення часу встановлення частоти коливань як одного із основних параметрів ПРП.

2. Перехід до багаточастотного режиму збудження КР, що необхідно для забезпечення інваріантності ПРП, значно ускладнює характер перехідних процесів в БПКС. Це викликано наявністю конкуренції коливань в каналах збудження, яка призводить до взаємовпливів динаміки одного коливання на інше.

3. Перехід до багаточастотного збудження вимагає більш жорсткого контролю сумарної потужності збудження та теплового стану КР. Швидкі зміни теплових потоків суттєво спотворюють температурне поле ПЕ, що обумовлює появу значних градієнтів температури. При цьому спостерігаються характерні термодинамічні зсуви частот, які помітно затягують динамічні процеси в БПКС. Цілком реальна ситуація, коли термодинамічні складові зсувів частоти є домінуючими; ситуація ускладнюється тим, що швидкі зміни температури різко спотворюють частотні властивості КР, при цьому таке поняття як ТЧХ в цих умовах втрачає зміст.

4. Необхідність виділення близько розташованих частот (ангармонік), забезпечення стійкості багаточастотного режиму генерації вимагає використання у фільтруючих колах ПРП вузькосмугових фільтрів (кварцових, ПАХ), що також погіршує динаміку перехідних процесів БПКС.

Висновки

Використання явища багаточастотної генерації в п’єзорезонансних пристроях, яке традиційно вважається шкідливим дозволяє значно знизити чутливість ПРП до ансамблю дестабілізуючих факторів за рахунок раціонального використання можливостей поточної ідентифікації останніх. Це дозволило сформулювати новий алгоритмічний підхід до проблеми інваріантності ПРП до факторів впливу, який використовує суміщення їх основних функцій з поточною ідентифікацією ФВ і орієнтований на різноманіття функціональних задач та на умови масового виробництва. Ідейною основою даного підходу є концепція багатобічного перетворювача О. О. Харкевича і принцип багатоканальності Б. М. Петрова. Матеріальну основу складають спільність найважливіших властивостей усіх ПКС (багаторезонансність і стаціонарність характеристик чутливості до ФВ). Отримані теоретичні результати стосуються не тільки всіх різновидів п’єзорезонансних пристроїв, але можуть бути поширені і на широке коло інших прецизійних радіотехнічних систем і пристроїв, які містять багаторезонансні високодобротні коливальні системи (об'ємні, діелектричні тощо).

Література:

1. Баржин В. Я. Многоволновый кварцевый резонатор – термодатчик / В. Я. Баржин, А. А. Зеленский, Ф. Ф. Колпаков [и др.] // Электронная техника. Сер. 10. Радиокомпон. – 1972. – Вып. I. – С. 54–57.

2. Харкевич А. А. Избранные труды в трех томах / А. А. Харкевич – Т. 1. М.: Наука, 1973. – 400 с.

3. Колпаков Ф. Ф. Многочастотный подход к проблеме инвариантности пьезорезонансных устройств / Ф. Ф. Колпаков // Радиотехника. – 1987. – № 9. – С.46 – 48.

4. Менский Б. М. Принцип инвариантности в автоматическом регулировании и управлении / Б. М. Менский – М.: Машиностроение. 1972. – 248 с.

5. Колпаков Ф. Теорія і реалізаційні основи інваріантних п’єзорезонансних коливальних систем: моногр. / Ф. Колпаков, С. Підченко; Нац. аерокосм. ун-т «Харьк. авіац. ін-т», – Х.: ХАІ, 2011. – 327 с.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ГИБРИДНОЙ СИСТЕМЫ ЗВУКОВОГО ВЕЩАНИЯ В ДИАПАЗОНЕ ОВЧ

Балан Н.М., Стрелковская И.В., Искендерзаде Ш.Г.
Одесская национальная академия связи им. А.С. Попова,
65021, г.Одесса, ул. Кузнечная, 1
E-mail: dekanat-is@rambler.ru

Presented hybrid systems digital sound broadcasting, where data transmits in analog and digital format at one time.

Известна система аналого-цифрового радиовещания в диапазоне ОВЧ FMeXtra, в которой для передачи суммарного сигнала левого и правого каналов $(A+B)$ используется полоса частот 0,03 – 15 кГц, для передачи разностного сигнала левого и правого каналов $(A-B)$ используются полосы частота 23 – 38 и 38 – 53 кГц, а для передачи цифрового сигнала дополнительной программы используется полоса частот 62 – 99 кГц. Пилот-тон передается на частоте 19 кГц, а сигналы RDS – на тройной частоте пилот-тона – 57 кГц. Недостатком системы радиовещания FMeXtra является повышенный уровень шумов в полосе передачи цифрового сигнала дополнительной программы на частотах 62 – 99 кГц.

Известна система аналого-цифрового радиовещания в диапазоне ОВЧ, в которой для передачи суммарного сигнала левого и правого каналов $(A+B)$ используется полоса частот 0,03 – 15 кГц, для передачи разностного сигнала левого и правого каналов $(A-B)$ используется однополосная модуляция и занимается полоса частота 23 – 38 кГц, а для передачи цифрового сигнала дополнительной программы используется полоса частот 41 – 53 кГц. Пилот-тон передается на частоте 19 кГц, а сигналы RDS – на тройной частоте пилот-тона – 57 кГц.

Недостатками такой системы является несовместимость стереофонического приема на типовой стереофонический приемник, предназначенный для приема стереопередачи по ДСТУ 4053-2001, поскольку в полосу частот разностного сигнала 23 – 53 кГц типового стереофонического приемника попадают разностный сигнал левого и правого каналов $(A-B)$, передаваемый на одной боковой полосе 23 – 38 кГц и цифровой сигнал дополнительной программы в полосе частот 41 – 53 кГц, который будет создавать шумы. В такой системе не возможно использование типового стереофонического приемника, поскольку он требует сложной переработки с установкой нового фильтра для выделения одной боковой полосы и сложной схемы демодуляции однополосного сигнала с применением синхронного детектора.

В основу новой предложенной авторами системы аналого-цифрового вещания в диапазоне ОВЧ поставлена задача уменьшения указанных недостатков. В предложенной системе аналого-цифрового вещания для передачи цифрового сигнала дополнительной программы используются симметричные относительно подавленной частоты поднесущей полосы частот 23 – 30 кГц и 46 – 53 кГц, у которых уровень шумов ниже, чем в полосе частот 62 – 99 кГц, а для передачи разностного сигнала, созданного с ограниченных по частоте до 7 кГц левого и правого каналов, используется балансно-модулированный сигнал с симметричными относительно подавленной частоты поднесущей нижней и верхней боковыми полосами в полосе частот 31 – 45 кГц. На рис. 1 представлен спектр составного стереофонического сигнала в новой системе аналого-цифрового радиовещания.

В предложенной системе аналого-цифрового вещания для передачи суммарного сигнала левого и правого каналов $(A+B)$ используется полоса частот 0,03 – 15 кГц, для передачи разностного сигнала $(A-B)$, созданного из ограниченных по частоте до 7 кГц левого и правого каналов, используется балансно-модулированный сигнал с симметричными относительно подавленной частоты поднесущей нижней и верхней боковыми полосами в полосе частот 31 – 45 кГц, а для передачи цифрового сигнала дополнительной программы используются симметричные относительно подавленной частоты поднесущей

полосы частот 23 – 30 кГц и 46 – 53 кГц. Пилот-тон передается на частоте 19 кГц, а сигналы RDS – на тройной частоте пилот-тона – 57 кГц.

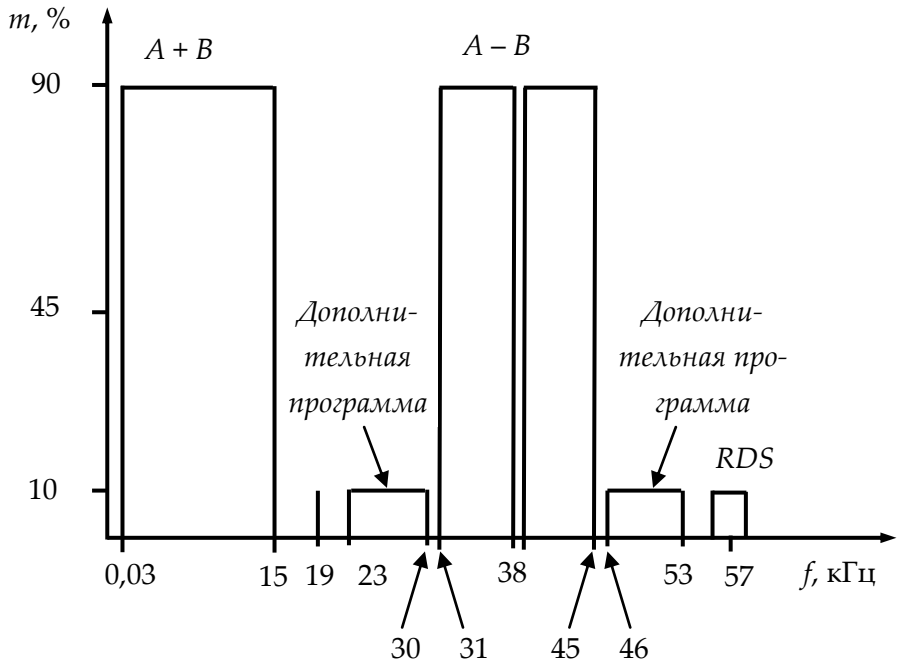


Рис. 1. Спектр составного стереофонического сигнала в системе [4] аналого-цифрового вещания

В предложенной системе аналого-цифрового вещания для передачи суммарного сигнала левого и правого каналов $(A+B)$ используется полоса частот 0,03 – 15 кГц, для передачи разностного сигнала $(A-B)$, созданного из ограниченных по частоте до 7 кГц левого и правого каналов, используется балансно-модулированный сигнал с симметричными относительно подавленной частоты поднесущей нижней и верхней боковыми полосами в полосе частот 31 – 45 кГц, а для передачи цифрового сигнала дополнительной программы используются симметричные относительно подавленной частоты поднесущей полосы частот 23 – 30 кГц и 46 – 53 кГц. Пилот-тон передается на частоте 19 кГц, а сигналы RDS – на тройной частоте пилот-тона – 57 кГц.

Существенным преимуществом предлагаемой системы при использовании типового стереофонического приемника является то, что требуется несложная замена только полосового фильтра разностного сигнала на фильтр с меньшей полосой пропускания в схемах с амплитудным или синхронным детектором или внедрения фильтрации выделенного разностного сигнала с ограничением его полосы до 7 кГц в любых схемах детектирования разностного сигнала, что позволяет оставить использование даже самых малогабаритных носимых приемников. Отсутствие в разностном сигнале частот больших 7 кГц, не влияющих на локализацию, будет компенсировано за счет поднятия уровня высоких частот в левом и правом каналах.

Обеспечение меньшего уровня шумов в системе аналого-цифрового вещания в диапазоне ОВЧ осуществляется следующим образом. Шумы в ограниченном полосе частот в системе стереофонического вещания в диапазоне ОВЧ с частотной модуляцией определяются по формуле

$$U_{ш} \approx \gamma_0 \omega_{в} \sqrt{\frac{2A}{P_0} \frac{\operatorname{arctg}(\Omega_{в}\tau)}{\tau}}\,, \qquad (1)$$

где γ_0 – коэффициент передачи тракта от входа частотного детектора к выходу приемника; $\omega_в$ – средняя частота занятой тем или иным сигналом полосы частот в составе составного стереофонического сигнала; A – спектральная плотность мощности; P_0 – мощность полезного сигнала; $\Omega_в$ – верхняя частота, равная половине занятой полосы частот; τ – постоянная времени звена предыскажений.

Отношение B шумов $U_{ш\,АЦВ}$ в полосах частот цифрового канала дополнительной программы в системе аналого-цифрового вещания в диапазоне ОВЧ относительно уровня шумов $U_{ш\,FMeXtra}$ в полосе частот цифрового канала дополнительной программы в системе радиовещания FMeXtra равна:

$$B = \frac{U_{ш\,АЦВ}}{U_{ш\,FMeXtra}}.$$

Учитывая, что для передачи цифрового сигнала дополнительной программы используются две полосы частот 23 – 30 кГц и 46 – 53 кГц, каждая из которых будет иметь шумы, соответственно, $U_{ш1\,АЦВ}$ и $U_{ш2\,АЦВ}$, то общие шумы в двух полосах

$$U_{ш\,АЦВ} = \sqrt{U^2_{ш1\,АЦВ} + U^2_{ш2\,АЦВ}},$$

тогда

$$B = \frac{\sqrt{U^2_{ш1\,АЦВ} + U^2_{ш2\,АЦВ}}}{U_{ш\,FMeXtra}}. \qquad (2)$$

Подставим формулу (1) в формулу (2) с внесением соответствующих буквенных индексов для каждой из систем: для полосы 23 – 30 кГц внесем индекс 1, а для полосы 46 – 53 кГц – индекс 2.

Получим отношение B

$$B = \frac{\sqrt{\left(\gamma_0 \omega_{в1\,АЦВ}\sqrt{\frac{2A}{P_0}\frac{\operatorname{arctg}(\Omega_{в1}\tau)}{\tau}}\right)^2 + \left(\gamma_0 \omega_{в2\,АЦВ}\sqrt{\frac{2A}{P_0}\frac{\operatorname{arctg}(\Omega_{в2}\tau)}{\tau}}\right)^2}}{\gamma_0 \omega_{в\,FMeXtra}\sqrt{\frac{2A}{P_0}\frac{\operatorname{arctg}(\Omega_{в\,FMeXtra}\tau)}{\tau}}}.$$

После ряда преобразований

$$B = \frac{1}{\omega_{в\,FMeXtra}}\sqrt{\frac{\omega^2_{в1\,АЦВ}\operatorname{arctg}(\Omega_{в1}\tau) + \omega^2_{в2\,АЦВ}\operatorname{arctg}(\Omega_в 2\tau)}{\operatorname{arctg}(\Omega_{в\,FMeXtra}\tau)}}.$$

Уровень L шумов $U_{ш\,АЦВ}$ в двух полосах частот цифрового канала дополнительной программы в системе аналого-цифрового радиовещания в диапазоне ОВЧ относительно уровня шумов $U_{ш\,FMeXtra}$ в полосе частот цифрового канала дополнительной программы системы радиовещания FMeXtra равна

$$L = 20\lg B = 20\lg\left(\frac{1}{\omega_{в\,FMeXtra}}\sqrt{\frac{\omega_{в1\,АЦВ}^2\ \mathrm{arctg}(\Omega_{в1}\tau) + \omega_{в2\,АЦВ}^2\ \mathrm{arctg}(\Omega_{в2}\tau)}{\mathrm{arctg}(\Omega_{в\,FMeXtra}\tau)}}\right). \qquad (3)$$

Подставим соответствующие значения параметров в формулу (3):

- в системе аналого-цифрового вещания в диапазоне ОВЧ в полосе частот 23 – 30 кГц $f_{в1\,АЦВ}$ = 26,5 кГц, $F_{в1\,АЦВ}$ = 7,0 кГц, τ = 75 мкс;

- в полосе частот 46 – 53 кГц $f_{в2\,АЦВ}$ = 49,5 кГц, $F_{в2\,АЦВ}$ = 7,0 кГц, τ = 75 мкс;

- в системе радиовещания FMeXtra в полосе частот 62 – 99 кГц $f_{в\,FMeXtra}$ = 80,5 кГц, $F_{в\,FMeXtra}$ = 18,5 кГц, τ = 75 мкс.

$$L = 20\lg\frac{1}{2\pi\cdot 80500}\times$$

$$\times\sqrt{\frac{(2\pi\cdot 25500)^2\,\mathrm{arctg}(2\pi\cdot 7000\cdot 75\cdot 10^{-6}) + (2\pi\cdot 49500)^2\,\mathrm{arctg}(2\pi\cdot 7000\cdot 75\cdot 10^{-6})}{\mathrm{arctg}(2\pi\cdot 18500\cdot 75\cdot 10^{-6})}} \approx -3{,}7\ \text{дБ}.$$

Выводы

1. В системе аналого-цифрового вещания в диапазоне ОВЧ полученный уровень L шумов $U_{ш\,АЦВ}$ в полосах частот цифрового канала дополнительной программы на 3,7 дБ меньше уровня шумов $U_{FMeXtra}$ в полосе частот цифрового канала дополнительной программы системы радиовещания FMeXtra 62 – 99 кГц, и является существенным выигрышем (3,7 дБ) от использования симметричных относительно подавленной частоты поднесущей полос частот 23 – 30 кГц и 46 – 53 кГц, в которых размещается цифровой сигнал дополнительной программы.

2. Наряду с передачей цифровых сигналов дополнительных программ использование балансно-модулированного сигнала с симметричными относительно подавленной частоты поднесущей нижней и верхней боковыми полосами в полосе частот 31 – 45 кГц, позволяет сохранить широкий парк типовых стереофонических приемников при несложной замене только полосового фильтра разностного сигнала на фильтр с меньшей полосой пропускания и имеет большое практическое значение для внедрения новых технологий цифрового вещания в диапазоне ОВЧ.

Литература:

1. Federal Network Agency. Documentation G771/00593/07. Compatibility Measurements FMeXtra interfering with Aeronautical Radionavigation. Germany, September, 2007.

2. Патент 40446 Україна, МПК H 04J 1/00. Спосіб аналого-цифрового радіомовлення у діапазоні ДВЧ / М.М. Балан, О.А. Виходець (Україна). Одеська національна академія зв'язку ім. О.С. Попова; заявл. 3.11.2008; опубл. 10.04.2009, бюл. № 7.

3. ДСТУ 4053-2001. Система стереофонічного звукового мовлення з пілот-тоном. Загальні технічні вимоги. Методи вимірювання. Київ, Держстандарт України, 2001.

4. Патент 47111 Україна, МПК H 04J 1/00. Спосіб аналого-цифрового мовлення у діапазоні ДВЧ / М.М. Балан, Ш.Г. Іскендерзаде, І.В. Стрелковська (Україна). Одеська національна академія зв'язку ім. О.С. Попова;заявл.26.10.2009;опубл.11.01.2010,бюл.№ 1.

5. Кононович Л. М. Стереофоническое радиовещание / Л. М. Кононович – М.: Связь, 1974. – 262 с.

МЕТОДЫ ОЦЕНКИ ПОМЕХОЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Серков А.А.
Национальный технический университет «Харьковский политехнический институт»
61002, Харьков, ул.Фрунзе, 21, каф. систем информации, тел.(057)707-66-18,
E-mail: saa@kpi.kharkov.ua ; факс (057)707-66-18

The given work is devoted to the modern developments in the field of antinoise telecommunication devices. Organized analysis and categorization of existing experimental methods of estimation of level noiseproof the telecommunication systems. Designed recommendations on use of the experimental methods with varied class of the systems.

Введение. Бурное развитие телекоммуникационных систем и технологий делает актуальной задачу обеспечения надежной и бесперебойной работы технических устройств телекоммуникационных систем в сложной электромагнитной обстановке, создаваемой работой базовых станций различных операторов. При этом общая решаемая задача включает как вопросы обеспечения внутрисистемной электромагнитной совместимости (ЭМС) отдельных узлов и блоков в составе телекоммуникационной системы, так и задачи обеспечения ЭМС, создаваемой внешними источниками помех. Внешними источниками помех, влияющими на качество предоставляемых телекоммуникационных услуг, являются базовые станции мобильной связи, молниевые разряды, радиолокационные станции и т.д.

Постановка проблемы. Сложность учета конструктивных особенностей создаваемых телекоммуникационных систем, а также внешней электромагнитной обстановки, где предполагается её использование, не дают возможности создания адекватных компьютерных моделей, позволяющих в полной мере исследовать достигнутый уровень помехозащищенности технических систем и принять конструктивные меры по их доработке. Наиболее полные и адекватные результаты дает проведение лабораторных исследований опытных образцов в условиях физического моделирования электромагнитной обстановки [1-4]. Испытания относятся к методам исследования, направленным на определение реального состояния и технических характеристик объекта экспериментальным путем Они остаются единственным достоверным критерием определения уровня электромагнитной помехозащищенности систем в условиях действия электромагнитных помех. При этом основным требованием, предъявляемым к испытаниям, является наиболее полное воспроизведение тех реальных условий, в которых будет происходить эксплуатация систем.

Целью исследования является анализ и систематизация существующих экспериментальных методик по оценке помехозащищенности телекоммуникационных систем.

Методы испытаний телекоммуникационных систем. Различают три основных метода испытаний. Это натурные испытания, воспроизведение реальной помеховой электромагнитной обстановки и имитация дестабилизирующих факторов в опасных трактах объектов. ***Натурные испытания*** являются самыми достоверными, но в то же время дорогостоящими и трудоемкими. Поэтому данный вид испытаний является мало перспективным и применяется в исключительных случаях. Более перспективным является метод, базирующийся на искусственном создании в ограниченных объемах испытательных площадок электромагнитной помеховой обстановки, которая по своим амплитудно-временным характеристикам соответствует реальной. Преимуществом данного метода является возможность многократного повторения воссозданной обстановки, что позволяет более точно определить реальные уровни помехозащищенности систем и оценить эффективность выполненных доработок. Для сложных разветвленных систем наиболее часто применяется метод, базирующийся на имитации токов и напряжений помех и их инжекции в опасные тракты систем. Однако его реализация требует выполнение ряда обязательных условий. В первую очередь необходимо наличие нормированных параметров токов и напряжений помех для всех видов опасных трактов систем от широкого класса электромагнитных воздействий. При этом необходима оснащенность испытательных ла-

бораторий и центров аттестованными генераторами этих помех, а также методическое обеспечение проведения испытаний, адаптированное к данной технической системе.

Метод, базирующийся на искусственном создании электромагнитной помеховой обстановки, предполагает использование соответствующих источников. В зависимости от амплитудно-частотных параметров воспроизводимой электромагнитной обстановки различают открытые волноводные системы (полосковые линии), излучающие системы ближней зоны и СВЧ-излучающие системы.

Открытые волноводы (полосковые линии) рекомендованы IEC 61000-4-23 для воспроизведения электромагнитной обстановки в частотном диапазоне от 10 до 150 МГц. Требуемые амплитудно-временные характеристики воспроизводимых электромагнитных полей в рабочем объеме системы определяются параметрами задающего генератора и согласованной нагрузки полосковой линии. Данный тип установок позволяет получать однократные импульсы электромагнитного поля с длительностью фронта от единиц до сотен наносекунд и длительностью импульса от десятков наносекунд до сотен микросекунд. Амплитудные значения варьируются от десятков до сотен киловольт на метр по электрическому полю и от десятков до сотен ампер на метр по магнитному полю. Моделирующие установки данного типа нашли свою практическую реализацию в ряде стран: Канаде, Израиле, Италии, России, Украине, США и др. [4].

Излучающие системы ближней зоны. Моделирующие установки данного типа рекомендованы для воспроизведения электромагнитной обстановки при горизонтальной поляризацией электрического поля. При этом воспроизводятся электромагнитная обстановка, соответствующая разряду молнии. Моделируются однократные импульсы электромагнитного поля с длительностью фронта от единиц до сотен наносекунд и длительностью импульса от десятков наносекунд до миллисекунд.

СВЧ-излучающие системы. В основу создания испытательных установок данного типа были положены радиолокационные технологии. При этом используются СВЧ-излучающие системы с зеркальными либо рупорными антеннами. Требуемые амплитудно-временные характеристики воспроизводимого импульсного электромагнитного излучения получают при помощи сверхширокополосного генератора емкостного или индукционного типа.

Метод имитации дестабилизирующих факторов в опасных трактах объектов основан на механизме проникновения энергии, наведенной во внешних цепях телекоммуникационных систем во внутрь экранированных корпусов. При этом появляется возможность проведения испытаний методом имитации токов и напряжений помех на их входах (выходах) исследуемых устройств. Такие электромагнитные помехи определяются как кондуктивные. Для имитации наводок, возникающих в типовых внешних цепях объектов, используют специальные генераторы кондуктивных помех. Причем такие методы испытаний подразделяют на три основных вида. В первую очередь это *непосредственная подача тока/напряжения* помехи на входы/выходы объекта. Другим видом испытаний является *подача помехи на внешние линии связи*, электропитания, заземления, находящиеся в рабочих режимах с использованием устройств развязки через разделительные емкости или зажимы и *инжекция помех* в линии связи, находящиеся в рабочих режимах без разделительных систем *посредствам емкостной или индуктивной связи.* Данные методы проведения испытаний наиболее применимы для распределенных систем, находящихся в опытной эксплуатации. Однако при проверке конструкторских решений по оценке защитных свойств корпусов на стадиях заводских доработок проводят *испытания по оценке уровней проникновения* электромагнитных полей в корпуса-экраны объектов [1]. Этот метод испытаний направлен на определение уровня проникновения электромагнитных полей в экранируемые корпусами-экранами области через электрические неоднородности - вентиляционные отверстия, стыковочные узлы, крышки и т.п. и относится к предварительным тест-испытаниям исследовательского типа. Целью таких испытаний является подтверждение правильности принятых конструктивных решений по размещению в корпусах-кранах электрических неоднородностей того или иного вида. Основу для

реализации данной методики проведения испытаний составляют измерения формируемых полей без экрана и при наличии экрана.

Выводы. Качество предоставляемых телекоммуникационных услуг зависит от надежной и бесперебойной работы технических устройств телекоммуникационных систем в сложной электромагнитной обстановке. Существующие методы оценки помехозащищенности телекоммуникационных систем позволяют оценить и произвести доработку систем как на ранних стадиях разработки, стадии заводских испытаний, так и на стадии приемо-сдаточных испытаний. Причем, для каждой из стадий следует использовать соответствующие методики, адаптированные к техническим особенностям исследуемой системы.

Литература:

1. Кравченко В.И., Серков А.А. и др. Определение защитных свойств объектов ракетно-космической техники при воздействии электромагнитных импульсных полей естественного и искусственного происхождения / Харьков: НТУ „ХПИ”, 2007. - 205с.
2. Кравченко В.И. Электромагнитное оружие / Харьков: НТУ „ХПИ”, 2008. - 185с.
3. Кравченко В.И. Оружие на нетрадиционных физических принципах. Электромагнитное оружие / Харьков: «НТТМ», 2009. - 266с.
4. Кравченко В.И. Электромагнитный терроризм / Харьков: «НТТМ», 2011. - 392с.

ПОДХОД К СОЗДАНИЮ КОМПЛЕКСНЫХ MDE-МОДЕЛЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Алексеев Н.А.[1], Глоба Л.С.[2]
[1]Национальный технический университет Украины «КПИ»,
[2]Институт телекоммуникационных систем
03056, Київ, пер. Индустриальный, 2, тел. (044) 406-82-99,
E-mail: alexeyev@its.kpi.ua ; факс (044) 406-82-99

The work is devoted to the new approach to creation of complex software models which employ application's distinction to business logic and interface, both described by XML. Syntax of offered for describing application's algorithm is similar to common programming languages. FaceXML[1] is used to describe user interfaces. Tools for WYSIWYG design of the algorithm and interface as well as interpreter which executes resulting model are developed.

I. Введение

Существует множество разнородных технологий для создания программного обеспечения. Реализация зависит от платформы, на которой предполагается работа, от типа приложения – будь то настольное приложение, веб-приложение, или же веб-сервис, разработчикам все это нужно учитывать при планировании, проектировании, и реализации программного обеспечения. Как решение этой и других проблем, была предложена методология разработки ПО под названием MDE (Model Driven Engineering), наиболее известной инициативой которой является методология MDA (Model Driven Architecture). В этой методологии различают два типа моделей: PIM — платформенно независимая модель и PSM — платформенно зависимая модель. MDA не специфицирует на каком языке описана PIM, но требует чтобы описание было на языке, который определен формально и пригоден к автоматической обработке. Но в итоге даже такой подход приводит к необходимости реализовывать ПО на каждой платформе, даже если и возможна автоматическая генерация платформенно-зависимого кода. MDA сосредотачивается на описании логики, опуская столь важную часть любого программного продукта, как интерфейс взаимодействия с пользователем. К тому же, шаги преобразования из PIM в PSM никак не ускоряют процесс разработки, хотя одной из целей MDA была реализация RAD (Rapid Application Development). Для преодоления описанных недостатков предлагается методология создания комплексной (и логики, и пользовательского интерфейса) модели программного обеспечения, способной к непосредственному выполнению, опуская шаг преобразования из PIM в PSM.

II. Описание методологии

На рис. 1 приведена схема, отображающая архитектуру применяемой технологии, применяемой в данной методологии. Описание основных архитектурных элементов приведено ниже:

Скрипт - та часть технологии, которая отвечает за бизнес-логику. Другими словами это – алгоритм работы приложения. Бизнес-логика описывается посредством xml-тегов, подобных к синтаксису большинства обычных языком программирования.

Интерфейс – использует FaceXML[1] для кросс-платформенного описания интерфейса, к событиям которого могут быть привязаны операции из скрипта.

Интерпретатор – интерпретатор реального времени выполнения, выполняющий приложение. Выполняет его с выводом пользовательского интерфейсом, или без, в зависимости от параметров. Параметры позволяют задать 3 режима выполнения приложения:

1. *Запуск в виде локального приложения* – запуск приложения на локальной машине с отображением пользовательского интерфейса.

2. *Запуск в виде веб-приложения* – на локальной машине запускается встроенный в интерпретатор веб-сервер, и на нем выполняется приложение, интерфейс отображается в

виде HTML (формы), бизнес-логика выполняется на стороне сервера (т.е. локального компьютера), интерфейс обновляется средствами AJAX[2].

3. *Запуск в виде веб-сервиса* – на локальной машине запускается встроенный в интерпретатор веб-сервер, интерфейса пользователя не использует, а работает в режиме веб-сервиса, предоставляя указанные в скрипте операции и их параметры. Веб-сервис[3] может быть как RESTful, так и использовать для маршалинга SOAP[4]. Также, при данном выполнении приложения, можно получить доступ к автоматически сгенерированному WSDL[5] для импорта этого веб-сервиса.

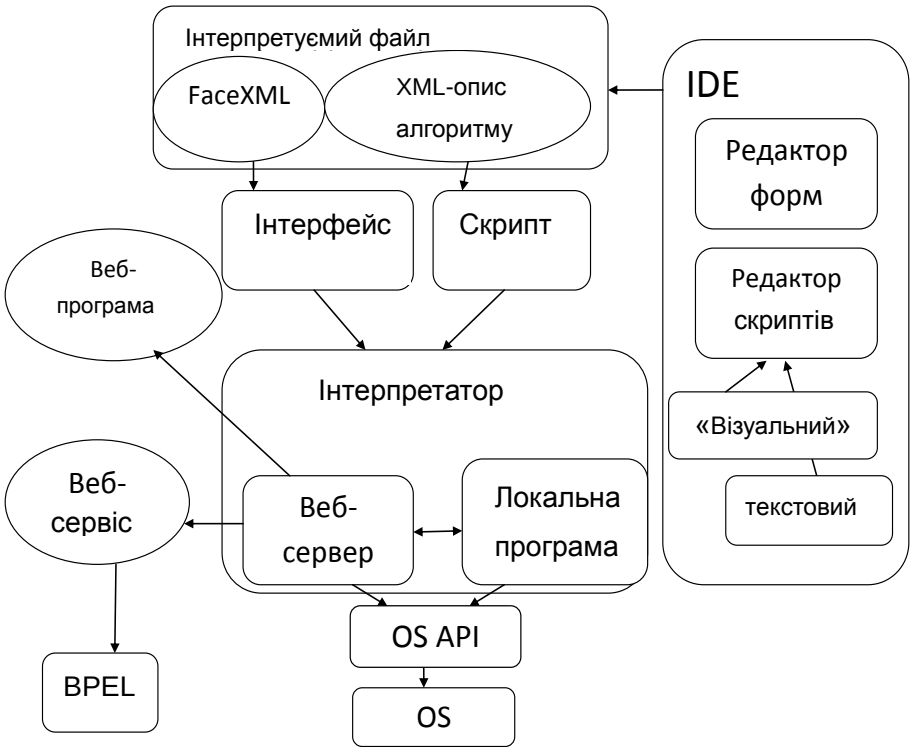


Рис. 1. Архитектура системы для построения комплексной MDE-модели ПО

IDE – среда для визуального создания пользовательского интерфейса и/или скриптов, которые могут взаимодействовать с интерфейсом. Результат сохраняется в одном файле. Визуальное создание скриптов осуществляется с помощью построения блок-схем требующегося алгоритма работы, в качестве блоков используя конструкции переходов, циклов и т.д., а также объектов для работы с БД, сетью и т.д. У каждого блока есть точки входа – параметры скрипта, который данный блок представляет и точка выхода – возвращаемое значение. Соединяя в требующейся последовательности входы и выходы строится алгоритм. Специальный блок – точка начала выполнения привязывается к некоторому событию от интерфейса или системному событию. Также существует точка окончания выполнения, куда привязываются все ветки скрипта ведущие к окончанию обработки события. Каждый блок имеет свойства, специфичные для объекта который он представляет, например имя базы данных, имя пользователя и пароль. При сохранении проекта такая блок схема преобразуется в скрипт вышеописанного формата. Также существует возможность вручную редактировать скрипт представленный блок схемой в среде, используя вкладку с исходным кодом скрипта.

III. Выводы

Предлагаемый подход позволит избежать описанные выше проблемы. Используя FaceXML[1] для кросс-платформенного описания интерфейса, а также специализированный язык программирования, и промежуточный слой выполнения для программного

обеспечения предлагаемой технологии, позволяет запускать ПО на многих платформах, как настольных (Windows, Linux, Unix), так и мобильных (Android, Java ME, Windows Mobile).

Результатом применения данной методологии является модель программного обеспечения, которая пригодна к выполнению. Разделение технологии на интерфейс и бизнес-логику, позволяет промежуточному слою интерпретировать приложение и как локальное, и как веб-приложение, и как веб-сервис без каких-либо изменений со стороны разработчика.

В случае выполнения в виде веб-сервиса, результат может использоваться в виде единицы для построения enterprise-приложений, например средствами BPEL[6][7]. В данном ракурсе технология позволяет перейти к более высокому уровню абстракции, и отказаться от написания веб-сервисов средствами традиционных языков.

Для написания логики приложения предлагается использовать среду, которая использует диаграммы и связи между ними, описывая необходимые действия. Полученная диаграмма автоматически преобразовывается в модель бизнес-логики, а также привязывается к интерфейсу.

Литература:

1. Глоба Л.С., д.т.н., проф., Ермольчев А.В., Оленюк В.Н. Инструментарий проектирования и разворачивания бизнес-процессов в распределенных системах// источник

2. Ullman, Chris. Beginning AJAX// Wiley Pub., 2007, 498 p. ISBN0470106751

3. Benslimane, Djamal; Schahram Dustdar, and Amit Sheth. Services Mashups: The New Generation of Web Applications // IEEE Internet Computing, vol. 12, no. 5, 2008

4. Martin Gudgin, Marc Hadley, Noah Mendelsohn,Jean-Jacques Moreau, Henrik Frystyk Nielsen, Anish Karmarkar, Yves Lafon. SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) // W3C Recommendation 27 April 2007.

5. Roberto Chinnici, Jean-Jacques Moreau, Arthur Ryman, Sanjiva Weerawarana. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language // W3C Recommendation 26 June 2007

6. OASIS consortium. OASIS Web Services Business Process Execution Language TC - Web Services Business Process Execution Language Version 2.0 //OASIS Recommendations, 11 April 2007

7. Anneke Kleppe. MDA Explained, The Model Driven Architecture: Practice and Promise // Addison-Wesley, 2003, 170p. ISBN 0-321-19442-X

ОЦЕНКА ЭФФЕКТИВНОСТИ ОДНОМАРШРУТНОГО И МУЛЬТИМАРШРУТНОГО МЕТОДОВ ПЕРЕДАЧИ СООБЩЕНИЙ

Лосев, Ю.И., Шматков С.И., Руккас К.М., Щебенюк В.С.
Харьковский национальный университет радиоэлектроники
(61166, г. Харьков, пр. Ленина,14, каф. ТКС)
e-mail: krukkas@gmail.com

The article provides a comparative analysis unicast and multicast transmission techniques in modern computer networks. As an indicator of efficiency, we use message delivery time. On the basis of comparative analysis, the necessary conditions for the use multicast messaging

Введение

Управление потоком информации при многопутевой передаче является достаточно сложным процессом, учитывающее особенности передачи как по одному каналу, так и с учетом совместимого функционирования нескольких каналов.

В наиболее простом варианте многоканальная система представляет совокупность независимо функционирующих каналов. В этом случае, как показано ранее, характеристики системы будут определяться характеристиками худшего канала.

Поэтому, прежде чем разработать модель процесса управления в многоканальной системе, разработаем модель управления одним информационным каналом, в соответствии с которой определим методику оценки таких основных вероятностно – временных характеристик канала, как среднее время доставки сообщения и вероятность доставки за заданное время.

Сначала разработаем математическую модель, обеспечивающую возможность определения таких основных характеристик, как среднее значение и дисперсию времени доставки сообщений.

Разработанная модель должна учитывать влияние указанных параметров на основные вероятностно-временные характеристики.

В настоящее время описаны математические модели многопутевой маршрутизации, основанные на теории графов и теории массового обслуживания [1-4]. Проведенный анализ указанных работ показывает, что описанные модели обеспечивают возможность оценки основных вероятностно-временных характеристик при ограничениях на входящий поток заявок. При использовании этих моделей невозможен учет особенностей применяемого протокола; отсутствие возможности учета влияния на основные вероятностно-временные характеристики (ВВХ) таких режимов работы систем, как цикловая и межпутевая синхронизация; трудность в получении общих выражений для определения основных ВВХ для многоканальных систем с различными интенсивностями обслуживания и т.п.

Известны математические модели, основанные на использовании линейного программирования [4]. Однако все эти модели посвящены решению задачи маршрутизации и не устраняет указанные выше недостатки. Управление потоком предполагает, что выбор маршрута уже проведен. Необходимо обеспечить качественную параллельную доставку фрагментов сообщения таким же образом, как и в случае последовательной передачи этих фрагментов.

Изложение основного материла

В распределённых системах обмен информацией между отдельными или группами пользователей может осуществляться по одному маршруту целыми сообщениями с их фрагментацией и с передачей фрагментов по разным маршрутам.

Для определения этих условий проведём сравнения метода мультимаршрутной передачи с методом передачи по одному пути (маршруту). При передаче по одному пути блок данных может передаваться без фрагментирования, с фрагментированием и с последующей последовательной передачей фрагментов.

Предположим, что блок разделен на M фрагментов. Каждый фрагмент содержит $m_{П}$ информационных и $k_{сл}$ служебных символов.

В системах с обратной связью каждый фрагмент может повторяться в случае обнаружения ошибки. Между двумя оконечными пунктами находится β промежуточных узлов. Поскольку задержка на узлах не зависит от числа передаваемых фрагментов, а определяется только числом промежуточных узлов, время передачи блока, будет определяться выражением

$$T_{ПЕРбл} = \sum_{j=1}^{M} T_{ПЕРj} \cdot \theta_j , \qquad (1)$$

где $T_{ПЕРj} = T_{ФРj} \cdot r_{31} + \sum_{i=1}^{\beta+1} T_{Pij} + \sum_{i=1}^{\beta} T_{ЗАДуij}$,

$T_{ЗАДуij}$ - время задержки на узле $T_{ЗАДуij} = T_{ФРj} \cdot r_{31}$;

$T_{ФРj}$ - длительность фрагмента $T_{ФРj} = \frac{m_{nj} + k_{сл}}{B}$, $k_{сл} = \log(m_n)$.

r_{31} – избыточность за счет заголовка фрагментов.

Коэффициент θ_j , в соответствии с [5], учитывает влияние обратной связи в дуплексном канале.

Поскольку информационная нагрузка равна сумме поступающей нагрузки $\sum_{j=1}^{M} m_{nj}$, скорость передачи информационных символов будет равна

$$C_1 = \frac{\sum_{j=1}^{M} m_{nj}}{T_{ПЕРбл1}} . \qquad (2)$$

Если участки сети имеют одинаковые характеристики и фрагменты одинаковой длины, то при последовательной передаче фрагментов выражение (1) будет иметь вид

$$T_{ПЕРбл1} = M \cdot T_{ПЕР1} \cdot \theta_1 ;$$

$$T_{ПЕРj} = T_{ФРj} \cdot r_{31} + (\beta + 1) \cdot T_P + \beta \cdot T_{ЗАДу1} .$$

Входящие в эти выражения величина θ_1 определяются по следующей формуле:

$$\theta_1 = 1 + \frac{\left(1 + \frac{T_{TA1}}{T_{ПЕР1}}\right) \cdot \left(P_{ПОТ_1} + P_{OO_1}\right)}{1 - P_{ПОТ_1} - P_{OO_1}} . \qquad (3)$$

где время таймаута равно $T_{TAj} = T_{ПЕРj} \cdot \eta$; $\eta > 1$; $P_{OO_1} \cong n \cdot \left(1 - 2^{-k_{сл}}\right) \cdot P_{ОШ}$; $P_{ош}$ - вероятность ошибки в принятом фрагменте.

При средней нагрузке время задержки на узле равно $T_{ЗАДу1} = T_{ФР}$.

Вероятность потери фрагмента определяется по формуле

$P_{ПОТ1} = (1 - \lambda_1 \cdot T_{ФР}) \cdot (\lambda_1 \cdot T_{ФР})^W$, где W – емкость буферного запоминающего устройства на узле коммутации;

Если блок передается без деления на фрагменты, то время его передачи будет равно $T_{ПЕРбл2} = M \cdot T_{ПЕР2} \cdot \theta_2 \le$,

где $T_{ПЕР2} = T_{БЛ} \cdot r_{32} + \sum_{i=1}^{\beta+1} T_{Pi} + \sum_{i=1}^{\beta} T_{ЗАДi}$, $T_{БЛ} = M \cdot T_{ФР}$. При средней нагрузке системы $T_{ЗАДi} = T_{БЛ}$.

В соответствии с (3), коэффициент θ_2 , определяется по выражению:

$$\theta_2 = 1 + \frac{\left(1 + \frac{T_{TA2}}{T_{ПЕР2}}\right) \cdot \left(P_{ПОТ_2} + P_{OO_2}\right)}{1 - P_{ПОТ_2} - P_{OO_2}},$$

где $T_{TA2} = T_{ПЕР2} \cdot \eta$; $P_{OO_2} \cong M \cdot n \cdot \left(1 - 2^{-k_{сл}}\right) \cdot P_{ОШ_2}$; $P_{ПОТ_2} = (1 - \lambda_2 \cdot M \cdot T_{ФР}) \cdot (\lambda_2 \cdot M \cdot T_{ФР})^W$.

Поскольку $\lambda_2 = \lambda_1 / 1$, получим

$$P_{ПОТ_2} = (1 - \lambda_1 \cdot T_{ФР}) \cdot (\lambda_1 \cdot T_{ФР})^W,$$

т.е. $P_{ПОТ_1} = P_{ПОТ_2}$.

Время задержки на узле при средней нагрузке в сети равно

$$T_{ЗАДу2} = M \cdot T_{ФР} \cdot r_{32} = T_{БЛ} \cdot r_{32}.$$

Для сравнения двух методов передачи возьмем и отношение $\frac{T_{ПЕРбл1}}{T_{ПЕРбл2}}$

$$\frac{T_{ПЕРбл1}}{T_{ПЕРбл2}} = \frac{\left[M \cdot T_{ФР} \cdot r_{31} + \beta \cdot T_{ФР} \cdot r_{31} + (\beta + 1) \cdot T_P\right] \cdot \theta_1}{\left[M \cdot T_{ФР} \cdot r_{32} + M \cdot \beta \cdot T_{ФР} \cdot r_{32} + (\beta + 1) \cdot T_P\right] \cdot \theta_2}. \quad (4)$$

Определим отношение $\frac{\theta_1}{\theta_2}$

$$\frac{\theta_1}{\theta_2} = \frac{1 + \frac{T_{KB}}{T_{ПЕР1}} + \frac{\left(1 + \frac{T_{TA1}}{T_{ПЕР1}}\right) \cdot \left(P_{ПОТ1} + P_{OO1}\right)}{1 - P_{ПОТ1} - P_{OO1}}}{1 + \frac{T_{KB}}{T_{ПЕР2}} + \frac{\left(1 + \frac{T_{TA2}}{T_{ПЕР2}}\right) \cdot \left(P_{ПОТ2} + P_{OO2}\right)}{1 - P_{ПОТ2} - P_{OO2}}}. \quad (5)$$

Учитывая, что $P_{OO1} < P_{OO2}$, $P_{ПОТ2} = P_{ПОТ1}$, $\frac{T_{TA1}}{T_{ПЕР1}} = \frac{T_{TA2}}{T_{ПЕР2}}$ получим неравенство $\frac{\theta_1}{\theta_2} \le 1$.

Поскольку $T_{ЗАДу1} < T_{ЗАДу2}$, несмотря на то, что r_{31} несколько больше, чем r_{32} получим неравенство $\frac{T_{ПЕРбл1}}{T_{ПЕРбл2}} < 1$.

Таким образом, время передачи сообщения одним блоком больше, чем при передаче фрагментами. Следовательно, скорость передачи информационного символа при делении на фрагменты будет больше.

Это объясняется тем, что вероятность повтора блока больше, чем вероятность повтора фрагмента, т.к. длина блока больше. Кроме этого, при повторе длина повторяемого сообщения больше.

Выводы

Разработана математическая модель управления информационным каналом. Модель для систем с обратной связью обеспечивает возможность определения основных вероятностно-временных характеристик канала: среднее значение и дисперсию времени доставки фрагментов, а также вероятность доставки за заданное время. Разработанная модель учитывает возможность управления шириной окна и длительностью тайм-аута,

параметрами, влияющими на эффективный обмен. На основании разработанных моделей определения основных вероятностно-временных характеристик проведена сравнительная оценка различных методов передачи. Доказано, что для уменьшения времени доставки целесообразно разделение передаваемого сообщения на фрагменты.

Определена необходимость применения мультимаршрутной передачи. Показана полезность такой передачи для повышения скорости, уменьшения времени доставки, повышения надежности и живучести системы передачи, уменьшения вероятности ошибки. Обоснованы условия, при которых ввод нового дополнительного канала дает положительный результат по скорости передачи информации.

Литература

1. Лосев Ю. И., Бердников А. Г., Гойхман Э. Ш. Адаптивная компенсация помех в каналах связи. – М.: Радио и связь, 1988. – 209 с.

2. Bolch G., Greiner S., De Meer H., Trivedi K. – Queueing networks and Markov chains: modeling and performance evaluation with computer science approach 2nd ed. Wiley-Interscience, 2006. 869 p.

3. Филлипс Д., Гарсиа-Диас А. Методы анализа сетей: Пер. с англ. – М.: Мир, 1984. - 496 с., ил.

4. Шварц М. Сети связи: протоколы, моделирование и анализ. В 2 ч.: Пер. с англ. – М.: Наука, Гл. ред. физмат. лит., 1992. – Ч. 1. – 336 с

5. Лосев Ю. И., Руккас К. М., Шматков С.И. Математическая модель процесса информационного обмена при многопутевой передаче.// Збірник наукових праць. Системи управління, навігації та зв'язку. – Київ,2010. – Вип. 1. (13). – С. 205 – 209.

МОДЕЛЬ ВЫСОКОУРОВНЕВОЙ ВРЕМЕННОЙ ФРАГМЕНТАЦИИ ЦИКЛИЧЕСКИХ ЗАДАЧ

Шматков С.И.
Харьковский национальный университет имени В.Н. Каразина
61077, Харьков, пл. Свободы 4, факультет компьютерных наук,
каф. теоретической и прикладной системотехники, тел. (057) 707-50-22,
E-mail: tps_kharkov@mail.ru

A model for high-level temporal fragmentation of cyclic tasks, providing the opportunity to optimize the structure of cycles running programs on the basis of accounting harmonization limits users to an available computational resource and time requirements for solving problems. A model for high-level temporal fragmentation of cyclic tasks, providing the opportunity to optimize the structure of cycles running programs on the basis of accounting harmonization limits users to an available computational resource and time requirements for solving problems.

1. Введение.

Высокоуровневую фрагментацию определим как процесс разделения задачи на фрагменты, в основу которого положена детализация до циклических участков Си – программы задачи. Следует отметить, что этот подход к декомпозиции задач рассматривался в целом ряде работ [1-5] и нашел широкое практическое применение в известных многопроцессорных ВС. Общим недостатком этих известных решений является отсутствие поддержки времяпараметризованной (временной) фрагментации задач[1,4,5].

2. Постановка задачи исследования.

Сформулируем общую постановку задачи высокоуровневой фрагментации циклических Си – программ следующим образом.

Исходные данные:

- Си - программа исходной циклической задачи;
- характеристики архитектуры и ресурса вычислительной сети [6];
- ограничения на доступный ресурс вычислительных узлов ($NU_{зад}$);
- метод параллельной обработки данных – совмещение независимых операций.

Примем, что характеристиками ресурса *RC* ВС являются:

- количество *NU (Number of computing Unit)* вычислительных узлов в составе вычислительной подсистемы РВС;
- топология связей коммуникационной подсистемы РВС;
- классы вычислительных узлов – персональные компьютеры (*PC*), многопроцессорные ВС с общей разделяемой памятью (*SMP, NUMA*), многопроцессорные *MPP* ВС с распределенной памятью и передачей данных между узлами в виде «сообщений»;
- ресурс процессоров узла – это количество *NM* процессоров в ВУ;
- типы *TYP* процессоров – суперскалярные процессоры и/или *VLIW* - процессоры с «длинным командным словом» (с числом $lk \geq 2$ одновременно выполняемых каждым процессором инструкций/функций, *lk* - «длина командного слова»);
- длительности t_j^0 выполнения операций/функций языка Си (в тактах);
- ограничения пользователей на количество $KV_{зад}$ виртуальных процессоров, доступных задаче.

Требуется:

Разработать модель высокоуровневой временной фрагментации циклических задач, обеспечивающую формальное разделение задач на временные макрофрагменты/ординарные фрагменты с учетом доступного количества процессоров $KV_{зад}$ РВС с оценкой времени выполнения.

3. Результаты исследования.

При ограничении доступного ресурса сети высокоуровневая временная фрагментация включает решение следующих задач:

- определения количества *ko* и состава ординарных циклов в исходной задаче;
- определения количества $ko_{зад}$ и состава ординарных циклов исходной задачи, которые могут выполняться одновременно (параллельно) на доступном/заданном количестве виртуальных процессоров $KV_{зад}$;
- определения количества *kmf* и формирования состава макрофрагментов, к одновременному выполнению которых должно сводиться решение исходной циклической задачи;
- расчета ожидаемого времени *T(Z)* решения задачи при учете заданного пользователем ограничения $KV_{зад}$ на количество виртуальных процессоров, доступных задаче.

```
#include <stdio.h>
void main(void)
{
   int  i,j;
   int  x[2][4];
   int  y[2][4];
   int  z[2][4];
        for(i=0;i<=1;i++)
         {
          for(j=0;j<=3;j++)
             {
               scanf("%d",&x[i][j]);
               scanf("%d",&y[i][j]);
             }
         }
        for(i=0;i<=1;i++)
          {
           for(j=0;j<=3;j++)
              {
                z[i][j] = x[i][j] + y[i][j];
                printf(" %3d ",z[i][j]);
              }
          }
}
```

Рис.1. Циклическая Си - программа с вложенными циклами

Поясним содержание перечисленных этапов макрофрагментации с помощью циклической задачи, исходный текст Си–программы которой показан на рис.1. Длительности выполнения операторов, принятые при синтезе временных параллельных моделей задачи, задает табл.1.

Таблица 1

Длительности t_i^0 выполнения операторов различных типов «*typ*»(такты)

typ	vx, vix	+,-, ++	=	*	%, /	&, *	l.o, a.o	bp, bpv	stop	con C_
t_i^0	1.00	1.00	2.00	10.00	35.00	1.00	1.00	1.00	1.00	1.00

Первым этапом высокоуровневой временной фрагментации является расчет минимально необходимого количества NU_{min} вычислительных узлов сети, содержащих заданное число $KV_{зад}$ виртуальных процессоров

$$NU_{min} = \left]KV_{зад}/(NM * lk)\right[.$$

Отметим, что в этом соотношении *NM* характеризует число виртуальных процессоров в одном узле сети, параметр *lk* задает количество одновременно выполняемых процессором команд. Значения *NM* и *lk* определяются конкретным классом ЭВМ вычислительного узла и типом процессоров архитектуры конкретных ВУ РВС.

Содержанием второго этапа является: оценка количества *kor* ординарных циклов в составе исходной циклической Си – программы

$$kor = \begin{cases} [i], \\ [i] * [j], \\ [i] * [j] * [k], \end{cases}$$

при работе с одномерными, двухмерными и трехмерными массивами соответственно количество *kof* ординарных фрагментов (в составе каждого из $kmf = NU_{min}$ макрофрагментов), к выполнению которых с использованием NU_{min} вычислительных узлов должно сводиться решение исходной свернутой циклической задачи, при заданном ограничении на число $KV_{зад}$ виртуальных процессоров равно *kof = ko / kmf.*

Количество *kor* ординарных циклов (*in*-циклов и *pr*-циклов) в исходной свернутой циклической Си – программе равно *kor =[i] * [j] =16.*

Содержанием третьего этапа является объединение каждой группы из *kof = 8* ординарных циклов FO_r, $r \in FO(Z) = \{1,2,...,16\}$ в соответствующие макрофрагменты MF_l, $l=1...$, NU_{min} для последующего «закрепления» каждого макрофрагмента MF_l за соответствующим виртуальным вычислительным узлом.

Для рассматриваемой задачи $NU_{min} = 2$, *NM =4.* Это означает, что ординарная СиО – программа - в интересах ее распределения на выделенное количество вычислительных узлов (каждый из которых имеет четыре процессора с длиной командного слова *lk = 1*) должна быть представлена в виде двух Си – программ, содержащих по два макрофрагмента (по четыре ординарных фрагментов в каждом макрофрагменте (рис.2).

```
Файл  Правка  Параметры  Справка
#include <stdio.h>
void main(void)
{
        int  i,j;
               int  x[2][4];
               int  y[2][4];
               int  z[2][4];

         for(i=0;i<=0;i++)
           { for(j=0;j<=3;j++)
             { scanf("%d",&x[i][j]);
               scanf("%d",&y[i][j]);
             }
           }
         for(i=0;i<=0;i++)
           { for(j=0;j<=3;j++)
             { z[i][j] = x[i][j] + y[i][j];
               printf(" %3d ",z[i][j]);
             }
           }
}
```

```
Файл  Правка  Параметры  Справка
#include <stdio.h>
void main(void)
{
        int  i,j;
               int  x[2][4];
               int  y[2][4];
               int  z[2][4];

         for(i=1;i<=1;i++)
           { for(j=0;j<=3;j++)
             { scanf("%d",&x[i][j]);
               scanf("%d",&y[i][j]);
             }
           }
         for(i=1;i<=1;i++)
           { for(j=0;j<=3;j++)
             { z[i][j] = x[i][j] + y[i][j];
               printf(" %3d ",z[i][j]);
             }
           }
}
```

Рис.2. Макрофрагментные Си – программы двух виртуальных вычислительных узлов РВС (*NU=2, NM=1, kl = 1*)

Задачей четвертого этапа является оценка процессорного времени $T_{PR}(Z)$ параллельного выполнения множества макрофрагментов MF_l , $l=1...$, NU_{min}, одновременно реализуемых с помощью NU_{min} виртуальных вычислительных узлов.

Решение этой задачи включает следующие шаги:

- синтез времяпараметризованной модели исходной циклической Си – программы с шириной параллельного процесса *H = lk*;

- оценка с помощью временной модели длительности *TO(H)* выполнения ординарного цикла (для рассматриваемой задачи *TO(H=1) = 43.00* тактов);
- расчет процессорного времени $T_{PR}(Z)$ параллельного выполнения множества макрофрагментов MF_l , $l=1…$, NU_{min}, одновременно реализуемых с помощью NU_{min} виртуальных вычислительных узлов с одновременным выполнением каждым процессором *lk* инструкций/функций

$$T_{PR}(Z) = (TO(H) * ko) / (NU_{min} * NM * lk).$$

Для значений $NU_{min} = 2$, *NM =4, lk = 1, TO(H=1) = 43.00,* $T_{PR}(Z) = 86.00$ (такты).

5. Выводы.

1. Особенностью известных подходов к фрагментации циклических задач является недостаточный учет требований пользователей к взаимному влиянию доступного вычислительного ресурса и времени решения задач.
2. Предложенный подход обеспечивает возможность оптимизации структуры циклов результирующей программы на основе согласования учета ограничений на доступный вычислительный ресурс и требований к времени решения задач.

6. Литература:

1. Воеводин В.В. Параллельные вычисления / В.В. Воеводин, Вл.В. Воеводин - СПб.: БХВ Петербург, 2002. – 608 с.
2. Лацис А. Как построить и использовать суперкомпьютер / А. Лацис – М.: Бестселлер, 2003. – 240 с.
3. Поляков Г.А. Адаптивные самоорганизующиеся системы с мультипараллельной обработкой данных - стратегия развития цифровой вычислительной техники в XXI–м веке / Г.А. Поляков // Прикладная радиоэлектроника, Том 1, №1, АН ПРЭ.- Харьков, 2002. С.57 –69.
4. Немнюгин С.А., Стесик О.Л. Параллельное программирование для многопроцессорных вычислительных систем. – СПб.: БХВ-Петербург, 2002. – 400 с.
5. Антонов А.С., Воеводин Вл. Эффективная адаптация последовательных программ для современных векторно-конвейерных и массивно-параллельных супер-ЭВМ // Программирование. – 1996. - № 4. – С. 37-51.
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2008. – 958 с.

ПРИНЦИПЫ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ ПО ТЕХНОЛОГИИ UA-ITT

Воробиенко П.П., Тихонов В.И., Голубова О.В.
Одесская национальная академия связи им. А.С.Попова
Ул. Кузнечная 1, г. Одесса, 65029, тел.7232244, onat@onat.edu.ua

This paper discusses the issues of computer network routing in respect to the Ukraine Integrated Telecommunication Technology (UA-ITT) developed by the authors. Six general principles of routing are proposed to minimize the routing time consumption.

Одной из проблем в теории и практике телекоммуникаций является повышение качества сервиса при передаче трафика реального времени по компьютерным сетям, и в частности уменьшение возможных временных задержек. Основными причинами задержек передачи информации в компьютерных сетях являются очереди и отказы обслуживания в моменты критических нагрузок, а также необходимость поиска в таблицах маршрутизации, размеры которых могут быть достаточно большими. Минимизация очередей достигается увеличением производительности сетевого оборудования, оптимальным выбором топологии сетей и другими методами трафик-инжиниринга. Для сокращения затрат на маршрутизацию IP-пакетов в транспортных телекоммуникационных сетях используются различные методы коммутации потоков, например, MPLS [1], Provider Backbone Bridge Traffic Engineering (PBB-TE) [2] и др.

Методы коммутации потоков сводят задачу маршрутизации в транзитных узлах к решению этой задачи только на входе и выходе соответствующего транспортного домена, за счет чего ускоряется продвижение IP-пакета внутри этого домена. Маршрут IP-пакета может пересекать несколько транспортных доменов, а доставка пакета от отправителя к получателю содержит участки маршрута, которые не покрываются доменами с коммутацией потоков. На этих участках задача маршрутизации IP-пакетов решается традиционными методами. Кроме того, добавление меток в MPLS (или дополнительных MAC-адресов в PBB-TE) усложняет многоуровневую схему инкапсуляции данных реального времени по протоколам стека TCP/IP, в результате чего доля служебной информации в канале связи может достигать 50÷80 % от общего цифрового потока [3].

Целью данного исследования является разработка принципов маршрутизации в компьютерных сетях, которые обеспечивают быструю коммутацию потоков и отдельных сообщений по всей протяженности маршрута от источника к получателю, и при этом значительно сокращают долю служебного трафика в общем цифровом потоке канала связи.

Для решения поставленной задачи авторами предложена концепция интегрированной технологии телекоммуникаций для сетей NGN (Ukraine Integrated Telecommunication Technology – UA-ITT) [4], в которой используется динамическая коммутация потоков без многоуровневой инкапсуляции данных, а также динамическая адресация объектов телекоммуникационной сети с иерархической структурой опорной сети [5]. Это позволяет просто вычислять т.н. *гарантированный маршрут* продвижения информации от источника к получателю, который однозначно определяется парой адресов источника и получателя.

Адрес терминального физического устройства в сети UA-ITT состоит из двух частей переменной длины: префикса Pr (структурированного адреса узла опорной сети, с которым связано терминальное устройство) и суффикса *Sf* (физического адреса терминального устройства в локальной сети соответствующего узла опорной сети). Префикс адреса состоит из отдельных октетов, каждый из которых имеет значение номера ветви иерархического дерева адресации. Например, для шестиуровневой системы адресации на рис.1 узлы «X», «C» и «D» имеют префиксы: $\mathrm{Pr}(X) = 1.1.2.1.2.2;\ \mathrm{Pr}(C) = 1.1.2.2.0.0;\ \mathrm{Pr}(D) = 1.1.3.0.0.0.$

Физическое устройство с локальным адресом 150 в локальной сети узла D, имеет сетевой адрес «*1.1.3.0.0.0-150*».Суффикс адреса состоит из одного или более октетов. Для идентификации различных цифровых потоков к адресу терминального устройства может быть добавлена третья часть – индекс *Id* , содержащий от 1 до 3 октетов. Индекс является аналогом 16-битового номера логического порта в протоколах TCP и UDP.

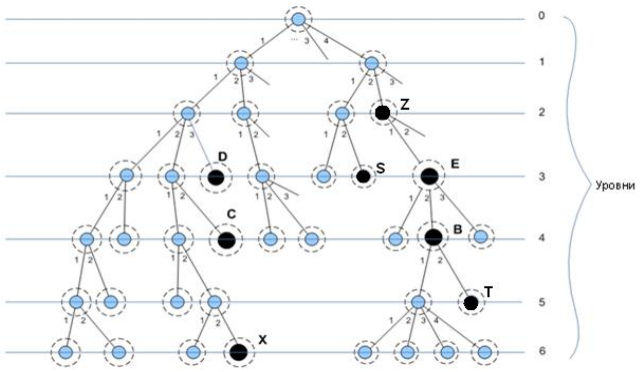


Рис. 1 – Шестиуровневая опорная сеть (логическая топология)

Древовидная иерархическая структура опорной сети соответствует логической топологии, которая определяет доменную структуру адреса. Физическая топология может отличаться от строгой иерархии дерева. Например, отдельные или даже все сегменты опорной сети могут иметь кольцевую физическую топологию. На рис.2 показан пример сети с кольцевой физической топологией, которая соответствует древовидной логической топологии на рис.1.

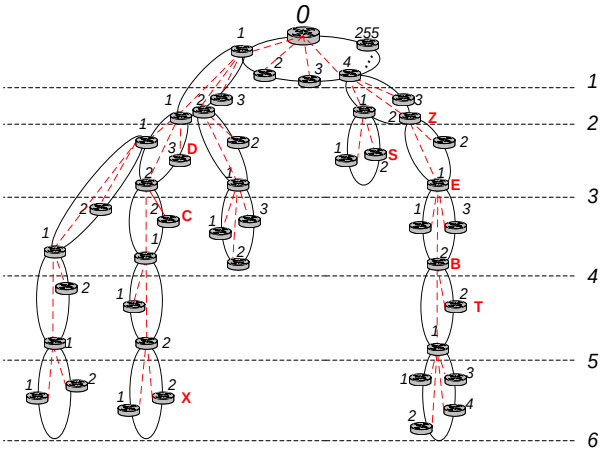


Рис. 2 –Шестиуровневая опорная сеть (физическая топология)

Помимо вертикальных связей между узлами опорной сети на каждом уровне иерархии возможны дополнительные горизонтальные связи. Если узел опорной сети имеет одну или более горизонтальных связей, то в задаче маршрутизации появляются несколько альтернатив для принятия решения о продвижении очередного сегмента данных на каждом шаге маршрутизации. В этом случае решается задача о выборе кратчайшего пути при заданной метрике сети. В качестве метрики абстрактного расстояния $d(A,B)$ между парой узлов A и B при передаче информации из A в B будем использовать взвешенную сумму двух физических величин (τ_1 и τ_2):

$$d(A,B) = \alpha \cdot \tau_1 + \beta \cdot \tau_2, \qquad (1)$$

где τ_1 – время распространения электромагнитного сигнала по линии связи между узлами A и B; τ_2 – ожидаемое время задержки передачи информации через транзитный узел B; α и β – весовые коэффициенты. Параметр τ_1 является достаточно стабильным для каждого сегмента лини связи, поскольку он зависит в основном от физической длины этой линии. Параметр τ_2 является в значительной мере случайной величиной, вероятностные характеристики которой могут изменяться во времени.

Точность решения данной оптимизационной задачи маршрутизации зависит от многих факторов, в т.ч. от того, какие и сколько горизонтальных связей опорной сети известны маршрутизатору в узле A, а также от вычислительной мощности процессора маршрутизации. Число различных возможных вариантов решения быстро растет с увеличением глубины расчета маршрута в окрестности узла маршрутизации. Например, если каждый узел опорной сети имеет m горизонтальных связей, то общее число альтернатив на каждом шаге маршрутизации равно $m+1$ (одно вертикальное направление по гарантированному маршруту опорной сети и m горизонтальных направлений). Пусть n − глубина расчета маршрута. Тогда общее количество вариантов равно m^n, т.е. имеет характер экспоненциального роста. Оптимизационные задачи такого рода относятся к классу NP-полных проблем, для которых, как правило, используются приближенные итерационные методы нахождения квази-оптимальных решений (например, метод случайного поиска).

Для того, чтобы итерационный метод оптимизации устойчиво работал при ограниченном (достаточно малом) времени решения задачи, необходимо обеспечить приемлемую точность начального приближения. В качестве начального приближения для квазиоптимального решения в UA-ITT используется гарантированный маршрут по линиям связи опорной сети. Критерием качества гарантированного маршрута является его абстрактная длина в метрике (1).

Исходя из сказанного выше, *первый принцип* маршрутизации по технологии UA-ITT заключается в следующем: для каждого узла опорной сети необходимо планировать трафик таким образом, чтобы в часы максимальной нагрузки обеспечить заданное допустимое время задержки при передаче информации по гарантированным маршрутам опорной сети. Этот принцип является достаточно общим и абстрактным, и требует конструктивной детализации в каждом конкретном случае.

Второй принцип маршрутизации по технологии UA-ITT предполагает способность маршрутизаторов к самообучению на основании статистического анализа проходящего через маршрутизатор трафика. Каждый маршрутизатор формирует ограниченное подмножество адресов назначения S_{DA}, которые наиболее часто встречаются в его транзитных потоках. Для подмножества S_{DA} на основании предшествующего опыта решения задачи маршрутизации формируется таблица маршрутизации с набором эвристических правил для каждого адреса S_{DA}, которые ускоряют процесс поиска кратчайшего пути в метрике (1) с учетом динамически изменяющегося во времени параметра τ_2.

Третий принцип маршрутизации – кэширование. При передаче больших файлов имеет место т.н. *пачечность*, т.е. появление на входе маршрутизатора сегмента с адресом назначения DA означает, что с достаточно большой вероятностью через небольшой промежуток времени снова появится сегмент с таким же адресом DA. Поэтому наряду с основной таблицей маршрутизации, каждый маршрутизатор поддерживает диамическую кэш-таблицу, в которой хранятся последние N адресов назначения и номера выходных шлюзов для продвижения сегментов данных по оптимальным (или квази-оптимальным) маршрутам. Параметр N зависит от производительности процессора маршрутизации и максимально допустимого времени сканирования кэш-таблицы.

Четвертый принцип − распараллеливание процессов маршрутизации. При поступлении заявки на обслуживание очередного сегмента цифрового потока, параллельно запускаются несколько различных алгоритмов (например, поиск кратчайшего пути по об-

щему методу согласно обозначенному выше первому принципу маршрутизации, сканирование основной таблицы маршрутизации и отыскание кратчайшего пути с помощью эвристических правил по второму принципу маршрутизации, сканирование динамической кэш-таблицы маршрутизации и др.). Параллельные алгоритмы работают по принципу состязания (кто первый найдет лучшее решение).

Пятый принцип маршрутизации − использование трех режимов передачи: без установления соединения, по установленному соединению; запрос на установление соединения. Для установления соединения используются двумерная шкала типов соединения (q_1, q_2): переменная q_1 определяет среднюю пропускную способность соединения, а q_2 − меру стабильности пропускной способности этого соединения. При передаче по установленному соединению управление цифровым потоком осуществляется по идентификаторам потоков (аналог меток в MPLS), а задача маршрутизации решается только на этапе установления соединения. Это значительно сокращает время на обработку информации в узле маршрутизации.

Шестой принцип маршрутизации направлен на сокращение времени установления соединения. Для этого каждый маршрутизатор, на основе статистического анализа трафика и принципа самообучения, заранее в фоновом режиме разрабатывает план распределения определенной части своего ресурса между различными потоками и адресами назначения. Этот план согласовывается со смежными маршрутизаторами, на основании чего составляется динамическая таблица зарезервированных виртуальных соединений для отдельных временных интервалов (например, на каждый из 24 часов в сутки). При поступлении заявки на установление соединения, имеющееся в наличии свободное соединение выделяется приложению без решения задачи маршрутизации. В противном случае для установления соединения оперативно решается задача маршрутизации по общим правилам.

Сформулированные выше принципы маршрутизации по технологии UA-ITT позволяют сократить временные задержки при передаче статистически мультиплексированных цифровых потоков по компьютерным сетям, а также уменьшить удельный вес служебной информации в общем цифровом потоке канала связи.

Литература:

1. Understanding MPLS-TP and Its Benefits. – Available: http://www.cisco.com/en/US/technologies/tk436/tk428/white_paper_c11-562013.pdf

2. Understanding PBB-TE for Carrier Ethernet. – Available: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/UnderstandingPBBTE.pdf

3. *Воробиенко П.П.* Формирование служебной информации в процессе сеанса связи сетевых компьютерных приложений / П.П. Воробиенко, М.И. Струкало, С.М. Струкало // 64-а науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів: матеріали конф. Ч.1 Інфокомунікації. – О.: ОНАЗ ім.. О.С.Попова, 1-4 грудня 2009. – С. 92-94.

4. *Воробиенко П.П., Тихонов В.И.* Основы интегрированной технологии телекоммуникаций UA-ITT // Інфокомунікації: проблеми та перспективи розвитку. Матеріали Міжнар. науково-практ. конф. (Одеса, 8-10 вер. 2010р.). – Одесса, 2010. – С.41-44.

5. Пат. 46477 Україна; МПК H04L 12/28. / Спосіб адаптивної адресації вузлів телекомунікаційних пакетних мереж / Воробієнко П.П., Тіхонов В.І. ; заявник та власник патенту Одеська нац. Академія зв'язку ім. О.С.Попова. – u 2009 06513; заявл. 22.06.2009; опубл. 25.12.2009. Бюл. № 24.

СИНХРОНІЗАЦІЯ ХАОСУ ЧЕРЕЗ КАНАЛ ЗВ'ЯЗКУ З ОБМЕЖЕНОЮ ПРОПУСКНОЮ ЗДАТНІСТЮ

Галюк С. Д.[1], Політанський Л. Ф.[2], Кушнір М. Я.[3]
Чернівецький національний університет ім. Ю. Федьковича
Кафедра радіотехніки та інформаційної безпеки
58000, Чернівці, вул. Сторожинецька 101, тел. +38(0372)24-24-36
E-mail: [1] galiuk@inbox.ru, [2] politanskyy@chnu.cv.ua, [3] kushnirnick@gmail.com

Synchronization of chaotic systems in the presence of filtering in the communication channel is investigated. The results of experiments using low-pass filter are presented. Generalized synchronization between chaotic Chua circuits in the presence of filtering the chaotic signal is shown.

Фільтрація сигналу, що передається по каналу зв'язку є одним із факторів, що погіршує якість передачі інформації в хаотичних системах зв'язку. Це унеможливлює встановлення синхронізації між передавачем і приймачем, оскільки за своєю природою хаотичні сигнали є широкосмуговими, а амплітудні та фазові спотворення сигналу при проходженні через канал зв'язку спотворюють вхідний сигнал приймача. На сьогодні відомі наступні методи боротьби з фільтрацією сигналів у каналі зв'язку: використання вузькосмугових хаотичних сигналів, використання на вході приймача коректуючих фільтрів з АЧХ оберненою до АЧХ каналу зв'язку, включення в кола хаотичного генератора приймача і передавача фільтруючих елементів з характеристиками еквівалентними характеристикам каналу зв'язку [1]. Перераховані методи при дії значних завад стають неефективними і не забезпечують задовільної синхронізації хаотичних систем.

Для передавання інформації серед багатьох способів хаотичної синхронізації найбільше уваги приділяється повній та узагальненій синхронізації. Відомо, що досягнення повної синхронізації хаотичних систем при наявності навіть слабкої фільтрації в каналі зв'язку неможливе [2, 3]. Тому використання таких способів хаотичної модуляції як хаотичне маскування, переключення хаотичних режимів та нелінійне підмішування є проблематичним при використанні каналів зі смугою пропускання меншою ніж спектр частот хаотичного сигналу. Проведені в останні роки дослідження показали, що найбільш перспективним способом синхронізації хаосу з точки зору використання в системах передавання інформації є узагальнена синхронізація [4]. Узагальнена синхронізація означає, що після закінчення перехідних процесів між станами двох зв'язаних систем існує деяка функціональна залежність $y = F(x)$, де x, y – вектори стану ведучої та веденої систем. Функція $F(x)$ може мати складний вигляд і бути навіть фрактальною. Узагальнена синхронізація в порівнянні з іншими видами хаотичної синхронізації володіє значною стійкістю до шумів.

Доповідь присвячена аналізу результатів експериментального дослідження явищ синхронізації хаотичних систем при передаванні сигналу через канал з обмеженою пропускною здатністю та питанню формування і використання вузькосмугових хаотичних сигналів для передавання інформації.

Розглянемо одну з найпростіших хаотичних систем - схему Чуа. Для виявлення режиму узагальненої синхронізації використаємо метод допоміжної системи. Експериментально досліджувана схема приведена на рис. 1. Параметри елементів схеми мають наступні значення: R_1 = 1587Ом, R_2 = 1582Ом, R_3 =1585Ом , L_1= L_2= L_3=20мГн C_{11}=11,3нФ, C_{12}=11нФ, C_{13}=11,5нФ, C_{21}=98,2нФ, C_{22}=98,4нФ, C_{23}=98,2нФ, C=98,9нФ, R=0..10кОм R_{e1}, R_{e2} =0...10кОм, *NR*1, *NR*2, *NR3* - діоди Чуа [1]. Після закінчення перехідних процесів узагальненій синхронізації відповідає синхронна поведінка веденої та допоміжної систем, та десинхронізація між ведучою і веденою системами в розумінні повної синхронізації.

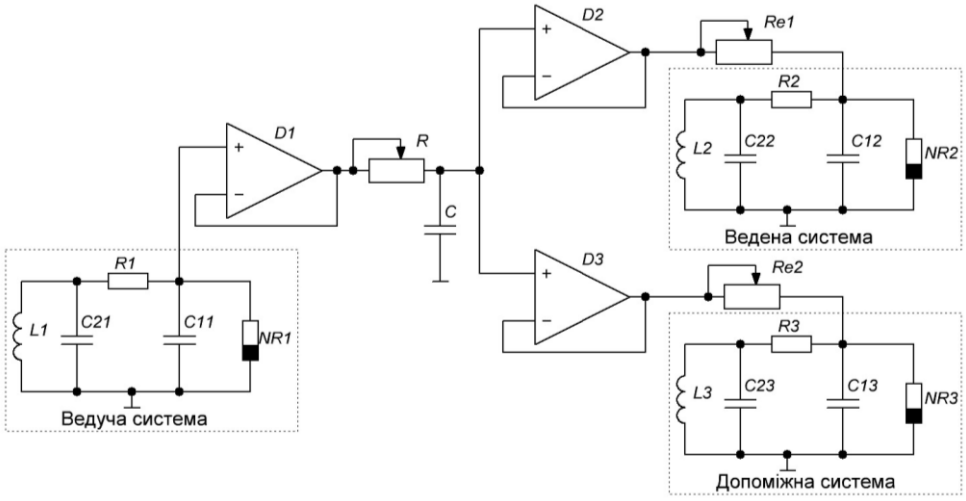


Рис. 1. Встановлення узагальненої синхронізації методом допоміжної системи

Нехай пропускна здатність каналу зв'язку має обмеження зверху по частоті. Промоделюємо такий канал за допомогою *RC*-фільтра нижніх частот. Математична модель системи в безрозмірному вигляді описується наступною системою рівнянь:

$$\begin{cases} \dot{x}_1 = \alpha_1\left(y_1 - x_1 - g(x_1)\right) \\ \dot{y}_1 = x_1 - y_1 + z_1 \\ \dot{z}_1 = -\beta_1 y_1 \\ \dot{v} = u\left(y_1 - v\right) \\ \dot{x}_{2,3} = \alpha_{2,3}\left(y_{2,3} - x_{2,3} - g(x_{2,3})\right) + e(v - y_{2,3}) \\ \dot{y}_{2,3} = x_{2,3} - y_{2,3} + z_{2,3} \\ \dot{z}_{2,3} = -\beta_{2,3} y_{2,3} \end{cases}$$

де x_i, y_i, z_i, i=1, 2, 3 – змінні стану системи, пропорційні відповідно напругам на конденсаторах C_{1i}, C_{2i} та струму через індуктивності L_i. Параметри системи: α_1 = 9,27, α_2 = 9,26, α_3 = 9, 28, β_1 = 12,84, β_2 = 12,85, β_3= 12,84, v – безрозмірний вихідний сигнал фільтра, u - безрозмірна частота зрізу *RC*-фільтра . Нелінійна характеристика генератора описується виразом:

$$g(x_i) = m_0 x_i + \frac{1}{2}(m_1 - m_0)\left[\left|x_i + 1\right| + \left|x_i - 1\right|\right]$$

де m_0 = -1,238; m_1 = -0,6665.

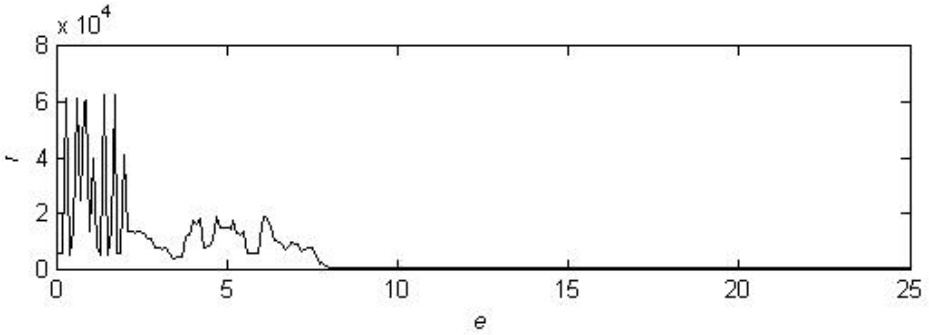


Рис. 2. Залежність помилки синхронізації r між веденою і допоміжною системами від коефіцієнта зв'язку e при u=0.2.

На рис. 2 приведено залежність помилки синхронізації r між веденою і допоміжною системами від коефіцієнта зв'язку для частот зрізу фільтра u=0.2. Видно, що при e> 7,9 помилка синхронізації різко зменшується до нуля, тобто ведена і допоміжна системи знаходяться в режимі узагальненої синхронізації.

Результати експериментального дослідження узагальненої синхронізації підтверджують дані моделювання. Хаотичний атрактор веденої системи (рис. 3*б*) при $R_{e1}=R_{e2}=2.9$кОм та $R=1.2$кОм відрізняється від оригінального хаотичного атрактора ведучої системи рис. 3*а*. З рис. 3*а-в* випливає, що повна синхронізація між ведучою і веденою системами відсутня. Водночас, залежність $U_{C22}(U_{C23})$ має вигляд прямої лінії (рис. 3*г*), що означає наявність узагальненої синхронізації між системами.

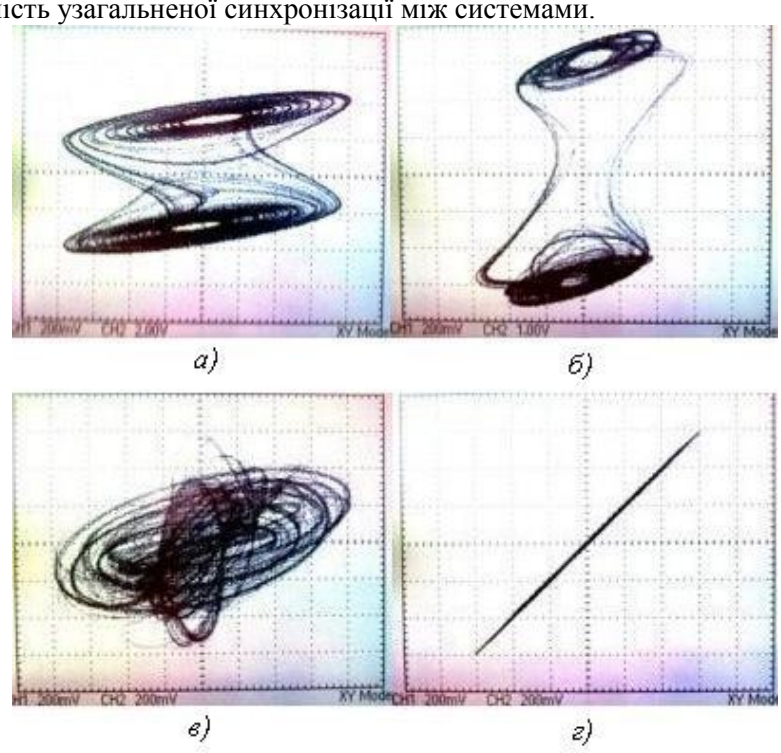


Рис. 3. Узагальнена синхронізація схем Чуа: *а*) хаотичний атрактор ведучої системи; *б*) хаотичний атрактор веденої системи; *в*) залежність $U_{C22}(U_{C21})$; *г*) залежність U_{C22} (U_{C23})

При експериментальних дослідженнях узагальнена синхронізація була досягнута при використанні фільтра високих частот, смугового та режекторного фільтрів зі смугами пропускання (затухання) в спектрі частот хаотичного сигналу.

Результати роботи свідчать про можливість використання вузькосмугових хаотичних сигналів для передавання інформації. При цьому вузькосмугові хаотичні сигнали формуються з широкосмугових за допомогою спеціальних фільтрів на виході хаотичного генератора передавача.

Література:

1. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А. С. Дмитриев, А. И. Панас. – М.: Издательство Физико–математической литературы. – 2002. – 252с.

2. Прохоров А.А. Синхронизация хаоса с учетом искажений сигнала в канале связи: Эксперимент и численное моделирование / А. А. Прохоров, Е. С. Мчедлова // Журнал технической физики. – 2008. – Т. 78. – Вып. 11. – ст. 77–84.

3. Галюк С.Д. Синхронізація хаотичних систем і фільтрація сигналів в каналі зв'язку / С.Д. Галюк, М.Я. Кушнір, Л.Ф. Політанський, Р.Л. Політанський // Східно-Європейський журнал передових технологій. – № 1/5(43). – 2010. – с. 20-24.

4. Короновский А. А. Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов / А. А. Короновский, О. И. Москаленко, А. Е. Храмов // Журнал технической физики. – 2010. – Т. 80. – Вып. 4. – ст. 1-8.

СИНХРОНІЗАЦІЯ ГІПЕРХАОТИЧНИХ СИСТЕМ ЛЮ ОБЕРНЕНИМ ЛІНІЙНИМ ЗВ'ЯЗКОМ

Іванюк П.В.[1], Політанський Л.Ф.[2], Політанський Р.Л.[3]
[1]Чернівецький національний університет ім. Юрія Федьковича
[2]Кафедра радіотехніки та інформаційної безпеки
58000, Чернівці, вул. Сторожинецька 101, +38(0372)24-24-36
E-mail: ivanyukpetro@ukr.net [1], politanskyy@chnu.cv.ua [2], polyr@mail.ru[3]

The possibility of synchronization driving and responsive Liu hyperchaotic systems by a linear feedback has been shown. The impact of power of linear feedback on extent of correlation of signals between driving and responsive Liu hyperchaotic systems has been investigated.

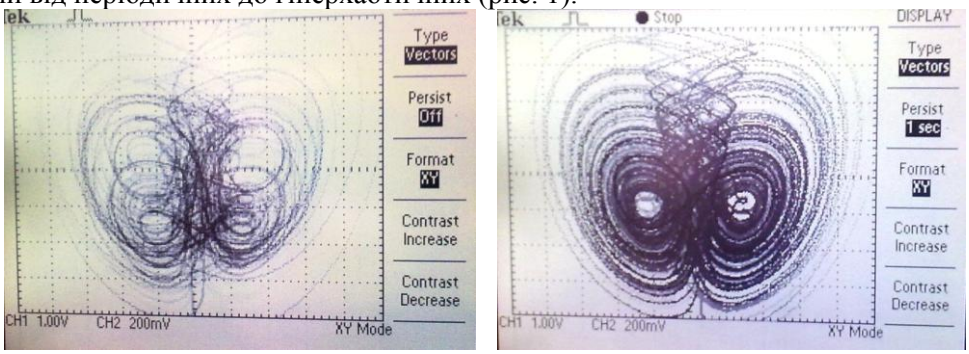
У зв'язку з використанням детермінованого хаосу в телекомунікаційних системах проблема синхронізації їх передавальної та приймальної частин набуває особливої актуальності. Існує ціла низка методів синхронізації хаотичних систем: повна, узагальнена, фазова, випереджаюча та ін. [1].

За останнє десятиліття розроблені нові моделі хаотичних атракторів шляхом модифікації системи Лоренца серед яких заслуговують увагу атрактор Чена (Chen's attractor) [2] та система Лю (Liu Systems) [3-4].

В доповіді приведені результати дослідження явища синхронізації двох ідентичних хаотичних систем Лю, синхронізованих між собою оберненим лінійним зв'язком. Досліджувана система описується чотирма диференціальними рівняннями першого порядку, що мають наступний вигляд [3]:

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= bx - hxz + \lambda w, \\ \dot{z} &= cx^2 - dz, \\ \dot{w} &= -ny. \end{aligned} \tag{1}$$

При проведенні досліджень були задані наступні значення параметрів системи a = 15, b = 30, h = 1, λ = 1, c = 4, d = 2.5. Зміною параметра n досягалися різні види коливань, починаючи від періодичних до гіперхаотичних (рис. 1).



а) *б*)

Рис. 1. Експериментально отримані фазові траєкторії системи (1), хаотичні (n = 42) та гіперхаотичні (n = 20) *а*) та *б*) відповідно.

Синхронізовані лінійним оберненим зв'язком ведучу та ведену системи Лю (рис. 2) можна описати наступними системами лінійних диференціальних рівнянь (2) та (3) відповідно

$$\begin{aligned} \dot{x}_1 &= a(y_1 - x_1), \\ \dot{y}_1 &= bx_1 - hx_1z_1 + \lambda w_1, \\ \dot{z}_1 &= cx_1^2 - dz_1, \\ \dot{w}_1 &= -ny_1. \end{aligned} \tag{2}$$

$$\begin{aligned}
\dot{x}_2 &= a(y_2 - x_2),\\
\dot{y}_2 &= bx_1 - hx_2 z_2 + \lambda w_2 + e(y_1 - y_2),\\
\dot{z}_2 &= c{x_1}^2 - dz_2,\\
\dot{w}_2 &= -ny_2
\end{aligned} \qquad (3)$$

де $y_1 - y_2$ похибка синхронізації між ведучою та веденою системами. Системи (2) та (3) синхронізовані між собою за допомогою лінійного зворотного зв'язку. Ведуча та ведена системи формують сигнали, що володіють хаотичною динамікою, $x_1(t)$, $y_1(t)$, $z_1(t)$, $w_1(t)$ та $x_2(t)$, $y_2(t)$, $z_2(t)$, $w_2(t)$ відповідно. Для прикладу, приведемо результати синхронізації між сигналами $y_1(t)$ та $y_2(t)$.

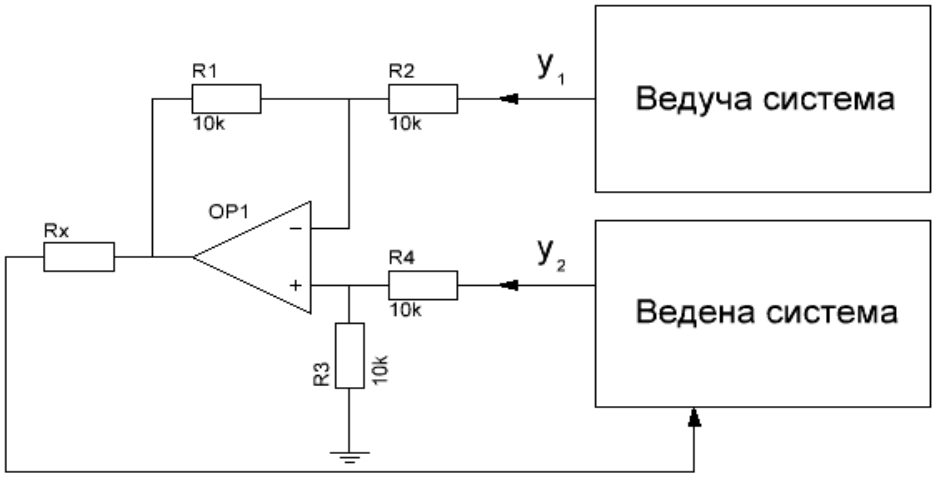
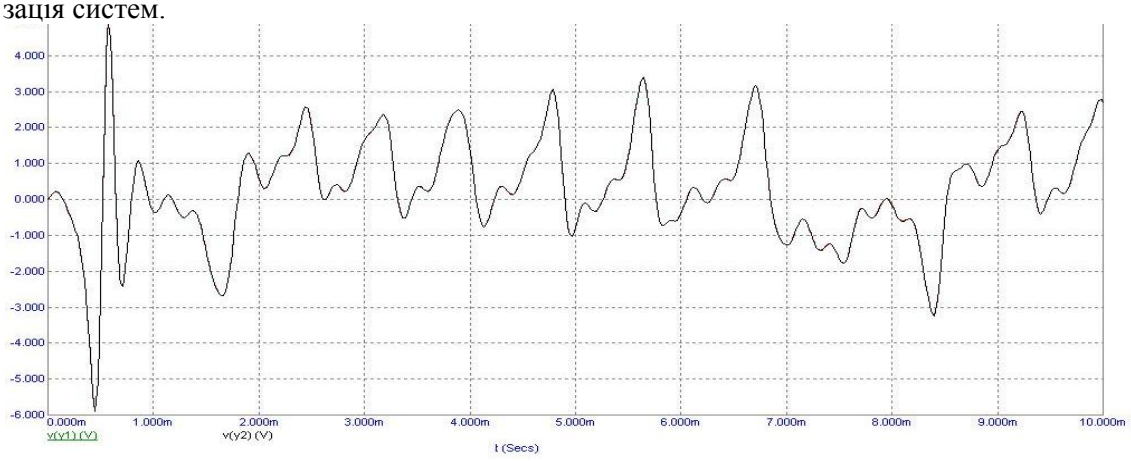
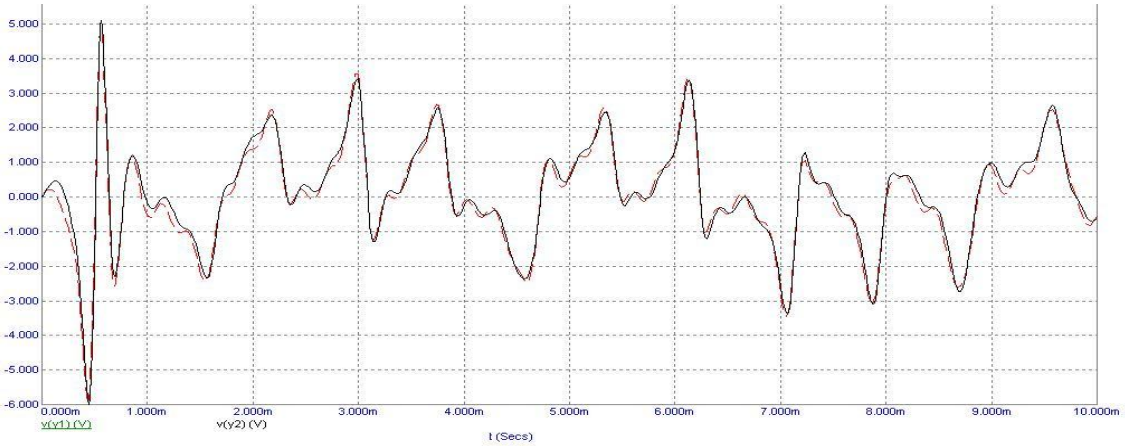


Рис. 2. Функціональна схема синхронізації двох хаотичних систем лінійним зворотнім зв'язком.

Глибину зв'язку між системами можна регулювати за допомогою зміни значення опору R_x. Для вивчення явища синхронізації між ведучою та веденою системою використовували програмне середовище Micro-cap 9 в якому проводилося моделювання даного процесу. Ступінь корелювання між сигналами $y_1(t)$ та $y_2(t)$, при різних значеннях R_x, встановлювалася шляхом порівняння часових діаграм (рис. 3). Як видно з рис. 3*а* часові діаграми $y_1(t)$ та $y_2(t)$ майже повністю накладаються одна на одну, що вказує на наявність синхронізації ведучої та веденої систем при R_x = 100 *Ом*. При значеннях R_x = 3 *кОм* часові діаграми сигналів $y_1(t)$ та $y_2(t)$ не співпадають (рис. 3*б*), чітко видно, що вони розходяться між собою. При подальшому збільшенні значення опору R_x має місце повна розсинхронізація систем.



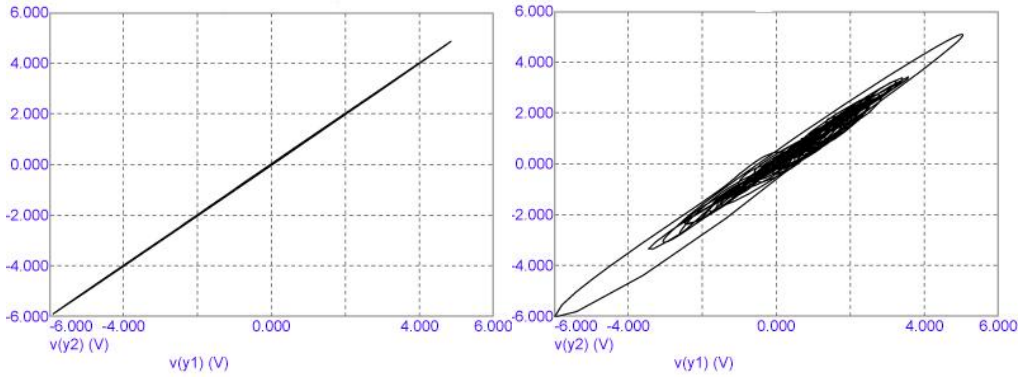
а)



б)

Рис. 3. Часові діаграми хаотичних сигналів $y_1(t)$ та $y_2(t)$ для досліджуваної системи при значеннях R_x = 100 *Ом* та R_x = 100 *Ом*, а) та б) відповідно.

На рис. 4 приведено залежності сигналу $y_2(t)$ веденої системи від $y_1(t)$ ведучої системи. Ця залежність є прямою лінією з кутом нахилу $\varphi = \frac{\pi}{4}$ при значенні R_x = 100 *Ом* (рис. 4*а*). Це вказує на ідентичність сигналів $y_1(t)$ та $y_2(t)$ ведучої та веденої систем. Із збільшенням R_x має місце розсинхронізації систем (рис. 4*б*).



а) *б*)

Рис. 4. Залежність $y_2 = f(y_1)$ для досліджуваної системи: при R_x = 100 *Ом* та R_x = 3 *кОм*, *а*) та *б*) відповідно.

Показана можливість синхронізації гіперхаотичних ведучої та веденої систем Лю за допомогою лінійного зворотного зв'язку.

Досліджений вплив глибини зворотного лінійного зв'язку на ступінь кореляції сигналів між ведучою та веденою гіперхаотичними системами Лю.

Література:

1. Короновский А. А., О применении хаотической синхронизации для скрытной передачи информации. / А. А. Короновский, О. И. Москаленко, А.Е. Храмов // Успехи физических наук. – 2009. – Т. 179 №12. – С. 1281–1310.

2. Jinhu Lu, The compound structure of a new chaotic attractor. / Jinhu Lu, Guanrong Chen, Suochun Zhang // Chaos, solitons and fractals. – 2002. – No. 14. – P. 669–672.

3. Wang Fa-Qiang, Hyperchaos evolved from the Liu chaotic system. / Wang Fa-Qiang, Liu Chong-Xin // Chinese Physics. 2006. – Vol. 15 No. 5. – P. 963–968.

4. Luo Xiao-Hua, Circuitry implementation of a novel four-dimensional nonautonomous hyperchaotic Liu system and its experimental studies on synchronization control / Luo Xiao-Hua at al. // Chinese Physics B. – 2009. Vol. 18 No. 6. – P. 2168–2175.

ПРОЕКТУВАННЯ МЕРЕЖІ АБОНЕНТСЬКОГО ШИРОКОСМУГОВОГО ДОСТУПУ

Барба І.Б., Орєшков В.І.
Одеська національна академія зв'язку ім.. О.С. Попова
65029, Одеса, вул. Ковальська 1, кафедра Телекомунікаційних систем, тел.:(048)720-77-53
E-mail: irina_barba@mail.ru

The broadband access design procedure on the base of the domestic producer's single-site network multi-pair telephone cable is described taking into account the parallel operation of transmission systems for the purpose of the carrier capacity increase.

Для забезпечення високошвидкісного доступу користувачів до Internet використовуються цифрові абонентські лінії (ЦАЛ) (DSL - Digital Subscriber Line), які забезпечують абонентський доступ зі швидкістю від сотень кбіт - до сотень Мбіт в секунду. Серед технологій широкосмугового доступу(ШД) найбільш популярними являються xDSL – технології (Рекомендації ITU G-992. G-993) [1,2]. Сьогодні у світі найбільше число ЦАЛ - більше 60 відсотків будується на базі телефонних ліній з використанням даної технології, яка була розроблена спеціально для передачі інформації по існуючих мідних кабелях місцевої телефонної мережі зв'язку.

Телефонні кабелі розроблялися для передачі низькочастотних розмовних сигналів і їх характеристики нормовані лише в низькочастотній області, через ненормованність симетрії пар, кабелі чутливі до електромагнітних полів і завад від кіл електроживлення, електропостачання та заземлення. У зв'язку з невисокими перехідними згасаннями між парами в багатопарних телефонних кабелях основним фактором, що визначає такі характеристики ЦАЛ, як довжину АЛ або досяжну швидкість передачі, є перехідні завади від паралельно працюючих в одному кабелі ЦАЛ, а також від інших систем передачі, які застосовуються на вітчизняній абонентській мережі.

Побудова цифрової мережі високошвидкісного абонентського доступу висуває ряд завдань перед розробниками обладнання зв'язку, проектувальниками мереж доступу та експлуатацією ЦАЛ, вирішення яких є необхідною умовою ефективного розвитку мережі доступу. Серед найважливіших завдань є розробка методик проектування ЦАЛ з урахуванням характеристик телефонних кабелів та електромагнітної сумісності різних типів систем передачі, що працюють в одному кабелі. У доповіді приводиться методика програмного забезпечення проектування ЦАЛ абонентського доступу з урахуванням характеристик вітчизняних абонентських багатопарних кабелів. Проектуванню підлягають електричні характеристики xDSL- ліній, довжини та типи кабелів на розподільній та магістральній ділянках (рис.1).

При проектуванні мережі xDSL-доступу по багатопарних телефонних кабелях з металевими жилами виникають задачі двох основних класів. До першого класу відносяться задачі проектування мережі xDSL-доступу з використанням АЛ вже існуючої телефонної мережі з визначеними параметрами і характеристиками, діючими на мережі різноманітними системами передавання (xDSL-лініями, системами охоронної, протипожежної сигналізації, модемами, системами цифрового ущільнення і т.д.). Типова структура АЛ телефонної мережі показана на рис.1.

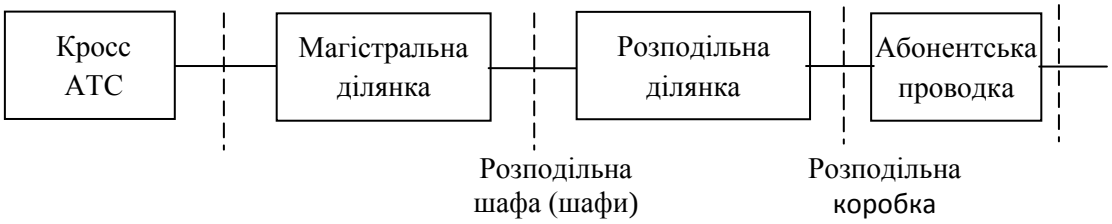


Рис. 1 – Типова структура АЛ телефонної мережі

До другого класу відносяться задачі проектування мережі xDSL-доступу одночасно з проектуванням традиційної телефонної мережі – нове будівництво, розвиток існуючої телефонної мережі.

В обох класах можливі різні постановки задач.

Найбільш розповсюдженими (актуальними) задачами першого класу є наступні.

Задача 1.1 Задані параметри існуючої телефонної мережі, існуючої мережі xDSL-доступу (якщо вона є), побудованої на базі цієї телефонної мережі, і вимоги до проектованої (планованої) мережі xDSL-доступу. Треба визначити, чи можливо реалізувати плановану мережу xDSL-доступу.

Задача 1.2 Виникає у випадку неможливості вирішити у повному обсязі задачу 1.1. У цьому випадку можливі такі варіанти проектування: зниження бажаних швидкостей передавання по xDSL- лініях, зменшення кількості планованих xDSL- ліній, прокладання кабелю з підвищеним перехідним згасанням на найбільш критичних (до перехідних завад) ділянках кабельної мережі. Таким чином, задача полягає у визначенні, скільки і які саме xDSL- лінії із заданими швидкостями передавання можна організувати або які максимальні швидкості передавання можуть бути забезпечені кожною xDSL- лінією із заданої сукупності xDSL-ліній. При цьому нові xDSL- лінії не повинні порушувати працездатність вже працюючих xDSL-ліній.

Серед задач другого класу можливі два види задач: по-перше, це розвиток існуючої телефонної мережі шляхом прокладання нових кабелів від діючої комутаційної станції (КС) до абонентів (задача 2.1), по-друге, це будівництво нової телефонної мережі, включаючи телефонні станції, підстанції, виносні абонентські модулі та кабелі (задача 2.2).

Задача 2.1 Задані характеристики проектованої телефонної мережі та мережі xDSL- доступу: проектована кількість телефонів, xDSL- ліній з відповідними швидкостями передавання, кількість розподільних коробок (РК), відстані від існуючої КС до груп компактно розташованих абонентів (ГКРА). Необхідно визначити довжини і типи кабелів на магістральних і розподільних ділянках проектованої мережі.

Задача 2.2 Задані характеристики проектованої телефонної мережі та мережі xDSL- доступу: проектована кількість телефонів, xDSL- ліній з відповідними швидкостями передавання, кількість розподільних коробок (РК), місця розташування груп компактно розташованих абонентів (ГКРА). Необхідно визначити місця розташування планованих КС, підстанцій і т.д., а також довжини і типи кабелів на магістральних і розподільних ділянках проектованої мережі.

Можливі також інші постановки задач другого класу, які можуть розглядатися як варіанти задач 2.1 або 2.2, наприклад, такі:

а) при заданому відсотку пар кабелів, завантажених xDSL-лініями із заданими однаковими швидкостями передавання, визначити довжини і типи кабелів на магістральних і розподільних ділянках проектованої мережі (варіант задачі 2.1);

б) при заданому відсотку пар кабелів, завантажених xDSL-лініями із заданими однаковими швидкостями передавання, визначити місця розташування планованих КС, підстанцій і т.д., а також довжини і типи кабелів на магістральних і розподільних ділянках проектованої мережі (варіант задачі 2.2).

Проектування здійснюється з використанням спеціалізованого програмного забезпечення (ПЗ), призначеного для проектування мережі абонентського широкосмугового доступу (xDSL- доступу) на ділянці від мультиплексора доступу DSLAM до абонентських xDSL-модемів, що являє собою сукупність xDSL- ліній, на основі технологій доступу ADSL (асиметрична цифрова абонентська лінія) по багатопарних телефонних кабелях місцевої телефонної мережі[3].

ПЗ має наступні можливості:

а) щодо задавання вихідних даних для проектування:

- використання візуального механізму побудови структури мережі xDSL-доступу;
- задавання довжин ліній, з'єднуючих елементи мережі xDSL-доступу;
- задавання параметрів кабелів;

- задавання розташування та типу систем передавання (СП) абонентів;

- задавання взаємного розташування пар, використовуваних системами передавання, у кабелях ділянок мережі xDSL-доступу;

- задавання необхідних швидкостей передавання інформації для кожної СП.

б) щодо результатів проектування:

- визначення швидкостей передавання, на яких можлива робота кожної заданої СП;

- визначення максимальної довжини ділянки мережі xDSL-доступу, за якої забезпечується робота СП із заданими необхідними швидкостями передавання;

- визначення типу кабелю з мінімальним числом пар, при використанні якого на обраній ділянці забезпечується робота СП із заданими необхідними швидкостями передавання;

- визначення оптимального (за критерієм мінімізації перехідних завад між парами, використовуваними для передавання сигналів xDSL) взаємного розташування пар, використовуваних системами передавання, в кабелях ділянок мережі xDSL-доступу;

- визначення типу кабелю з мінімальною ціною, при використанні якого на обраній ділянці забезпечується робота СП із заданими необхідними швидкостями передавання.

в) щодо створення звітів:

- створення звіту про швидкості передавання СП в одній групі компактно розташованих абонентів (ГКРА);

- створення комплексних звітів про стан мережі для двох типів задач проектування.

Крім того, програма дозволяє відкоригувати загрузку кабелю (*Сценарий загрузки кабеля),* і якщо потрібно перемістити СП в іншу пару кабелю для збільшення пропускної спроможності лінії передачі.

Сегмент ШД в Україні стрімко розвивається. За даними українського офісу iKS-Consulting[4], в Україні на 30 вересня 2010 року загальна кількість абонентів широкосмугового доступу склала близько 3,35 мільйона, з яких 2,87 мільйона - домашні користувачі (по даним вікіпедії на 31 березня 2011 року - 3,93 млн.- кількість абонентів, з яких 3,4 – домашні користувачі). Переважно це абоненти телефонної мережі, доступ за якою залишається найбільш економічно перспективним. Запропонована методика проектування є зручним інструментом для вирішення завдань розвитку та модернізації телефонної мережі на базі сучасних технологій.

Література:

1. Recommendation ITU-T G.992.1. Asymmetrical Digital Subscriber Line (ADSL) Transceiver. Geneva, 12-23 October, 1998.

2. Recommendation ITU-T G.993.1. Very-high-speed Digital Subscriber Line Foundation. August 2001.

3. В.А.Балашов Технологии широкополосного доступа xDSL/ Инженерно – технический справочник/ Под общей редакцией В.А. Балашова. – М.: Эко-Трендз, 2009.- 256с.:ил.

4. http://www.iks-consulting.ru/

МЕТОДИКА ТЕНЗОРНОГО ОБОБЩЕНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Евсеева О.Ю.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: evseeva.o.yu@gmail.com

In the paper by summarizing the known results technique of implementation of tensor approach for solving network problems is offered. The general methodology of synthesis of the tensor model of the telecommunications system is described.

На сегодняшний день в литературе представлен достаточно широкий спектр математических моделей телекоммуникационных систем (ТКС), обладающих разной степенью общности и нацеленных на решение различных телекоммуникационных задач. При этом используются результаты, полученные в рамках теории графов и комбинаторики, теории массового обслуживания, теории игр, нейронных сетей, сетей Петри, аппарата производящих функций, марковских управляемых случайных процессов, тензорного анализа сетей и ряда других. Среди наиболее результативных в плане решения задачи управления трафиком в мультисервисных ТКС с гарантированным качеством обслуживания следует отметить тензорные модели, полученные путем обобщения векторно-матричных представлений и перехода к тензорным операторам, что способствует выявлению скрытых ранее закономерностей, а в целом обеспечивает повышение системности и адекватности описания.

Тензорный подход к исследованию систем различной природы представляет собой конкретизацию более общего категориального подхода и основывается на идеях, заложенных американским ученым-электроинженером Г. Кроном в рамках разработанного им аппарата тензорного анализа сетей (ТАС) [1]. Г. Крон, основываясь на понятиях и положениях тензорного исчисления и анализа, одновременно обобщает их и развивает для использования в анизотропном (дискретном) пространстве-структуре. В рамках ТАС сетевая структура выступает в качестве основы как при геометризации моделируемой системы, так и при дальнейшем тензорном обобщении ее функциональных уравнений поведения. В рамках теории телекоммуникационных систем тензорный подход, преломляющий и развивающий идеи тензорного анализа сетей Г.Крона к решению задач телекоммуникаций, получил развитие благодаря работам Пасечникова И.И. [2], Петрова М.Н, Веревкиной Е.В. [3], Поповского В.В., Лемешко А.В. [4], Стрелковской И.В., Григорьевой Т.И. [5].

Применительно к телекоммуникациям возможность совместного исследования структуры ТКС и процессов, которые протекают в ней, представляется главным преимуществом тензорной методологии исследований, основанной на объединении возможностей дифференциальной геометрии с возможностями комбинаторной топологии. То есть при анализе (синтезе) системы совместно с функциональными уравнениями поведения ТКС может использоваться также и ее топологическое описание, представленное одно- и многомерными симплициальными моделями, которое представляет дополнительный источник информации для эффективного составления и решения этих уравнений [1].

В зависимости от того, какая скалярная или векторно-матричная модель элемента телекоммуникационной сети получила тензорное обобщение, в рамках тензорного моделирования ТКС можно выделить три направления. Первые два базируются на тензорном обобщении известных в теории массового обслуживания формул: формулы Литтла в рамках первого направления и формулы $\lambda=\mu\rho$ в рамках второго. При этом обоим направлениям свойственны серьезные недостатки. В первую очередь, это узкая область их применения. В рамках этих подходов не учитывается разнородность сетевого трафика, особенности в обслуживании каждого отдельного типа трафика и тем более его многопродуктовость, что снижает ценность подобных описаний. Использование формулы Литтла позволяет работать только с одним показателем качества обслуживания – средней за-

держкой передачи, и не позволяет оперировать другими – вероятностью потерь пакетов (или своевременной их доставки) и джиттером. В то же время в рамках второго направления вообще отсутствуют в явном виде показатели QoS.

В таком свете наиболее перспективным видится третье направление, основы которого заложены в работах авторов [4]. В рамках этого направления тензорному обобщению может подлежать любая представленная в аналитическом виде модель элемента ТКС, которая связывает необходимые в ходе исследования ТКС показатели качества обслуживания с характеристиками сети и передаваемого трафика. В целом данный подход, во-первых, обеспечивает возможность непосредственного оперирования показателями сетевого QoS, причем могут быть охвачены все группы QoS-показателей: скоростные, временные и вероятностные; во-вторых, учитывает, в отличие от выше изложенных подходов, потоковый характер сетевого трафика; в-третьих, допускает моделирование ТКС не только однопродуктовыми двухполюсными сетями, но и многопродуктовыми многополюсными сетями; в-четвертых, допускает учет типа сетевого трафика и особенностей его обслуживания (через компоненты метрических тензоров); в-пятых, что свойственно всем тензорным моделям, обеспечивает единство структурного и функционального описания ТКС.

Основные положения тензорного подхода к моделированию ТКС

В целом на основании обобщения и развития известных результатов можно предложить следующую, представленную в общем виде методику применения тензорного подхода при решении сетевых задач.

I. Этап тензорного описания ТКС.

1. Анализ поставленной прикладной задачи. Подбор математических моделей элементов системы, согласующихся с целью проводимых исследований и подлежащих дальнейшему тензорному обобщению.

2. Геометризация системы: введение понятий пространства, систем координат и обоснование их размерности; определение правил ко- и контравариантного координатного преобразования.

3. Тензорное обобщение математической модели системы. Обоснование тензорного характера основных сетевых параметров, определение инвариантов, ковариантных и контравариантных величин. Уточнение метрических свойств введенного пространства на основании принятой модели трафика и ее обслуживания.

II. Этап тензорного расчета ТКС.

Далее возможно два основных сценария, связанных с непосредственным решением поставленной задачи прикладного характера в рамках тензорного описания ТКС.

Первый сценарий. 1. Поиск системы координат (СК), в которой решение поставленной задачи возможно с наименьшими затратами описательного и вычислительного характера. Такая система координат, как правило, носит название «примитивной» [1].

2. Если такая «примитивная» СК существует, то необходимо осуществить прямое координатное преобразование сетевых параметров, имеющих тензорный характер, из СК исходных данных в «примитивную» СК. В результате модель ТКС уже будет представлена в матричной форме, основываясь на проекциях образующих ее тензоров в «примитивной» СК.

3. Непосредственное решение с использованием традиционных методов науки поставленной телекоммуникационной задачи в рамках математической модели ТКС, отнесенной к «примитивной» СК.

4. Интерпретация полученных результатов решения в исходной системе координат. В результате интерпретации осуществляется обратное координатное преобразование рассчитанных сетевых параметров из «примитивной» системы координат в систему координат исходных данных.

Подобный подход является «классическим» при использовании методологии Г. Крона к анализу и синтезу сложных систем различной физической природы. С усложнением самой постановки задачи, основанной, например, на учете большего числа условий и ограничений на параметры модели, более предпочтительным выглядит ***второй сценарий*** использования тензорного подхода в ТКС. Второй сценарий предполагает использование множества систем координат, в рамках которых возможно осуществить расчет искомых параметров ТКС. То есть в отличие от первого сценария не отдается предпочтение единственной, т.н. «примитивной» СК, а в процесс формализации вовлекается большее число СК, в каждой из которых проекции ранее введенных тензоров представляют собой либо исходные данные, либо прогнозируемые результаты расчетов. В этом случае тензорное описание ТКС, обладая максимальной целостностью, позволяет восстановить общую картину по частям, обобщая и взаимодополняя имеющуюся информацию об известных координатах искомых тензоров в различных координатных системах. В дальнейшем данный сценарий (как и выше описанный «классический») основывается на использовании правил координатного преобразования и получении инвариантных условий, связывающих известные и искомые сетевые параметры как проекции моделирующих тензоров в базовых системах координат.

Методика тензорного обобщения функциональной модели ТКС

Основу построения тензорных моделей систем телекоммуникаций, а также систем другой физической природы составляют впервые сформулированные Г. Кроном [1] обобщающие постулаты. Фактически, эти постулаты отражают иерархию способов описания сложных систем и являются своеобразными ступенями, ведущими в конечном итоге к тензорным моделям. В соответствии с обобщающими постулатами можно предложить следующую методику синтеза тензорной модели ТКС (рис. 1).

Этап 1. Для элемента сети, будь-то отдельный тракт передачи или некоторая их совокупность (путь, контур, разрез), записывается алгебраическое уравнение, отражающее его функциональные свойства. Для одного и того же элемента в общем случае в зависимости от выбранного аспекта описания может быть записано несколько уравнений, каждое из которых может быть положено в основу тензорной модели. Количество таких уравнений и, как следствие, синтезированных на их основе тензорных моделей определяется лишь требованиями решаемой прикладной задачи. Согласно предварительному постулату обобщения Г. Крона, функциональное уравнение для элемента должно быть записано таким образом, чтобы сохраняло свою справедливость для большого их числа.

Этап 2. Объединение алгебраических уравнений, записанных для отдельных элементов сети, и представление их совокупности единым векторно-матричным уравнением. Возможно, потребуется предварительная перекомпоновка уравнений отдельных элементов с целью приведения их всех к единой форме.

Этап 3. Трактовка полученного векторно-матричного уравнения как проекции инвариантного тензорного уравнения в системе координат, где базисными являются элементы, для которых на первом этапе записывались уравнения поведения. Это позволяет записать и само тензорное уравнение моделируемой системы, переход к которому должен сопровождаться проверкой тензорной природы всех геометрических объектов, установлением характера (ко-, контра- или инвариантности) и валентности всех входящих в него тензоров – моделей системы.

Этап 4. Формализация правил координатного преобразования для проекций тензоров при переходах между различными системами координат, представляющими интерес с точки зрения прикладной задачи. Данный этап первоначально предполагает выбор таких систем координат, что должно быть основано на анализе исходных данных и искомых величин, и сопровождаться составлением для них матриц ко- и контравариантного координатного преобразования.

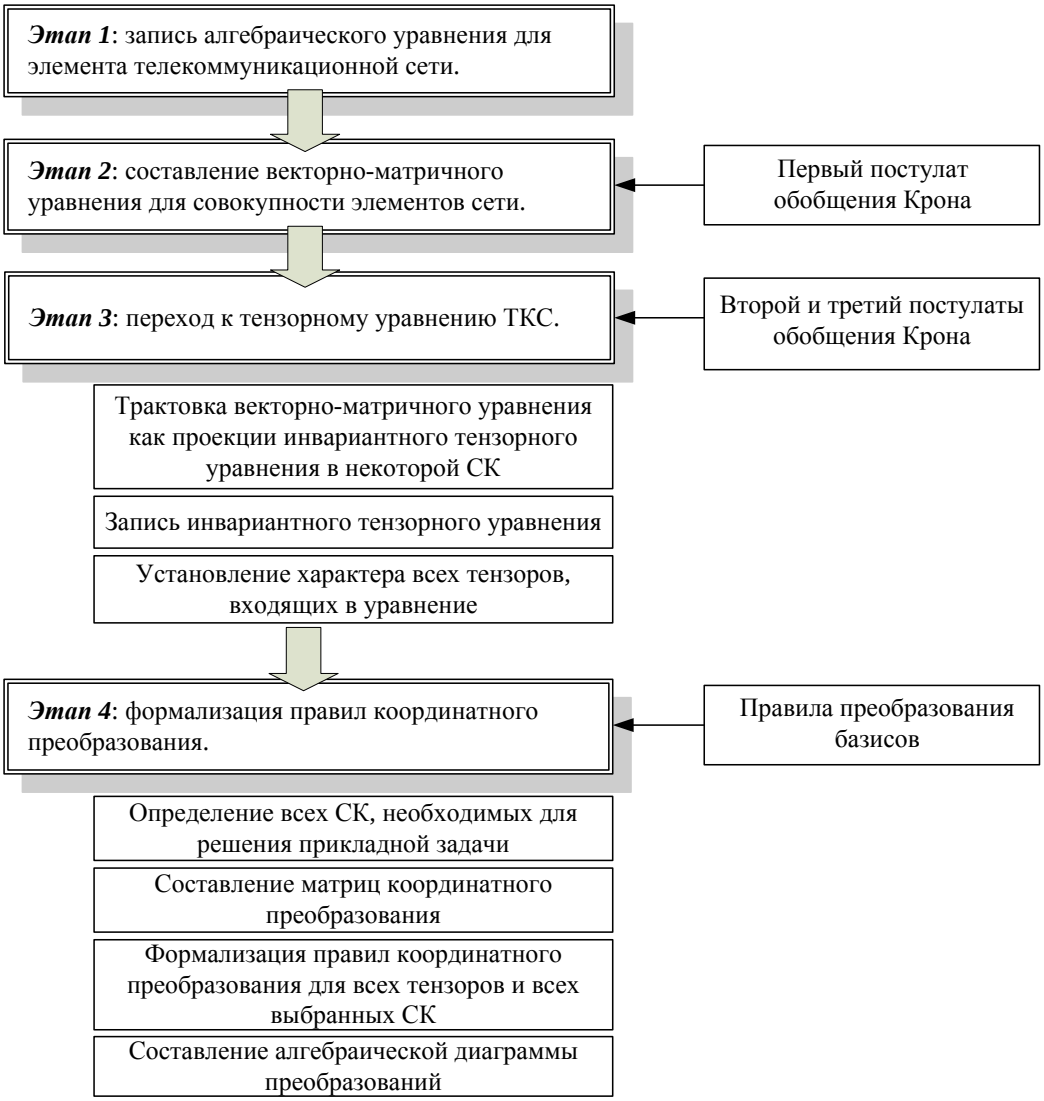


Рис. 1. Основные этапы синтеза тензорной модели ТКС

Теперь на основании тензорной модели, зная правила координатного преобразования и трактуя все известные и искомые величины как проекции (или отдельные координаты проекций) в некоторых, зачастую разных СК, существует возможность выявить их взаимосвязь между собой и тем самым решить поставленную прикладную телекоммуникационную задачу, например, оценки качества обслуживания, достигаемого при заданном распределении трафика по трактам передачи, или, наоборот, поиска порядка управления трафика, обеспечивающего заданные показатели его качества обслуживания.

Литература: 1. *Крон Г.* Тензорный анализ сетей. – М.: Сов. радио, 1978. – 720 с. 2. *Пасечников И.И.* Методология анализа и синтеза предельно нагруженных информационных сетей. – М.: Изд-во «Машиностроение-1», 2004. – 216 с. 3. *Веревкина Е.В., Захарченко М.О., Петров М.Н.* Тензорная методология в информационных сетях. – Красноярск: НИИ СУВТП, 2001. – 158 с. 4. *Поповский В.В., Лемешко А.В.* Тензорный анализ в задачах системного исследования телекоммуникационных систем // Радиотехника. Всеукр. межведомств. науч.-техн. сб. – 2002. – Вып. 125. – С. 156 – 164. 5. *Стрелковская И.В., Григорьева Т.И.* Применение теории моделей и тензорного анализа при моделировании телекоммуникационных систем // Радиотехника: Всеукр. межведомств. науч.-техн. сб. – 2007. – Вып. 148. – С. 102 – 106.

МЕТОД ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ДОСТАВКИ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ С КОММУТАЦИЕЙ ПАКЕТОВ

Польщиков К.А., Рвачева Н.В.
Полтавский национальный технический университет имени Юрия Кондратюка
36007, Полтава, пр. Первомайский 24, каф. компьютерной инженерии,
тел. (0532) 7-55-1, E-mail: rvacheva_n@mail.ru

Proposed by method of choice intersegment interval in the transport protocol of the telecommunications network, which involves determine of the current value of interval between sent to adjacent segments as an output parameter of fuzzy inference. According to the results of research using this method reduces the average time data delivery, reduce the number of retransmissions of data packets and more efficient use of available throughput telecommunications network..

Введение

Наблюдаемый в последние годы стремительный рост объемов информации, передаваемой в телекоммуникационных сетях с коммутацией пакетов, приводит к дефициту сетевых ресурсов, доступных для трафика данных. Анализ требований, предъявляемых к доставке данных в современных сетях, показал, что при передаче этого вида трафика необходимо обеспечить не только безошибочность, но и достаточно высокую оперативность доставки информационных сообщений. На сегодняшний день, скорость наращивания пропускной способности телекоммуникационных сетей меньше, чем скорость роста объемов информации, передаваемой в них, это приводит к возникновению задержек при передаче трафика и нарушению требований по своевременности доставки данных [1].

Целью исследований является повышение оперативности доставки данных в телекоммуникационной сети с коммутацией пакетов.

Основная часть

Для повышения качественных параметров передачи данных применяются дополнительные методы управления интенсивностью отправки данных источником, которые позволяют избежать перегрузок и потерь пакетов при максимальном использовании доступной для трафика данных пропускной способности сети.

Как правило, указанные методы управления интенсивностью отправки данных источником реализуются в протоколах транспортного уровня модели взаимодействия открытых систем. Наибольшее распространение в сетях с коммутацией пакетов получил транспортный протокол TCP и его модификации, например: TCP Reno, TCP Tahoe, TCP Vegas, BICTCP, Fast TCP, ARTCP. Однако, практически все модификации протокола TCP имеют ряд общих недостатков, таких как [2]:

- не согласованность между интенсивностью отправки данных источником и доступной пропускной способностью сети;
- интерпретация потери пакета как признака перегрузки;
- аналитические выражения для обоснования интенсивности отправки данных подобраны экспериментально.

Таким образом, ограниченность сетевых ресурсов, несовершенство существующих методов управления интенсивностью отправки данных источником, увеличение объема передаваемых данных, отсутствие достоверной информации о текущем состоянии сети приводят к необходимости создания нового метода выбора интенсивности отправки данных источником.

Управление интенсивностью отправки данных на передающем конце можно эффективно осуществить, зная точное значение доступной в данный момент времени пропускной способности сети. Получить такую информацию вовремя невозможно. Одним из научных направлений, позволяющих эффективно решать задачи управления в условиях отсутствия прямой достоверной информации об объекте управления, является применение интеллектуальных нечетких систем (систем нечеткого вывода).

Предложенный в докладе метод предполагает определение текущего значения межсегментного интервала как выходного параметра системы нечеткого вывода. Особенности построения такой системы во многом определяются составом ее входных сигналов, на основе анализа которых осуществляется расчет текущего значения выходной переменной. Результаты многочисленных имитационных экспериментов показали, что наиболее информативными параметрами, позволяющими определить текущее состояние телекоммуникационной сети, являются: предыдущее и текущее значения величины скользящего среднего времени ожидания квитанции, а также предыдущее значение межсегментного интервала. Эти параметры целесообразно использовать в качестве входных переменных системы нечеткого вывода.

Для выбора межсегментного интервала предлагается использовать один из наиболее распространенных на практике алгоритмов нечеткого вывода – алгоритм Мамдани [3]. Процесс выбора значения межсегментного интервала заключается в осуществлении нечеткого вывода, состоящего из следующих последовательно выполняемых этапов: фаззификации, агрегирования, активизации, композиции и дефаззификации.

На этапе фаззификации определяются значения функций принадлежности входных переменных соответствующим нечетким множествам. На этапе агрегирования определяются степени истинности условий каждого правила. Этап активизации предполагает вычисление результирующей степени истинности каждого правила. В результате программной реализации процесса формирования нечетких правил получено 23 нечетких правила, степень истинности которых не меньше 0,675. Этап композиции включает определение результирующей функции принадлежности всей совокупности правил. Этап дефаззификации представляет собой определение четкого значения выходной переменной – значения межсегментного интервала.

С целью определения эффективности применения предложенного метода выбора межсегментного интервала по сравнению с наиболее популярными версиями протокола транспортного уровня TCP разработана имитационная модель передачи трафика в телекоммуникационной сети. С использованием этой модели проведен ряд имитационных экспериментов. Аналогичные эксперименты были проведены для других методов управления интенсивностью отправки данных источником. Анализ результатов исследований показывает, что при использовании метода выбора межсегментного интервала на основе системы нечеткого вывода наблюдается снижение среднего времени передачи сообщения на 15,8% – 39% по сравнению с результатами применения других методов управления интенсивностью отправки данных источником, а также значительно уменьшается количество повторных передач пакетов, вызванных сетевыми перегрузками.

Выводы

Таким образом, в результате исследований разработан новый метод выбора межсегментного интервала в транспортном протоколе телекоммуникационной сети. Новизна этого метода заключается в том, что определение текущего значения межсегментного интервала осуществляется с помощью системы нечеткого вывода. Применение указанного метода позволяет обеспечить в сети отсутствие повторных передач сегментов, а также снизить среднее время передачи сообщения на 15,8% – 39%.

Литература:

1. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет / Кучерявый Е.А. – СПб.: Наука и техника, 2004. – 336 с.

2. Польщиков К.О. Математична модель процесу обміну інформацією згідно з протоколом TCP / Польщиков К.О., Лаврут О.О., Александров М.М. // Системи обробки інформації. – Харків: ХУПС, 2007. – Вип.1(59). – С. 82 – 84.

3. Пегат А. Нечеткое моделирование и управление / А. Пегат; [пер. с англ.]. – М.: БИНОМ. Лаборатория знаний, 2009. – 798 с.

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ПРИ МОДЕЛИРОВАНИЕ ПРОЦЕССА МАРШРУТИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Павленко М.А.
Харьковский университет Воздушных Сил имени Ивана Кожедуба
г. Харьков ул. Сумская 77/79, 063-347-25-33, bpgpma@list.ru

The article analyzes the possibility of using neural networks for solving the routing problem in telecommunication networks. Study of quality of the solution of routing using neural networks such as multilayer perceptron, RBF network and Hopfield network.

Развитие телекоммуникационных систем в настоящее время связано с широким внедрением новых технологических решений в их построение и использование. В современном мире развитие телекоммуникационных систем (ТКС) направлено на создание единой интегральной мультисервисной широкополосной сети связи, которая будет способна обеспечить возрастающие потребности пользователей к качеству обслуживания и количеству используемых сервисов. Решение данной задачи может быть осуществлено с помощью использования единой интегральной мультисервисной широкополосной сети связи. Переход к новым технологическим основам построения ТКС потребует решения множества задач управления в таких системах, в частности задач управления маршрутизацией.

Реализованные в аппаратуре маршрутизации алгоритмы решают задачи маршрутизации через определенные таймерами промежутки времени от 0 до 30 с. Однако при изменениях топологии сети или характеристик каналов передачи данных расчет новых маршрутов не всегда реализуется в заданные интервалы обновления маршрутных таблиц. Это, в свою очередь, приводит к значительным задержкам в передачи информации, снижении качества передачи данных и потере данных. Таким образом, необходимо проводить дополнительные исследования, связанные с поиском альтернативных методов решения задач маршрутизации, которые позволят решать данные задачи в реальном масштабе времени без снижения качества их решения. Одним из подходов к решению задачи маршрутизации является использование аппарата искусственных нейронных сетей. На сегодняшний день разработано несколько десятков моделей искусственных нейронных сетей. Однако не для всех моделей искусственных нейронных сетей проведена оценка возможности использования для решения задач маршрутизации. Проведем анализ возможности использования искусственных нейронных сетей (ИНС) для решения задачи маршрутизации в ТКС. В рассматриваемом случае решение задачи однопутевой маршрутизации сводится к решению оптимизационной задачи поиска пути с наибольшей пропускной способностью в сети.

В результате проведенного эксперимента получены следующие зависимости вероятности правильного решения задачи маршрутизации в ТКС с использованием ИНС прямого распространения (рис.1).

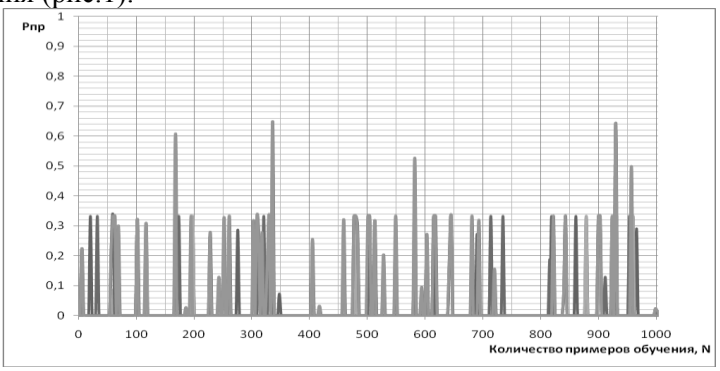


Рис. 1. Зависимость вероятности правильного решения задачи маршрутизации в ТКС с использованием ИНС прямого распространения от количества примеров обучения и эпох обучения.

На следующем этапе проводился анализ применимости для решения задачи маршрутизации ИНС Хопфилда (рис.2).

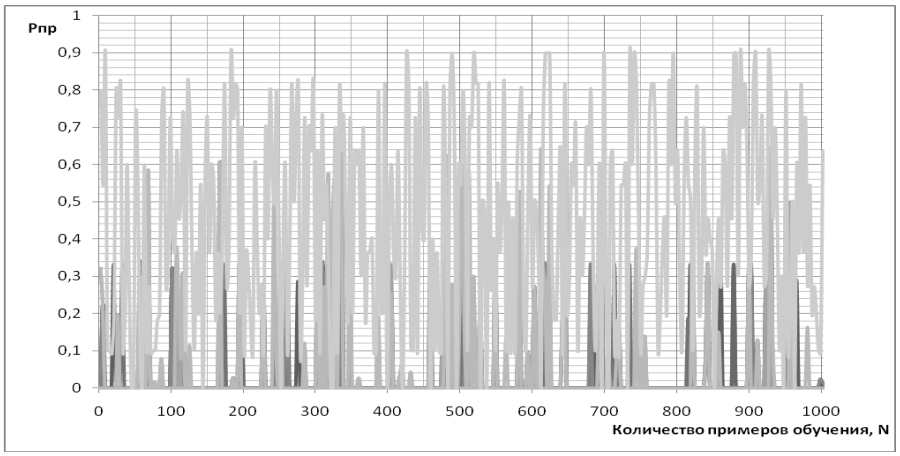


Рис. 2. Зависимость вероятности правильного решения задачи маршрутизации в ТКС с использованием ИНС Хопфилдаот количества примеров обучения и эпох обучения.

При обучении ИНС типа RBF удалось добиться того, что сеть запомнила все обучающие примеры, однако результаты тестирования показали худший результат работы ИНС по сравнению с сетями прямого распространения и сетью Хопфилда (рис.3). Сеть показала низкую устойчивость при изменении характеристик каналов передачи данных и не обеспечила постоянность качества решения данной задачи. Данная ИНС оказалась не способна обобщить результаты обучения и провести распознавание на данных немного отличающихся от обучающих примеров.

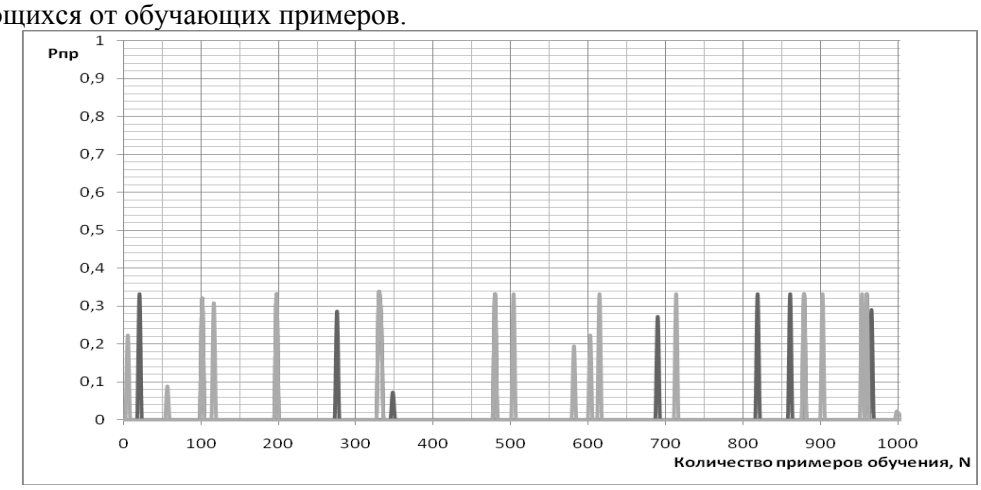


Рис. 3. Зависимость вероятности правильного решения задачи маршрутизации в ТКС с использованием ИНС Хопфилдаот количества примеров обучения и эпох обучения.

Выводы. В результате проведенных исследований о возможности использования ИНС с конфигурациями многослойный персептрон, сеть Хопфилда и RBF-сеть для решения задачи маршрутизации в ТКС было установлено:

1. Сети прямого распространения и сети Хопфилда могут быть использованы для решения задачи маршрутизации в ТКС.

2. Использование данных ИНС требует доработок их топологий и использовании модифицированных процедур обучения направленных на решения оптимизационных задач.

3. Необходимы дополнительные исследования по уточнению топологии связей в ИНС и их влияние на процесс обучения и качество решения задачи маршрутизации (учет

реальных связей в ТКС).

4. Необходимы дополнительно исследовать типы используемых передаточных функций нейронов ИНС, а так же виды оптимизационных функций (функций ошибки) ИНС которые влияют на качество решения задачи маршрутизации.

Таким образом, одним из дальнейших направлений исследований следует считать определение требований к структуре ИНС, типу передаточных функций и функций ошибки ИНС, которые бы обеспечили удовлетворительное качество решения задачи маршрутизации в ТКС. Наиболее перспективным объектом для дальнейшего исследования представляется ИНС Хопфилда.

ПОТОКОВАЯ МОДЕЛЬ ДИНАМИЧЕСКОЙ БАЛАНСИРОВКИ ЗАГРУЖЕННОСТИ ОЧЕРЕДЕЙ В MPLS-СЕТИ С ПОДДЕРЖКОЙ TRAFFIC ENGINEERING QUEUES.

Симоненко А.В.
Харьковский университет Воздушных Сил им. И. Кожедуба
ул.. Сумская, 77/79, 61023, Харьков, Украина, E-mail: 28186@mail.ru

The article proposes a flow-base model balancing queues at the nodes of MPLS-network. The novelty of the model is that it, in the contrast to the previously known models takes into account the features of the Traffic Engineering Queues technology, aimed at achieving a balanced buffer resource node load.

Введение

По причине стремительного развития телекоммуникационных технологий физического и канального уровня эталонной модели взаимодействия открытых систем (ЭМВОС) все большая ответственность за решение задач по обеспечению качества обслуживания (Quality of Service, QoS) в современных мультисервисных телекоммуникационных сетях (ТКС) перекладывается на средства (механизмы и протоколы) сетевого уровня этой модели. На сетевом уровне ЭМВОС решаются такие важные сетевые задачи системного характера, как маршрутизация, распределение и резервирование канального и буферного ресурса ТКС, которые условно объединены в комплекс задач по управлению трафиком. При этом, численные значения таких ключевых для мультимедийных приложений показателей QoS как средняя задержка, джиттер, уровень потерь пакетов во многом определяются эффективностью управления очередями (буферным ресурсом) на маршрутизаторах ТКС [1, 2]. Поэтому научно-практические разработки и исследования, связанные с оптимизацией процессов управления очередями на основе усовершенствования или разработки новых математических моделей и алгоритмов (методов), являются важными и актуальными.

I.Анализ известных решений по обслуживанию очередей в ТКС

В настоящее время в современных ТКС нашли свое применение достаточно большое число алгоритмов управления очередями [1, 2] с точки зрения их обслуживания и превентивного ограничения длины очереди.

К первой группе относятся такие алгоритмы, как *FQ, PQ, WFQ, LLQ* и др., которые обеспечивают формирование очередей, их обслуживание и в явном или неявном виде распределяют пропускную способность (ПС) исходящего канала связи между потоками пакетов различных очередей. Если же алгоритмы этой группы не справляются с поступающей нагрузкой, то для борьбы с перегрузкой очередей используются алгоритмы второй группы – *RED, WRED, ECN, SPD* и др., к задачам которых относится ограничение длины очереди путем выборочного отбрасывания пакетов различных потоков (*RED, WRED, SPD*) или явного уведомления узла источника о перегрузке (*ECN*).

Недостатки технологических решений определили актуальность проведения дополнительных научных исследований в области обслуживания очередей на узлах сети. Например, с целью учета характеристик обслуживаемого трафика необходимо использовать именно потоковые модели (*flow-based model*), в рамках которых учитывается также интенсивность трафика наряду с другими важными параметрами -длины пакета, его приоритета и т.д. Это особенно актуально ввиду того, что многие средства управления трафиком в настоящее время становятся потокоориентированными – *Flow-Based WFQ, Flow-Based Routing* или *Flow-Based Weighted RED*. Кроме того, при оптимизации управления трафиком в сетях *MPLS* (*MultiProtocol Label Switching*), которые находят свое все большее использование по причине внедрения концепции сетей следующего поколения *NGN* (*Next Generation Network*), важную роль играет технология инжиниринга трафика (*Traffic*

Engineering, TE). Это основывается на том, что в основу технологии инжиниринга трафика положены идеи балансировки использования разнородных сетевых ресурсов – информационных, буферных и канальных.

II. Потоковая модель балансировки очередей на принципах Traffic Engineering Queues

В процессе моделирования задач по обслуживанию очередей условимся, что число отдельных трафиков или агрегированных по классам или приоритетам потоков известно и равно *M*, что соответствует принятым на практике решениям в рамках известных методов маркировки пакетов. Наряду с этим примем, что максимальное число очередей на сетевом узле также фиксировано (*N*).

Кроме того, обозначим через a_i ($i = \overline{1, M}$) - интенсивность трафика *i*-го класса, поступающего на обслуживание сетевым узлом. Кроме того, пусть b_j ($j = \overline{1, N}$)- часть пропускной способности исходящего канала связи, которая выделена j -й очереди ($j = \overline{1, N}$), что типично, например, для алгоритма CBWFQ. Одно из ключевых отличий предлагаемого решения будет состоять в том, что переменные b_j ($j = \overline{1, N}$) будут рассчитывать адаптивно к изменению состоянию сетевого узла, а не административно, как, например, в CBWFQ.

В ходе управления очередями необходимо выполнить: условие отсутствия перегрузки канала связи (КС):

$$\sum_{j=1}^{N} b_j \le b , \tag{1}$$

где *b* - пропускная способность исходящего КС.

Кроме того, с целью предотвращения перегрузки сетевого узла необходимо обеспечить выполнение следующего условия:

$$\sum_{i=1}^{M} a_i \le b . \tag{2}$$

Выполнение условия (2) определяет необходимость превентивного ограничения интенсивности суммарного (агрегированного) потока пакетов, поступающих на сетевой узел, чтобы она не превышала пропускную способность исходящего канала связи.. Придать динамический характер управлению очередями в рамках предлагаемой модели можно путем введения переменной x_{ij} , под которой подразумевалась доля i -го трафика, поступающего для обслуживания в j -ю очередь. Согласно физическому смыслу переменной x_{ij} имеют место следующие дополнительные условия:

$$x_{ij} \in \{0,1\} \quad (i = \overline{1, M} , \ j = \overline{1, N}), \tag{3}$$

$$\sum_{j=1}^{N} x_{ij} = 1 \quad (i = \overline{1, M}), \tag{4}$$

$$\sum_{i=1}^{M} a_i x_{ij} \le b_j \quad (j = \overline{1, N}). \tag{5}$$

Выполнение условия (4) гарантирует отсутствие потерь пакетов на рассматриваемом сетевом узле. Условия (5) вводятся для предотвращения перегрузки пропускной способности отдельных очередей сетевого узла в процессе управления. По аналогии с моделью, рассмотренной в работах [5, 6], в качестве искомого вектора выберем вектор

$$\vec{x} = \begin{bmatrix} x_{ij} \\ -- \\ b_j \end{bmatrix} \quad (i = \overline{1, M}\ ;\ j = \overline{1, N}\ ). \tag{6}$$

в ходе расчета, которого удается обеспечить согласованность в решении задач обслуживания очередей и динамического распределения за ними пропускной способности исходящего канала связи.

III Формализация условий предотвращения перегрузки очередей на узле ТКС

В ходе выполнения условий (5) ввиду случайного и нестационарного характера сетевого графика на узле возникают очереди и связанные с ними задержки пакетов. С целью введения верхней границы подобных задержек на узлах ТКС общую буферную емкость, как правило, ограничивают. Таким образом, для каждой очереди определим ее текущую загруженность и максимальную вместимость, обозначив их соответственно через $\bar{n}_j$ и $n_j^{\max}$ ($j = \overline{1, N}$), и дополним условия предотвращения перегрузки отдельных очередей по их пропускной способности (5) условиями предотвращения перегрузки очередей по их длине. В самом общем виде искомые условия будут иметь следующий вид:

$$\bar{n}_j \le n_j^{\max}(\cdot) \tag{7}$$

и задача теперь сводится лишь к выбору (обоснованию) аналитического выражения для расчета средней длины очереди в процессе обслуживания. Для формулировки искомых условий необходимо задаться моделью трафика (его характеристиками - интенсивность, длина пакета и т.д.) и моделью обслуживания пакетов в рамках отдельно взятой очереди, в качестве которой на практике, как правило, реализуется модель FIFO (First In, First Out). При этом каждому типу трафика, а значит и каждой очереди, может соответствовать своя модель обслуживания, не обязательно отвечая перечню вариантов СМО, приведенных выше. Кроме того, нетрудно заметить, что условие (7) является более строгим, чем требование (5). С точки зрения обеспечения гарантий *QoS* по показателям межконцевой средней задержки в ряде случаев удобней неравенства (7) заменить на временные условия

$$\bar{\tau}_j \le \tau_j^{\max}(j = j = \overline{1, N}), \tag{8}$$

где средняя задержка обслуживания $\bar{\tau}$ в той или иной очереди может быть рассчитана по известной средней длине очереди на основе формулы Литтла. Это позволило в терминах предложенной выше модели получить условие (8) в более детальном виде.

$$\frac{n_j + \rho}{\sum_{i=1}^{M} a_i x_j} \le \tau_j^{\max}(j = \overline{1, N}). \tag{9}$$

Использование системы условий (9) особенно актуально в случае, если численные значения требуемой межконцевой средней задержки (как показателя *QoS*) нормированы по отдельным участкам сети. Тогда в процессе управления очередями важно не превысить эти нормированные (заданные) для отдельно взятой пары узел канал значения средней задержки пакетов, что особенно характерно при решении задач по обеспечению гарантированного *QoS* в рамках архитектурной модели *Integrated Services* (*IntServ*).

IV. Формулировка оптимизационной задачи по обслуживанию очередей на узле MPLS-сети с поддержкой Traffic Engineering Queues

В связи с тем, что, в общем случае, выбор управляющих переменных x_{ij} и b_j в рамках ограничений (1), (3), (4) и (7) или (9) можно произвести множеством случаев, то

целесообразно задачу, связанную с расчетом вектора (6), сформулировать в виде оптимизационной. Основным требованием к целевой функции является учет физики протекающих на узле процессов обслуживания пакетов (1)–(7), (9), а также соответствие получаемых решений принципам концепции *Traffic Engineering Queues*, касающихся обеспечения сбалансированной загрузки буферных ресурсов. С этой целью выше изложенную модель важно дополнить следующими условиями

$$\cdot f(p_j, d_j) \cdot n_j \le \alpha, \ (j = 1, N), \qquad (10)$$

где α – верхний динамически управляемый предел загруженности очередей на узле ТКС, $f(p_j)$ – некоторая функция от характеристик j -го потока, например, его приоритета p_j или длины пакета d_j. Именно эти характеристики на практике влияют на порядок обслуживания пакетов в очередях, например, в алгоритме FQ учитывается длина пакета, а в алгоритме WFQ – и длина пакета, и его приоритет. Как правило, чем меньше длина пакета, тем «качественней» обслуживается поток, т.к. небольшими пакетами передается трафик реального времени, который очень чувствителен к задержкам. Стоит отметить, что поток с более высоким приоритетом должен традиционно [2] обслуживаться лучше, чем трафик с низким приоритетом.

В результате, значение функции $f(p)$ должно быть тем больше, чем выше приоритет и чувствительность к задержке данного потока. В этой связи, в выражении (10) в качестве функции характеристик потока можно использовать следующее выражение:

$$\cdot f(p_j, d_j) = \frac{p_j}{\nu \cdot d_j}, \ (j = 1, N), \qquad (11)$$

где ν – некоторый нормировочный коэффициент, который должен сглаживать различие в порядке значений приоритета (0÷7) и длины пакета в байтах. По аналогии с алгоритмом *WFQ* значение этого коэффициента может варьироваться в зависимости от версии операционной системы (IOS) маршрутизатора.

Например, в операционных системах IOS версии 12.0(4)T и ниже $\nu = 4096$, а в операционных системах IOS версии 12.0(5)T $\nu = 32768$ [1]. Если в одной очереди обслуживаются потоки с различными (но по определению близкими) значениями длины и (или) приоритета пакета, то в выражении (11) целесообразно использовать их усредненные значения. Тогда задача обслуживания очередей может быть сведена к задаче балансировки их длины в ходе минимизации следующей целевой функции:

$$\min_{x,b,a} a, \qquad (12)$$

что соответствует минимизации верхнего порога загруженности очередей на узле ТКС, взвешенного относительно таких характеристик потока, как длина пакета и его приоритет, что способствует сбалансированной загруженности всех очередей в соответствии с требованиями технологии *Traffic Engineering Queues*.

В случае, если количество формируемых очередей превосходит число потоков трафика, то задача распределения потоков по очередям становится тривиальной, ввиду отсутствия дефицита очередей. Поэтому размерность искомого вектора (6) можно значительно снизить, т.к. переменные x_{ij} ($i = \overline{1, M}$; $j = \overline{1, N}$) рассчитывать нет необходимости, а требуемую балансировку очередей можно будет обеспечивать за счет вычисления лишь переменных b_j ($j = \overline{1, N}$).

Выводы

Таким образом, предложена потоковая модель балансировки очередей на узлах *MPLS*-сети. Новизна модели состоит в том, что она в отличие от ранее известных моделей учитывает особенности технологии *Traffic Engineering Queues*, нацеленной на обеспечение сбалансированной загруженности буферного ресурса – очередей сетевого узла. Важ-

ной особенностью предлагаемого решения является то, что балансировку в рамках предлагаемой модели планируется осуществлять с учетом приоритета и длины образующих ту или иную очередь пакетов.

Литература:

1. *Вегеншa Ш.* Качество обслуживания в сетях IP: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 386 с.

2. *Справочник* по телекоммуникационным технологиям: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 640 с.

5. *Лемешко А.В., Симоненко А.В., Ватти Махмуд*. Потоковая модель управления очередями с динамическим распределением пропускной способности исходящего канала связи // Наукові записки УНДІЗ. – 2008. – №3(5). – С. 34-39.

6. *Симоненко А.В.*, *Ахмад Хайлан, Али Али* Модель динамического управления очередями и пропускной способностью канала связи на маршрутизаторах мультиервисной сети // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2008. – Вып. 155. – С. 164–168.

МОДЕЛЬ УПРАВЛІННЯ ТРАФІКОМ З ГАРАНТІЯМИ НА ЯКІСТЬ ОБСЛУГОВУВАННЯ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Добришкін Ю.М., Воронов Д.М., Куценко В.В.
Харківський університет Повітряних Сил імені Івана Кожедуба
61023, Харків, вул. Сумська, 77/79, тел. (057) 341-22-15,
E-mail: dobr-73@mail.ru

In the given work is proposed approach to the task solution of the dynamic restriction of traffic intensity that comes in the network. The benefit of the suggested approach is to ensure compliance of the task solution of traffic intensity with the other tasks of management (routing, distribution of channel resource) and to ensure quality of service.

Вступ. Створення сучасних мультисервісних телекомунікаційних мереж (ТКМ) здійснюється в рамках концепції NGN (Next Generation Network), що дозволить переносити різнорідну за складом інформацію з наданням широкого спектру послуг із заданими значеннями обраних показників якості обслуговування (Quality of Service, QoS) [1]. Продуктивність телекомунікаційних мереж, побудованих за принципами NGN, багато в чому залежить від ефективності реалізації функцій системи управління мережними ресурсами, до числа яких, зокрема, відносяться й засоби управління трафіком як на границі, так і усередині мережі.

Як правило, в NGN на рівні транспорту управління трафіком полягає в його маршрутизації, управлінні чергами, а на рівні доступу – у його згладжуванні й обмеженні інтенсивності у випадку порушення вимог угоди про рівень сервісу (Service Level Agreement, SLA). Як показав проведений аналіз, сучасні аплікації мультисервісних ТКМ вимагають гарантій одночасно за декількома показниками якості обслуговування. З метою одержання заданих значень обраних для того або іншого типу трафіку показників якості обслуговування з мінімальним використанням мережних ресурсів необхідно забезпечити погоджене розв’язання окремих мережних задач управління – маршрутизації, розподілу пропускної здатності трактів передачі, обмеження трафіку, що надходить до мережі, й ін. Крім того, з огляду на мультисервісний характер сучасних ТКМ, відмови в обслуговуванні повинні погоджуватися у відповідності із заданими пріоритетами, а також і з підтримкою гарантій якості обслуговування одночасно за декількома показниками.

На жаль, в сучасних ТКМ в рамках існуючих мережних технологій вирішення різних задач управління трафіком практично не узгоджені. Існуючі засоби управління трафіком, що відповідають за його формування, розподіл (маршрутизацію) і обмеження інтенсивності носять розподільчий характер. Крім того, евристичні за своїм змістом моделі управління трафіком – пошуку найкоротшого шляху в мережі, корзини маркерів і дірявого відра не здатні врахувати зміну поточного навантаження мережного вузла і характеристик трафіків інших користувачів [2].

В зв'язку з цим, виникає актуальна задача по розробці моделей, здатних підтримувати багатошляхову маршрутизацію, превентивне обмеження інтенсивності трафіку на прикордонних вузлах мережі з урахуванням заданих пріоритетів, а також і з підтримкою гарантій якості обслуговування одночасно за декількома показниками.

Модель управління трафіком з гарантіями на якість обслуговування. Максимального рівня узгодженості вирішення задач управління мережними ресурсами і, зокрема, інформаційним трафіком можна забезпечити, лише грунтуючись на єдиній (комплексній) математичній моделі управління. За основу була взята відома раніше [3] потокова модель маршрутизації. Новизна моделі полягає в тому, що на відміну від раніш відомих моделей за рахунок введення додаткових змінних в умови збереження потоку, які характеризують інтенсивність трафіку, що отримав відмову в обслуговуванні мережею, забезпечується комплексний характер вирішення задач багатошляхової маршрутизації і обмеження трафіку, що надходить до мережі. Крім того, особливістю запропонованої моделі є те, що саме підбором координат вектора вагових коефіцієнтів можна вказати як на пріоритет у використанні тим або іншим

трафіком канальних ресурсів ТКМ, так і пріоритет при можливому обмеженні в обслуговуванні трафіків користувачів.

Задача управління в рамках запропонованої моделі сформульована як оптимізаційна задача, причому завдяки тензорному узагальненню вдалося отримати в аналітичному вигляді і ввести як додаткові обмеження умови забезпечення гарантій якості обслуговування за швидкісними, часовими (середня затримка, джитер) показниками QoS і показникам надійності (вірогідність своєчасної доставки пакетів). Як цільова були вибрані різні цільові функції, які мали лінійний або змішаний вигляд.

В результаті проведеного аналізу [4] встановлено, що при використанні в якості критерію оптимальності лінійної цільової функції забезпечується комплексне вирішення задач маршрутизації і адаптивного обмеження інтенсивності трафіку, що надходить до мережі, на основі абсолютних пріоритетів. Так, у випадку можливого перевантаження мережі превентивне обмеження буде стосуватись в першу чергу найменш пріоритетного трафіку – аж до повної відмови в доступі. Трафік з більш високим пріоритетом обмеження не буде стосуватись доти, поки можна відмовити низькопріоритетному. При цьому відмови здійснюються за рахунок послідовного відключення шляхів, починаючи з найбільшої "довжини". Подібна модель обмеження інтенсивності трафіка багато в чому схожа на модель пріоритетного обслуговування черг на мережних вузлах (Priority Queuing, PQ).

При використанні моделі із змішаною цільовою функцією по-перше, узгоджено реалізується багатошляхова стратегія маршрутизації з послідовним включенням шляхів, але, на відміну від моделі з лінійною цільовою функцією, наступний шлях використовується, не допускаючи повного завантаження попереднього, по-друге, організується управління трафіком на основі відносних пріоритетів, тобто у випадку перевантаження відмови в обслуговуванні стосуються всіх трафіків, при цьому в меншій мірі високопріоритетного, а в більшій – низькопріоритетного. Подібна модель управління трафіком нагадує роботу алгоритму зваженого рівномірного обслуговування черг на основі класу (CBWFQ).

Крім того, в рамках моделі за рахунок введення системи додаткових, у загальному випадку, нелінійних умов-обмежень на якість обслуговування забезпечуються гарантії QoS одночасно за декількома показниками в умовах узгодженого розв’язання задач багатошляхової маршрутизації і превентивного обмеження інтенсивності трафіка, що надходить до мережі. Характерною рисою запропонованої моделі є той факт, що відмови спостерігаються при неможливості задоволення вимог за часовими показниками якості обслуговування і показниками надійності, а першочергове обмеження стосується трафіків, які ініціюють перевантаження з урахуванням пріоритетів відповідно до значень вагових коефіцієнтів.

Висновки. Таким чином, у роботі запропонована модель управління трафіком з гарантіями на якість обслуговування в мультисервісних телекомунікаційних мережах. Реалізація запропонованої моделі, на відміну від раніше відомих, дозволяє забезпечити гарантії якості обслуговування інформаційних потоків одночасно за декількома показниками в умовах узгодженого вирішення задач багатошляхової маршрутизації і превентивного обмеження інтенсивності трафіку, що надходить до мережі.

Література:

1. Вегенша Ш. Качество обслуживания в сетях IP / Вегенша Ш.; пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 386 с.

2. Остерлох Х. Маршрутизация в IP-сетях. Принципы, протоколы, настройка / Х. Остерлох – СПб.: BHV. – СПб. – 2002. – 512 с.

3. Seok Yo., Lee Yo., Choi Ya. Dynamic constrained multipath routing for MPLS networks // Proc. of IEEE ICCCN. Scottsdale, 2001. Vol.2., №1. – P. 348-353.

4. Саваневич В.Е. Комплексна модель маршрутизації та обмеження трафіку в телекомунікаційних мережах військового призначення / В.Е. Саваневич, О.В. Лемешко, Д.В. Агеєв, Ю.М. Добришкін // Системи озброєння та військова техніка. – 2010. – 2 (22). – С. 78 - 84.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ БАЛАНСИРОВКИ НАГРУЗКИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ УРОВНЯ ДОСТУПА

Воробьев А.В.
Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ»
61070, Харьков, ул. Чкалова, 17, каф. №504, тел. (057) 707-43-52,
E-mail: and_vorobey@hotmail.com; моб. (050) 53-84-827

The load balancing methods of telecommunication network access level is analyzed. The method of local dynamic models for the load balancing is proposed. This method is a dynamic and balances traffic among routes with different cost. A comparison of methods used by the load balancing in the protocols OSPF, RIP, EIGRP with the method of local dynamic models is compared.

Введение

Эффективность функционирования телекоммуникационной сети (ТКС) во многом определяется решением задач маршрутизации. В большинстве современных маршрутных протоколов возможные пути следования сетевого трафика определяются значением наименьшей суммарной стоимости (метрики), на основе алгоритмов поиска «кратчайшего» пути. При наличии в сети нескольких равноценных альтернативных маршрутов осуществляется балансировка (распределение) нагрузки (БН) [1].

В большинстве случаев для реализации распределения нагрузки в ТКС уровня доступа протоколы маршрутизации используют алгоритм Round-robin, основанный на переборе по круговому циклу [2]. Так, по умолчанию протоколы OSPF, RIP, EIGRP поддерживают БН между четырьмя маршрутами с равной метрикой. В зависимости от того как маршрутизатор обрабатывает пакет БН может, выполняется по-пакетно (per-packet) или по-получателю (per-destination) [3].

Если же маршруты не являются полностью равноценными, распределение трафика между ними в большинстве случаев не происходит. Исключением является протокол EIGRP, который осуществляет БН между маршрутами с разной метрикой, однако при этом он требует выполнения ряда соответствующих условий. Эти условия далеко не всегда могут быть удовлетворены, и как следствие альтернативные маршруты не будут использованы [4].

Еще одним существенным недостатком существующих методов БН является то, что балансировка между альтернативными маршрутами осуществляется без учета текущей загрузки. Так, если один из маршрутов будет перегружен, то пакеты все равно будут посылаться по нему [1].

Приведенные недостатки указывают на то, что решение задачи балансировки нагрузки еще далеко от своего завершения, и требует дальнейших исследований.

В работе предложен метод локальных динамических моделей для решения задачи сбалансированного распределения нагрузки. Основными отличительными особенностями этого метода от большинства существующих, является то, что он динамический, а также позволяет распределять нагрузку в зависимости от состояния каналов между альтернативными маршрутами с разной стоимостью.

Этот метод распределения нагрузки предлагается реализовывать как дополнение к существующим протоколам маршрутизации, которые поддерживают помимо таблиц маршрутизации, топологические таблицы и располагают дополнительными сведеньями, отображающими состояние каналов.

В работе ставится задача исследования эффективности и сравнения методов балансировки нагрузки использующихся в протоколах RIP, OSPF, EIGRP на уровне доступа с методом локальных динамических моделей.

Исследования эффективности методов балансировки нагрузки

Исследования эффективности методов БН проводилось на однопродуктовой сети (рис. 1) при помощи моделирования в среде MATLAB. Сеть состояла из передающего

(формирует поступающую нагрузку на сеть) и принимающего хостов, 6 узлов и 8 трактов передачи с соответствующими величинами их пропускных способностей (в Мб). Процесс поступления нагрузки в сеть задавался интенсивностью поступления пакетов $y(k)$ как случайная величина (процесс), распределенная по нормальному закону с параметрами $M[y(k)]=200$, $D[y(k)]=100$. Балансировку нагрузки осуществлял маршрутизатор 1, в то время как остальные маршрутизаторы 2-5 выполняли функцию повторителей, а 6 сумматора с повторителем.

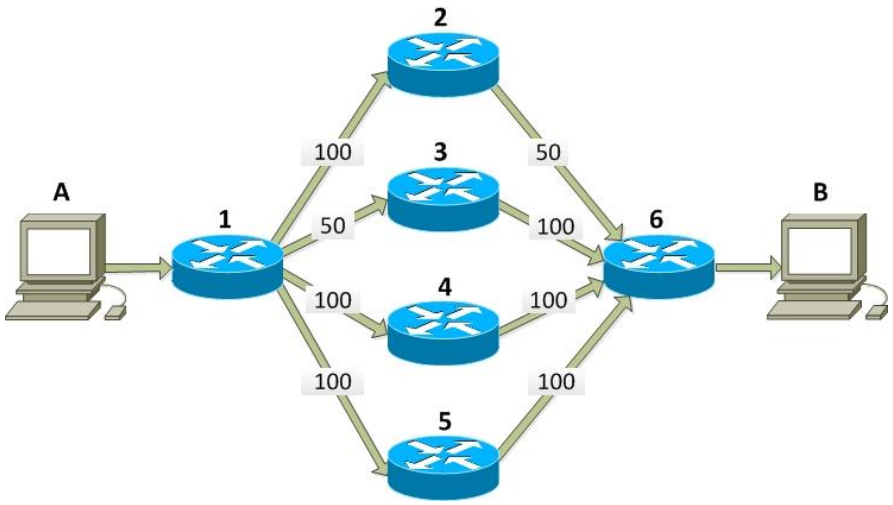


Рис. 1 - Топология сети

Выводы

Из полученных результатов сделан вывод, что максимальный выигрыш по производительности сети, и коэффициентам использования линий связи сети дают метод локальных динамических моделей и метод БН используемый в протоколе EIGRP. Такие результаты объясняются тем, что методы БН протоколов RIP и OSPF смогли распределять нагрузку только по двум маршрутам 1-4-6, 1-5-6, в то время как метод БН протокола EIGRP использовал в дополнение маршрут 1-3-6. В методе локальных динамических моделей помимо трех вышеприведенных маршрутов был задействован маршрут 1-2-6 на 50 Мбит/с, что обусловлено самым узким местом маршрута («бутылочным горлом») равным 50 Мбит/с. Таким образом, этот метод позволил максимально использовать все ресурсы сети.

Литература:

1. Инжиниринг трафика. / Интернет-Университет Информационных Технологий // Режим доступу. : http://www.intuit.ru/department/network/ndnets/13/.

2. Балансировка нагрузки. [Електронний ресурс] / Материал из Википедии — свободной энциклопедии // Режим доступу. : http://ru.wikipedia.org/wiki/ Балансировка_нагрузки.

3. Как работает средство балансировки нагрузки? [Електронний ресурс] / Cisco Systems, Inc // Режим доступу. : http://img.nag.ru/projects/setup/808/80a53ebe5051ac1df902d846da59debe.pdf .

4. Как работает распределение нагрузки с неравной стоимостью путей (вариация) в IGRP и EIGRP? [Електронний ресурс] / Cisco Systems, Inc // Режим доступу. : http://img.nag.ru/projects/setup/137/e4d99b180a1502c66a7f92f0863aff78.pdf .

МЕТОД ДИНАМИЧЕСКОГО УПРАВЛЕНИЯ ОЧЕРЕДЯМИ В СЕТИ MPLS-TE

Лемешко А.В., Али С. Али
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем,
E-mail: avlem@ukr.net, конт. тлф. 702-13-20

We propose are method and flow-base model balancing queues at the nodes of MPLS-network. The novelty of the model is that it is in contrast to the previously known models take into account the features of the technology Traffic Engineering Queues, aimed at achieving a balanced load buffer resource node.

Важным технологическим средством поддержки и повышения качества обслуживания (Quality of Service, QoS) в современных телекоммуникационных системах и сетях являются механизмы обслуживания очередей, возникающих на узлах (маршрутизаторах, маршрутизирующих коммутаторах) транспортной сети при перегрузках ее каналов связи [1, 2]. Именно задержки пакетов в очередях и их потеря при переполнении очереди определяющим образом влияют на межконцевые показатели QoS – среднюю задержку, джиттер, вероятность доставки пакетов и др.

Несмотря на обилие известных механизмов обслуживания очередей (PQ, CQ, CBQ, FQ, WFQ, LLQ и др.), поддерживаемых в современном сетевом оборудовании различных фирм производителей, проблема обеспечения эффективного решения данной задачи стоит все еще достаточно остро. При этом основное внимание при совершенствовании перечисленных механизмов уделяется следующим аспектам (требованиям):

- поддержка дифференциации пакетов, принадлежащих различным типам трафика;
- повышение уровня автоматизации при решении данной задачи с постепенным снижением роли административного вмешательства;
- переход от попакетной стратегии обслуживания очередей к потоковой, что должно снизить время обработки пакетов в очереди;
- обеспечение согласованности решений с другими задачами управления трафиком (маршрутизации, распределения пропускной способности (ПС) каналов связи (КС), ограничения длины очереди, резервирования ресурсов и др.).

К сожалению, сдерживающим фактором на пути реализации отмеченных требований является несовершенство, а то и полное отсутствие четкого формализованного описания процесса обслуживания очередями, т.к. большинство механизмов основывается на преимущественно эвристических решениях, под которые можно и нужно подвести необходимую теоретическую базу в виде математических моделей и методов. В этой связи, в настоящем докладе основное внимание будет уделено вопросам выбора математической модели и разработки метода управления очередями на узлах сети MPLS-TE, т.к. именно эта технология де-факто является основной транспортной платформой при построении и функционировании сетей следующего поколения (Next Generation Network, NGN).

При описании модели условимся, что число агрегированных потоков трафика известно и равно M, что соответствует принятым на практике решениям в рамках известных методов маркировки пакетов. Наряду с этим примем, что максимальное число очередей на сетевом узле также фиксировано (N). Кроме того, обозначим через a_i ($i=\overline{1,M}$) – интенсивность трафика i-го класса, поступающего на обслуживание сетевым узлом. Кроме того, пусть b_j ($j=\overline{1,N}$) – часть пропускной способности исходящего КС, которая выделена j-й очереди ($j=\overline{1,N}$). Переменные b_j ($j=\overline{1,N}$) будут рассчитывать динамично, адаптируясь к изменению состояния сетевого узла, а не административно, как, например, в большинстве известных решений.

В ходе управления очередями необходимо выполнить условие отсутствия перегрузки канала связи:

$$\sum_{j=1}^{N} b_j \le b\,, \tag{1}$$

и условие предотвращения перегрузки сетевого узла:

$$\sum_{i=1}^{M} a_i \le b\,. \tag{2}$$

где b – пропускная способность исходящего КС.

Придать динамический характер процессу обслуживания очередей в рамках предлагаемой модели можно путем введения управляющей переменной x_{ij}, под которой подразумевалась доля i-го трафика, поступающего для обслуживания в j-ю очередь. Согласно смыслу x_{ij} имеют место следующие условия:

$$x_{ij} \in \{0,1\} \quad (i = \overline{1,M},\ j = \overline{1,N}), \tag{3}$$

$$\sum_{j=1}^{N} x_{ij} = 1 \quad (i = \overline{1,M}), \tag{4}$$

$$\sum_{i=1}^{M} a_i x_{ij} \le b_j \quad (j = \overline{1,N}). \tag{5}$$

Выполнение условия (4) гарантирует отсутствие потерь пакетов на рассматриваемом сетевом узле. Условия (5) вводятся для предотвращения перегрузки пропускной способности КС, выделяемой для передачи пакетов той или иной очереди сетевого узла в процессе управления. В качестве искомого вектора выберем вектор

$$\vec{x} = \begin{bmatrix} x_{ij} \\ -- \\ b_j \end{bmatrix} \quad (i = \overline{1,M};\ j = \overline{1,N}), \tag{6}$$

в ходе расчета которого удается обеспечить согласованность в решении задач обслуживания очередей и динамического распределения за ними пропускной способности исходящего канала связи.

Для каждой очереди определим ее текущую загруженность и максимальную емкость, обозначив их соответственно через $\bar{n}_j$ и $n_j^{\max}$ ($j = \overline{1,N}$). Кроме того, дополним условия предотвращения перегрузки отдельных очередей по их пропускной способности (5) условиями предотвращения перегрузки очередей по их длине. В общем виде искомые условия будут иметь вид:

$$\bar{n}_j \le n_j^{\max} \quad (j = \overline{1,N}), \tag{7}$$

и задача теперь сводится лишь к выбору (обоснованию) аналитического выражения для расчета средней длины очереди в процессе обслуживания.

Средняя длина очереди, опуская индекс очереди, может выражаться различными аналитическими зависимостями. Например для СМО M/M/1/$n^{\max}$:

$$\bar{n} = \frac{\rho^2\left[1-(n^{\max}+1)\rho^{n^{\max}}+n^{\max}\rho^{n^{\max}+1}\right]}{(1-\rho^{n^{\max}+2})(1-\rho)} - \rho\,, \quad \text{где} \quad \rho = \frac{\sum_{i=1}^{M} a_i x_{ij}}{b_j}\,.$$

Целесообразно задачу, связанную с расчетом вектора (6), сформулировать в виде оптимизационной. Основным требованием к целевой функции является учет физики протекающих на узле процессов обслуживания пакетов (1)–(7), а также соответствие получаемых решений принципам концепции Traffic Engineering Queues, касающихся обеспечения сбалансированной загрузки буферных ресурсов. С этой целью выше изложенную модель важно дополнить следующими условиями

$$f(p_j, d_j)\cdot n_j \le \alpha\,, \quad (j = \overline{1,N}), \tag{8}$$

где α – верхний динамически управляемый предел загруженности очередей на узле ТКС, $f(p_j, d_j) = \frac{p_j}{v \cdot d_j}$ – функция от характеристик j-го потока: его приоритета p_j и длины пакета d_j, а v – некоторый нормировочный коэффициент, который должен сглаживать различие в порядке значений приоритета (0÷7) и длины пакета в байтах.

Тогда задача обслуживания очередей может быть сведена к задаче балансировки их длины в ходе минимизации следующей целевой функции:

$$\min_{x,b,\alpha} \alpha, \tag{9}$$

что соответствует минимизации верхнего порога загруженности очередей на узле ТКС, взвешенного относительно таких характеристик потока, как длина пакета и его приоритет, что способствует сбалансированной загруженности всех очередей в соответствии с требованиями технологии Traffic Engineering Queues.

В рамках модели данной модели (1)-(9) предложен метод динамического управления очередями на узлах сети, который основывается на решении следующих важных задач:

- сбор и обработка информации о состоянии (числе и загруженности) очередей, а также характеристиках обслуживаемого трафика (интенсивность, длина и приоритет пакетов). При этом, процесс сбора информации может носить как периодический характер (по аналогии с дистанционно-векторной маршрутизацией), так и апериодический, т.е. «по требованию»;

- расчет управляющих переменных, представленных вектором (6), в ходе решения оптимизационной задачи (9), что позволит придать процессу обслуживания очередей динамический характер. В результате расчетов формируется таблица обслуживания очередей паекетов в соответствии с их длиной и приоритетом;

- анализ полученных решений с последующей оценкой состояния очередей и характеристик трафика (т.е. возврат к п.1). Если решение обеспечить в рамках принятых ограничений невозможно, что обычно связано с переполнением очереди, то задействуются стандартные средства ограничения длины очереди.

Таким образом, в докладе предложены потоковая модель и метод динамического управления очередями на узлах сети MPLS-TE. Новизна модели состоит в том, что она в отличие от ранее известных моделей учитывает особенности технологии Traffic Engineering Queues, нацеленной на обеспечение сбалансированной загруженности буферного ресурса – очередей сетевого узла. Важной особенностью предлагаемого решения является то, что балансировку в рамках предлагаемой модели планируется осуществлять с учетом приоритета и длины образующих ту или иную очередь пакетов.

Сама технологическая по своей сути задача обслуживания очередей в общем случае была сведена к оптимизационной задаче смешанного математического программирования, связанной с минимизацией линейной функции (9) при наличии в т.ч. нелинейных ограничений (7) и (8), а также булевой природы некоторых рассчитываемых переменных (3). Решение данной задачи предполагает использование хорошо апробированных методов решения – округления (Rounding-off), ветвей и границ (Branch-and-bound), последовательной линеаризации (SLP), штрафных функций (Penalty function), множителей Лагранжа (Lagrangian relaxation) и различных смешанных методов.

МЕТОД ОЦЕНКИ ПАРАМЕТРОВ ИНФОРМАЦИОННЫХ ПОТОКОВ, ПЕРЕДАВАЕМЫХ ПО КАНАЛАМ СВЯЗИ МУЛЬТИСЕРВИСНОЙ СЕТИ ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГИ IPTV

Евлаш Д.В., Агеев Д.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем,
тел. (057) 702-55-92, E-mail: evlashdv@mail.ru

The given work is devoted to the development of a method for determining the characteristics of multicast traffic in a multiservice communication channels telecommunication system at providing IPTV services. The method takes into account the specifics of the service television, which is use multicasting, different ratings retransmitted channels, not permanence of multicast groups and the presence of prime time.

Введение

Услуги в мультисервисных сетях предоставляются с использованием индивидуальной и групповой адресации. Особенностью применения групповой адресации является то, что внутри сети создаются копии информационных пакетов. При применение групповой адресации в сети передается multicast трафик, а при индивидуальной — unicast трафик. Основная часть multicast трафика в современных мультисервисных сетях создается при предоставлении услуги IPTV. В то же время существующие методы оценки информационных потоков с групповой адресацией не учитывают специфики предоставления услуги IPTV. Следовательно, необходимо разработать метод позволяющий производить оценку информационных потоков создаваемых при предоставлении услуги IPTV.

Метод оценки информационных потоков

Специфика предоставления услуги IPTV заключается в том, что multicast поток телеканала передается только тем абонентам, которые в данный момент смотрят данный телеканал. Усложняет задачу оценки и то, что абоненты постоянно переключаются между телеканалами и на протяжении дней недели количество абонентов пользующихся услугой IPTV (активных) распределено не равномерно.

Следовательно, чтобы оценить потоки, передаваемые по транспортным каналам связи (КС), необходимо определить какие телевизионные каналы, передаются по ним к узлам доступа (УД). Для решения данной задачи воспользуемся тем фактом, что рейтинги различных телевизионных каналов различаются. Измерением рейтингов телеканалов занимаются компании по маркетинговым и социальным исследованиям, такие как, например, GfK Ukraine Media. Рейтинг телеканала показывает долю аудитории телеканала от общего количества активных телезрителей, которое в свою очередь зависит от дня недели и времени суток. Данная зависимость может быть оценена используя результаты статистических исследований (рис. 1), проведенных TNS Gallup Media.

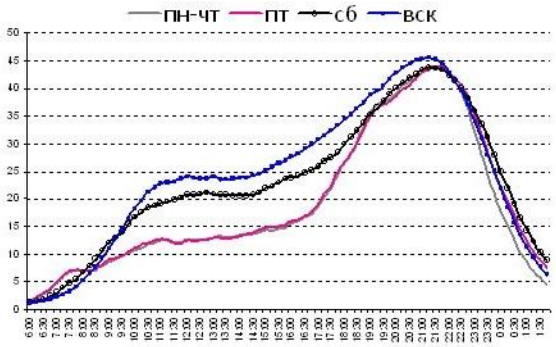


Рис. 1. Зависимость числа активных телезрителей от дня недели и времени суток

Из приведенного исследования видно, что наибольшее количество активных абонентов наблюдается с 21 до 22 часов (прайм-тайм). В это время услугой IPTV пользуется около 45% абонентов. Данное значение рекомендуется использовать для дальнейших расчетов.

Чтобы определить какие телеканалы ретранслируются по каждому каналу связи необходимо вначале рассчитать для какого количества активных абонентов рассматриваемые каналы связи являются транзитными при получении вещания телеканалов, а именно произвести распределение активных абонентов услуги IPTV между каналами связи. Для этого двигаясь вдоль маршрутной матрицы от всех узлов доступа, по очереди, к узлу, на технической площадке которого размещено оборудование «Headend», к каждому пройденному КС добавить количество активных абонентов подключенных к данному УД. За тем на основании рейтингов телеканалов произвести распределение полученных величин каждого КС между ретранслируемыми по сети телеканалами.

Распределение показывает сколько активных абонентов услуги IPTV одновременно смотрели данный телеканал, используя заданный КС в качестве транзитного, на протяжении рассматриваемого периода времени. Обозначим полученную величину как аудитория телеканала транзитного КС. Данная величина может быть целым числом, дробным или нулем. Если аудитория телеканала транзитного КС имеет целую и дробную часть, то это значит, что на протяжении рассматриваемого периода телеканал смотрело количество абонентов равное целой части, а один абонент смотрел рассматриваемый телеканал долю времени равную дробной части. Таким образом, по КС ретранслируются постоянно те телеканалы, аудитория которых больше единицы, то есть их постоянно смотрит хотя бы один абонент. Телеканалы, аудитория которых меньше единицы, ретранслируются по КС долю времени равную значению аудитории. Для определения параметров суммарного информационного потока в КС необходимо произвести суммирование потоков каждого, ретранслируемого в данном КС, телеканала, предварительно интенсивность потока не постоянно ретранслируемых телеканалов помножив на значение их аудитории.

Описанную выше медику определения параметров суммарного потока в КС при предоставлении услуги IPTV представим в виде алгоритма.

Введем следующие переменные:

$Z^{TV} = \left\| z_i^{TV} \right\|$ – матрица распределения абонентов услуги IPTV, между узлами доступа;

z_i^{TV} – количество абонентов подключенных к *i*-му УД;

N^{HD} – индекс узла на площадке которого расположено оборудование «Headend»;

$R = \left\| r_i \right\|$ – матрица рейтингов вещаемых телеканалов;

r_i – рейтинг *i*-го телеканала;

P^{TV} – доля активных абонентов услуги IPTV в прайм-тайм.

Вспомогательные данные:

$Q^S = \left\| q_{ij}^S \right\|$ – матрица характеризующая какое количество активных абонентов использует каждый из транспортных каналов связи сети для получения вещания телеканалов;

q_{ij}^S – количество активных абонентов, для которых канал связи (*i, j)* является транзитным при получении вещания телеканалов;

$Q^{TK} = \left\| q_i^{TK} \right\|$ – матрица характеризующая аудитории телеканалов для рассматриваемого транзитного КС;

q_i^{TK} – аудитория *i*-го телеканала для рассматриваемого транзитного КС;

$F^{CH.TV} = \left\| f_i^{CH.TV} \right\|$ – матрица размеров информационных потоков ретранслируемых по сети телеканалов, бит/с;

$F^{TV} = \left\| f_{ij}^{TV} \right\|$ - матрица значений информационных потоков в КС при предоставлении услуги IPTV.

Алгоритм определения информационных потоков передаваемых по каждому КС при предоставлении услуги IPTV состоит из двух этапов.

На первом этапе принимаем $i = N^{HD}$ и последовательно по средствам переменной j перебираем все индексы узлов доступа. Вследствие чего получаем конечное число однотипных итераций.

Опишем одну итерацию.

1. Для заданных i и j находим в маршрутной матрице M элемент m_{ij}, принимаем $k = m_{ij}$ и выполняем

$$q_{ik}^S = q_{ik}^S + z_j^{TV} \cdot P^{TV}$$

2. Если $k = j$, то переходим на следующую итерацию. Иначе принимаем $t = k$.

3. Находим в маршрутной матрице M элемент m_{tj}, принимаем $k = m_{tj}$ и выполняем

$$q_{sk}^S = q_{sk}^S + z_j^{TV} \cdot P^{TV}$$

4. Переходим на шаг 2.

На втором этапе последовательно по средствам переменных k и m перебираем все каналы связи. Для каждого транспортного канала связи по средствам переменной i перебираем все ретранслируемые телеканал и для каждого телеканала выполняем следующие расчеты:

$$q_i^{TK} = r_i \cdot q_{km}^S / 100;$$

если $q_i^{TK} \geq 1$, то

$$f_{km}^{TV} = f_{km}^{TV} + f_i^{CH.TV};$$

иначе

$$f_{km}^{TV} = f_{km}^{TV} + (q_i^{TK} \cdot f_i^{CH.TV}).$$

В результате работы алгоритма формируется матрица значений $F^{TV} = \left\| f_{ij}^{TV} \right\|$ информационных потоков в каналах связи при предоставлении услуги IPTV.

Выводы

Разработан метод определения характеристик группового трафика в каналах связи мультисервисной телекоммуникационной системы при предоставлении услуги IPTV. В методе учтена специфика предоставления услуги телевидения, которая состоит в использовании групповой адресации, разных рейтингов ретранслируемых телеканалов, не постоянство состава multicast групп и наличие прайм-тайма. Полученные с помощью этого метода данные в дальнейшем могут быть использованы для параметрического синтеза новых мультисервисных сетей или оценки требуемых сетевых ресурсов при внедрении услуги IPTV на уже существующих сетях.

УЛУЧШЕНИЕ ПАРАМЕТРОВ КАЧЕСТВА ТЕСТИРОВАНИЯ РАДИОТРАКТА НА АБОНЕНТСКОМ УЧАСТКЕ

Кадацкая О.И., Сабурова С.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Телекоммуникационных систем тел. (057) 702-13-02,
E-mail: tks@kture.kharkov.ua ; факс (057) 702-12-13

This work is devoted to developments in obtaining reliable information about quality parameters on the state of radiotract subscriber station in mobile communication. We investigated high-precision method for measuring one of the monitored parameters - frequency results can be used for testing the quality of the path radiotract

С развитием технологий новых поколений динамично совершенствуются методы управления и технической эксплуатации объектов телекоммуникаций. Повышаются требования к процессам получения достоверной информации о параметрах качества состояния радиотракта на абонентском участке в подвижной связи. Для оценки электромагнитной обстановки при внедрении новых систем, стандартов и широкополосных услуг подвижной связи совершенствуются существующие и внедряются новые методы регулирования и поддержки высокого качества работоспособности контролируемых объектов

Основные тенденции и направления развития таких средств и методов на участке абонентского радиотракта определяются двумя факторами:

- первый фактор определяет необходимость решения стратегических (долговременных) и текущих задач по регулированию использования методов оценивания норм;
- второй фактор — необходимость соответствия уровня методологии и технической оснащенности автоматизированных систем контроля и тестирования контролируемых параметров.

Относительно первого фактора следует заметить, что в условиях рыночных отношений основу процесса регулирования составляют, преимущественно, экономические и нормативно-правовые механизмы.

Основное назначение автоматизированных систем контроля и тестирования на участке абонентского радиотракта - обеспечения оценки параметров радиоизлучений на предмет их соответствия нормативным требованиям, в том числе сличение частот, которое предлагается осуществлять методом совпадения импульсов. Наблюдение (мониторинг) за радиоизлучением представляет собой процесс длительного и целенаправленного восприятия информации о наличии радиоизлучения в какой-то полосе частот (на заданной частоте) и измерении его параметров.

Наблюдение реализуется путем:

1) выявления наличия (обнаружения) радиоизлучения на протяжении заданного интервала времени и с заданной дискретностью;

2) идентификации обнаруженного радиоизлучения (радиосигнала);

3) измерения заданных параметров радиоизлучения, обобщения результатов.

Задачами контроля и тестирования на участке абонентского радиотракта является обеспечение:

- соответствия современному техническому уровню и возможностям элементов сети (радиобазовых станций и мобильных терминалов);
- решения задач мониторинга и радиоконтроля традиционных и технологий новых поколений.

Мониторинг реализуется путем использования основных методов:

1) поиск и обнаружение источников радиоизлучений в анализируемой полосе частот (на заданной частоте) — поисковый контроль;

2) наблюдение за радиоизлучением в заданной полосе частот (на заданной частоте);

3) селекция радиоизлучений;

4) измерение параметров радиоизлучения;

5) радиопеленгование источников радиоизлучений;

6) идентификация радиоизлучений и источников радиоизлучений:

- определение местонахождения (географических координат) источников радиоизлучения (ИРИ);

- оценка показателей качества обслуживания (QOS, Quality Operating Service) и качества предоставляемых услуг (QoS, Quality of Service) сетей общего пользования.

Уровень технической поддержки и принципы организации подвижной сети формируют требования к оснащению систем мониторинга высокочувствительными портативными измерительными средствами, обеспечивающими поиск, выявление и контроль параметров излучения мало- и сверхмаломощных источников радиоизлучений с высокой точностью, одним из которых является частота .

Оценим значение частоты методом совпадения импульсов пакетами, для которого погрешность сравнения временных интервалов, выраженных кодами No и Nx, (To и Tx - соответственно период образцовой и измеряемой частоты) снижена до длительности разности периодов $\Delta T = |Tx-To| = fp/(fxfo) = (fo-fx)/(fxfo)$

Канал измерения образован последовательностями импульсов двух близких частот fx и fo – измеряемой и образцовой, которые совмещаются во времени. Для совпадения импульсов пакетами их длительности должны удовлетворять условию $(\tau_x + \tau_0) >> |Tx-To|$. Если подсчитать число импульсов обеих частот в интервале между одноименными импульсами двух последовательно идущих пакетов совпадений, то

$$NoTo-NxTx=To-Tx$$

Искомая частота будет равна

$$fx =[Nx+(To-Tx)fx]fo/No$$

Полученные в процессе измерения коды содержат как систематическую так и случайную составляющие погрешности. Систематическая составляющая, вызываемая долговременной нестабильностью образцовой частоты может быть исключена из результата тем или иным способом. Поэтому можно полагать, что погрешность измерения величины fx определяется только случайными составляющими для Nx и No .

При наличии пакета совпадений интервал времени t между импульсами образцовой и первым импульсом измеряемой частот будет равен $t=[(\tau o+\tau x)fofx]^{-1}$. Пусть длительности импульсов последовательностей с периодом повторения To и Tx равны, то есть $\tau o=\tau x$ Весь пакет представляет собой сигнал, по которому осуществляется отсчет временного интервала. Этот сигнал может быть достаточно протяженным, в центре которого находится импульс длительностью τ, а к краям длительности импульсов в пакете убывают, следовательно, убывают и их амплитуды. Очевидно, что этот наиболее протяженный импульс пакета является адекватным импульсу одиночного совпадения и по нему и осуществляется отсчет. Величину $\Delta T=To-Tx$ можно уменьшить увеличением fo, и уменьшением разностной частоты fp= fo-fx .

Абсолютная методическая погрешность сличения, обусловленная квантованием по уровню, равна $\Delta fx =(t^2fo)^{-1}$.

При измерении частоты случайная погрешность имеет составляющие обусловленные квантованием, помехами на входе, нестабильностями образцовой частоты, порогов формирователей и характеристик поступающих на их входы сигналов.

Инструментальная погрешность метода обусловлена неточностью определения одинаковых по порядку импульсов последовательно идущих пакетов совпадений.

Суммарная погрешность сличения частот равна:

$$\Delta fx=fxM$$

где M - разность номеров между i–ым импульсом начала счета первого пакета и j–ым импульсом окончания счета второго пакета.

Доминирующей погрешностью в суммарной погрешности сличения остается погрешность от нестабильности частоты fx. Влияние на инструментальную погрешность всех остальных факторов может быть сведено к изменению длительности импульсов двух последовательностей. Для стандартных значений длительностей импульсов погреш-

ность сличения частоты составляет величину порядка 10^{-4} Гц., что позволяет улучшить качество тестирования радиотракта по указанному параметру.

Литература:

1. Кадацкая О. И. Преобразование длительности одиночного импульса в код // АСУ и приборы автоматики. Сб. науч. трудов. –Харьков: ХТУРЭ, 1998. – Вып. 107. -С.33-36.

МЕТОДИКА АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ РАСПРЕДЛЕННЫХ СИСТЕМ С СЕРВИС-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРОЙ

Коваленко Т.Н., Тулла Е.Н.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр.Ленина, 14, каф. телекоммуникационных систем,
тел. (057) 702-13-20, e-mail: tanya.n.kov@gmail.com

In this work technique for productivity analysis of distributed systems with service-oriented architecture (SOA) is presented. The technique is based on a hierarchical model using timed coloured Petri nets mathematical tool. In contrast to existing approaches it allows to study performance of SOA systems on the basis of different developers' solutions paying a great attention to characteristics of telecommunication infrastructure which is used for information exchange and transmission.

В современных информационных и телекоммуникационных системах одной из актуальных проблем является проблема интеграции приложений. Сервис-ориентированная архитектура (Service-Oriented Architecture, SOA) является в настоящее время одним из наиболее эффективных и популярных подходов к решению данной проблемы. Основные принципы построения систем с сервис-ориентированной архитектурой рассмотрены в [1], [2]. SOA-системы являются сложными распределенными системами, в которых при предоставлении сервиса конечному потребителю зачастую необходимо обеспечить сетевое взаимодействие нескольких поставщиков. Производительность и другие характеристики таких систем, а также качетство предоставляемых ими сервисов сущственно зависят от характеристик телекоммуникационных систем и сетей (ТКС), обеспечивающих информационный обмен в распределенной ситеме SOA. В связи с этим к ТКС, очевидно, необходимо выдвигать специфические требования, однако для количественной оценка влияния характеристик базовой ТКС на характеристики SOA-системы требуются адекватные математические модели, учитывающие телекоммуникационную составляющую таких систем. Однако предлагаемые на сегодняшний день подходы к оценке производительности распределенных систем с сервис-ориентированной архитектурой основаны на применении специализированного программного обеспечения с целью тестирования конкретного аппаратно-программного решения того или иного производителя. В данной работе для решения этой задачи предлагается применеие системы математических моделей на основе раскрашенных временных сетей Петри [3].

Архитектура SOA-систем и основные подходы к организации обмена данными в них рассмотрены в работах [1], [3]. Для организации взаимодействия сервисов, динамической маршрутизации запросов от прикладного компонента – потребителя сервиса и получения результатов от приложения – провайдера сервиса и решения других коммуникационных задач все большее распространение получает технология корпоративной сервисной шины (Enterprise Service Bus, ESB). ESB предоставляет единый механизм для передачи запросов и получения результатов сервисов, выполнения необходимых преобразований сообщений и транспортных протоколов и управления потоком обращений к сервисам (рис.1). Благодаря такому управлению выполняется необходи мая последовательность вызовов сервиса для реализации бизнес-процесса.

Сети Петри (СП) представляют собой математический аппарат моделирования и анализа стохастических динамических систем и процессов [4], [5]. Иерархическая раскрашенная СП (CPN) представляет собой совокупность нескольких CPN модулей, объединенных в единую модель сложной системы с помощью специальных переходов и позиций. Существующие модули могут использоваться в модели несколько раз, кроме того, на их основе можно создавать новые модули. Иерархическая структура такой модели может быть сколь угодно сложной – каждый модуль может состоять из нескольких более мелких CPN модулей, модули разного уровня иерархии могут иметь общие элементы (позиции слияния).

При построении модели сетевого взаимодействия распределенных компонентов SOA-системы применяется подход «сверху вниз», который предполагает построение обобщенной модели системы с постепенной детализацией моделей процессов, требующих более тщательного анализа. В этом случае любой переход при необходимости может быть преобразован в замещающий, а детальное описание соответствующего данному переходу процесса представляется отдельным CPN модулем [3].

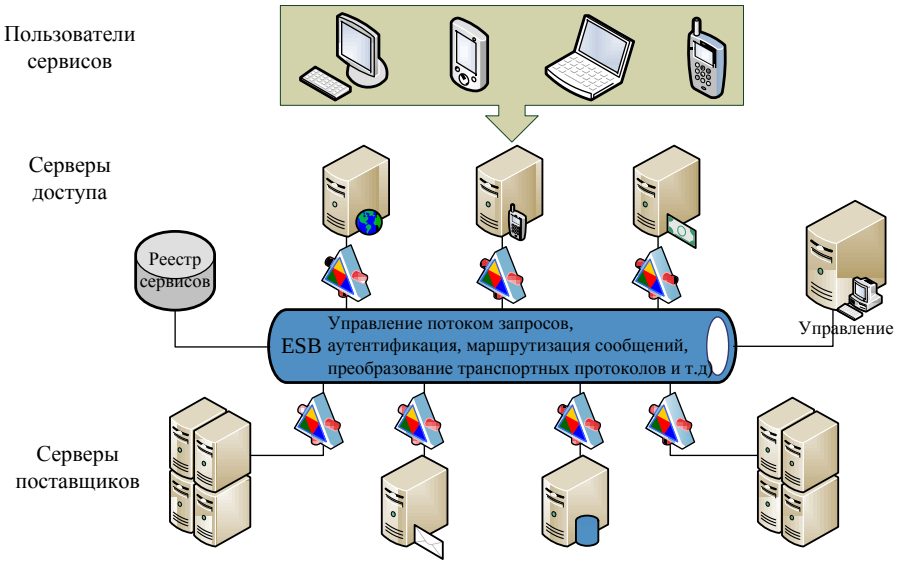


Рис. 1. Роль ESB в структуре SOA

Иерархическая структура предлагаемой модели приведена на рис.2. Верхний уровень модели представляет из себя CPN модуль, описывающий наиболее общие аспекты построения системы SOA, ее структуру и функциональные компоненты.

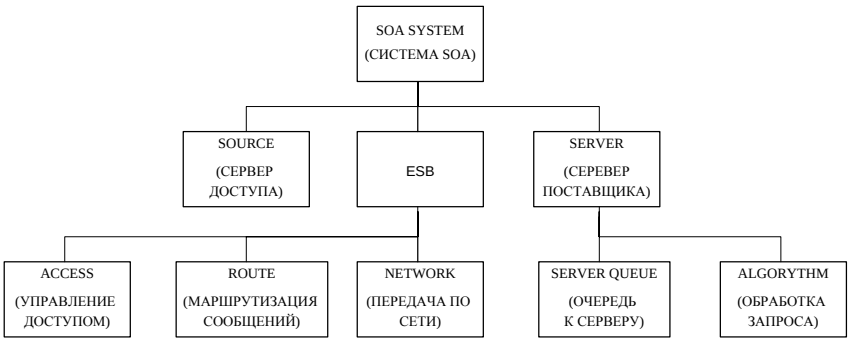


Рис. 2. Иерархическая структура модели взаимодействия компонентов SOA-системы

Обобщенная модель SOA-системы (SOA SYSTEM) соответствует структуре, приведенной на рис.1. Данный CPN модуль представлен на рис. 3,а. Основными компонентами модели являются замещающие переходы “Source” (сервер доступа пользователей к сервисам, предоставляемых системой), “ESB” и “Server” (сервер поставщика сервисов), каждый из которых представляет собой CPN модуль следующего более низкого уровня иерархии. Данные CPN модули был представлены ранее в работе [3]. CPN модуль сервера доступа к сервисам (SOURCE) описывает процесс формирования запросов к системе SOA. В данном модуле происходит моделирование входного трафика, задаются размер и

интенсивность передаваемых по сети блоков данных. Сбор статистической информации для ее дальнейшей обработки и анализа производительности моделируемой системы осуществляется с помощью позиций Amount и ServiceTime, на которых размещаются фишки успешно обработанных запросов на сервисы и времени обработки данных запросов соответственно.

CPN модуль корпоративной сервисной шины (ESB), состоит из трех основных модулей, реализующих функции ESB: управление входным потоком запросов к сервисной шине (ограничение потока, порядок обслуживания очереди запросов и т.д.) моделирует CPN модуль ACCESS (рис. 3,б); процедуры маршрутизации принятого к обслуживанию запроса к серверу поставщика моделирует CPN модуль ROUTE (рис. 3,в), который может реализовывать, например, процедуру оптимального выбора поставщика сервиса и распределения сетевых ресурсов при обслуживании потоков запросов на сервисы; процесс передачи сообщений-запросов и ответов на них по сети и возникающие при этом задержки моделирует CPN модуль NETWORK (рис.4).

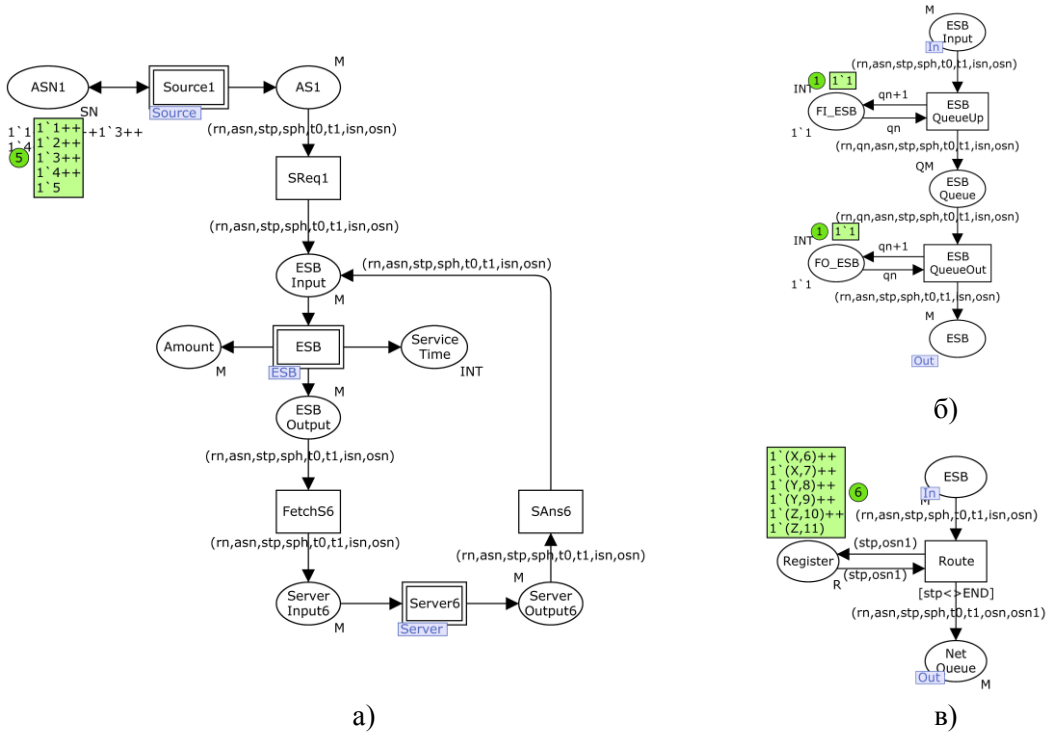


Рис. 3. Обобщенная модель SOA-системы (а), CPN модули управления доступом (б) и маршрутизации сообщений (в)

Модель сервера поставщика сервисов представлена в работе [3], она также включает два CPN модуля, описывающие процедуры обслуживания входной очереди запросов на каждом сервере (модуль SERVER QUEUE) и процесс обработки запросов на сервисы различного типа с учетом возникающих при этом задержек (модуль ALGORYTHM).

Представленная модель процессов сетевого взаимодействия в распределенных системах SOA позволяет проводить анализ таких характеристик, как производительность моделируемой системы, время обслуживания запросов, размеры очередей и т.д. Результаты, полученные в ходе моделирования с использованием предложенного подхода, приведены на рис. 5. Здесь представлены гистограммы, показывающие зависимость производительности системы SOA и среднего времени обработки запроса на сервис при различной пропускной способности базовой ТКС, соединяющей сервера поставщиков. Для получения более наглядных и легко интерпретируемых результатов пропускные способности всех участков сети предполагались одинаковыми и равными от 100 до 500 Мбит/с.

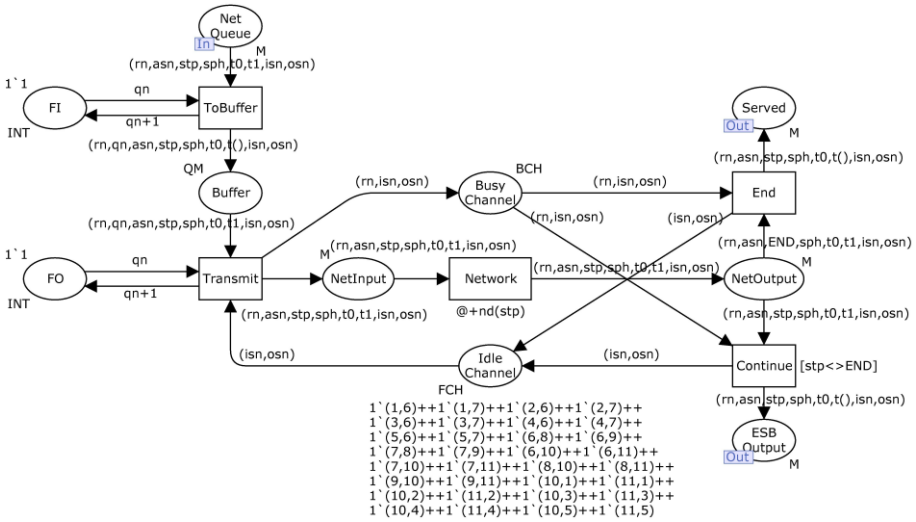
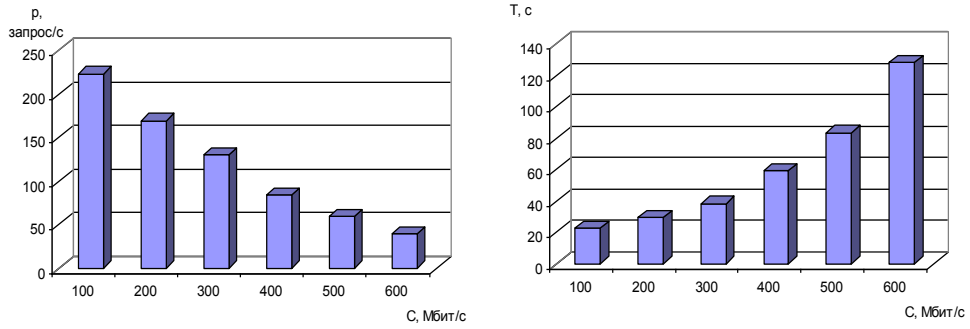


Рис. 4. Модель передачи сообщений по сети



а) б)

Рис.5. Зависимость производительности системы SOA (а) и среднего времени обработки запроса на сервис (б) от пропускной способности базовой ТКС

Таким образом, предлагаемая в работе методика позволяет проводить анализ производительности распределенных систем с сервис-ориантированной архитектурой. В основу методики положена иерархическая модель системы SOA в виде раскрашенной временной сети Петри, которая является достаточно гибкой и легко масштабируемой, что позволяет проводить исследование характеристик SOA-систем на основе аппаратно-программных решений различных производителей с учетом характеристик ТКС, на базе которых организовываются данные системы. Предложенный подход позволяет также проводить анализ эффективности различных технологических решений, разрабатываемых для распределенных систем SOA, с точки зрения из производителдьности и качества предоставляемых сервисов. К данным технологическим решениям можно, в частности, отнести методы управления входным потоком запросов к ESB, маршрутизации сообщений и т.п.

Литература: 1. *Nicolai M. Josuttis*. SOA in Practice: The Art of Distributed System Design (Theory in Practice). – O'Reilly Media, 2007. – 352 p. 2. *Дубова Н.* На пути к SOA // Директор ИС. – 2005. – №8. 3. *Коваленко Т.Н.* Оптимизация распределения сетевых ресурсов в системах с сервис-ориентированной архитектурой // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков, 2009. – Вып.159. – С.7–13. 4. Математичні основи теорії телекомунікаційних систем // В.В. Поповський, С.О. Сабурова, В.Ф. Олійник, Ю.І. Лосєв, Д.В. Агеєв та ін.: За загальною редакцією В.В. Поповського. – Харків: ТОВ «Компанія СМІТ», 2006. – 564 с. 5. *Jensen K.* Coloured Petri nets: basic concepts, analysis methods and practical use. – Berlin, Heidelberg, New York: Springer-Verlag, 1996.

ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ С УЧЕТОМ ТЕХНОЛОГИИ TRAFFIC ENGINEERING ДЛЯ СЕТЕЙ, ПРЕДСТАВЛЕННЫХ СОЕДИНЕННЫМ ГРАФОМ

Вавенко Т.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем,
E-mail: tv_vavenko@mail.ru; тел. 093-162-10-01,

This work is devoted to the problem of routing taking into account the load balancing for networks, which are presented as connecting graph. This paper contains a mathematical formulation of flow model of multipath routing with load balancing of technology Traffic Engineering. We study the telecommunication network which consists of several subnetworks, which are connecting to each other. We identified problems that occur when solving the problem of routing for such networks, identified the causes of it and propose solutions.

На сегодняшний день наблюдается стремительный рост объема информационного трафика, передаваемого через телекоммуникационную сеть (ТКС). Разнородный характер трафика выдвигает более высокие требования по его мультисервисному обслуживанию. В области построения ТКС наиболее перспективным решением является концепция сетей нового поколения (Next Generation Network, NGN) [1], которая создана для обеспечения более широкого набора услуг с гибкими настройками по управлению и персонализации и базируется на технологии IP/MPLS [2]. Это позволяет обеспечить более высокую скорость продвижения IP-пакетов по сети, сократить время обработки маршрутной информации, предоставить возможность организации информационных потоков в каналах ТКС и обеспечить качество обслуживания (Quality of Service, QoS).

Проблема обеспечения требуемого уровня QoS, несмотря на высокий уровень развития современных сетевых технологий, остается достаточно актуальной [3]. Значения показателей QoS, таких как производительность, средняя задержка, джиттер, уровень потерь пакетов и др., зависит от эффективности решения задач управления трафиком, и в первую очередь – задачи маршрутизации, относящейся к задачам сетевого уровня эталонной модели взаимодействия открытых систем (ЭМВОС). Чтобы обеспечить требуемый уровень показателей QoS решение задачи маршрутизации должно носить многопутевой характер и учитывать технологию балансировки нагрузки.

При решении задачи маршрутизации, как правило, используют математические оптимизационные модели. К настоящему моменту времени известно достаточно большое количество потоковых моделей маршрутизации, среди которых наиболее перспективной является модель, которая учитывает технологию балансировки нагрузки (технология Traffic Engineering). В связи с этим она была выбрана для дальнейшего исследования.

Анализ характера решения задачи маршрутизации для сетей, представленных соединенным графом

Выбранная потоковая модель, в рамках которой реализуется многопутевая стратегия маршрутизации с учетом технологии балансировки нагрузки (технология Traffic Engineering), описана в [4].

Пусть структура ТКС описывается с помощью графа $G=(V,E)$, где V – это множество узлов сети, E – множество каналов сети. Для каждой дуги $(i,j)\in E$ характерна ее пропускная способность c_{ij}. Каждому трафику из множества K сопоставлен ряд параметров: пусть d_k, s_k, t_k – интенсивность k-го трафика, узел-источник и узел-получатель соответственно. Управляющей переменной служит величина X_{ij}^k, которая характеризует интенсивность k-го трафика, протекающего в канале $(i,j)\in E$. Вводиться величина α, которая определяет максимальное использования каналов сети:

$$\alpha = \max \frac{\sum_{k \in K} X_{ij}^k}{c_{ij}}, \ (i, j) \in E. \quad (1)$$

В ходе решения задачи маршрутизации минимизируется величина α:

$$\alpha \to \min. \quad (2)$$

Важно не допустить потери пакетов на сетевых узлах и в сети в целом, для этого необходимо обеспечить выполнение условий сохранения потока:

$$\begin{cases} \sum_{j:(i,j)\in E} X_{ij}^k - \sum_{j:(j,i)\in E} X_{ji}^k = 0, \ k \in K, \ i \neq s_k, t_k, \\ \sum_{j:(i,j)\in E} X_{ij}^k - \sum_{j:(j,i)\in E} X_{ji}^k = 1, \ k \in K, \ i = s_k, \\ \sum_{j:(i,j)\in E} X_{ij}^k - \sum_{j:(j,i)\in E} X_{ji}^k = -1, \ k \in K, i = t_k. \end{cases} \quad (3)$$

Кроме этого, необходимо обеспечить выполнение условий предотвращения перегрузки в каналах сети:

$$\sum_{k \in K} d_k X_{ij}^k \le c_{ij}\alpha, \ \ (i, j) \in E. \quad (4)$$

В соответствии с физикой решаемой задачи (1)-(4) на переменные X_{ij}^k и α накладываются следующие ограничения:

$$0 \le X_{ij}^k \le 1, \ \ 0 \le \alpha \le 1. \quad (5)$$

Рассмотренная потоковая модель (1)-(5) представляет собой задачу линейного программирования и описывает процесс маршрутизации с учетом технологии балансировки нагрузки (технология Traffic Engineering). Преимуществом данной модели является то, что распределение трафика при решении задачи маршрутизации носит сбалансированный характер (загружаются все ресурсы сети) за счет рационального выбора путей прохождения трафика через сеть. Это позволяет не допустить перегрузки на узлах сети, что существенно снижает рост средних задержек при передаче пакетов.

Данная модель маршрутизации была проанализирована для различных исходных данных: топологий, величины и характера поступающего в сеть трафика. Установлено, что для некоторых топологий решение задачи маршрутизации в рамках данной модели не обеспечивает рост показателей QoS. Данная ситуация наблюдается и при решении задачи маршрутизации для сети, представленной соединенным графом.

Соединенный граф представляет собой множество подграфов, соединенных между собой некоторым количеством ребер. Соответственно телекоммуникационная сеть, представленная соединенным графом, состоит из подсетей, которые связанны между собой некоторым заданным числом каналов. Данная топология часто используется при построении телекоммуникационных сетей (глобальные сети, объединение локальных сетей и др.). При исследовании было замечено, что в случае, когда пропускная способность каналов, соединяющих подсети, меньше пропускной способности внутри каждой из подсетей, значения показателей QoS внутри подсетей при решении задачи маршрутизации значительно хуже, чем могли бы обеспечить данные подсети. Поэтому возникает задача исследовать и проанализировать выбранную потоковую модель при решении задачи маршрутизации для сетей, представленных соединенным графом, определить причины возникновения проблем и найти пути их устранения.

Пусть телекоммуникационная сеть, а также пропускные способности ее каналов передачи (Мбит/с) имеют вид, представленный на рис.1. Пусть узел 1 – узел-источник, а узел 9 – узел-получатель. Данная топология сети является многосвязной. Пусть в сеть поступает поток некоторой величины, например трафик интенсивностью 15 Мбит/с. Тогда решение задачи маршрутизации, а также значение коэффициента максимальной за-

грузки α в рамках модели (1)-(5) представлено на рис.2 ($\alpha = 0.3750$).

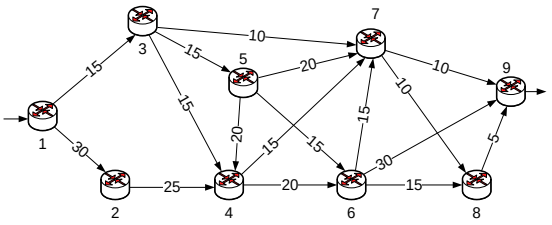


Рис. 1. Структура рассматриваемой телекоммуникационной сети с многосвязной топологией

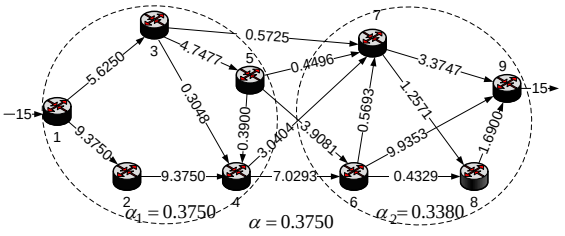


Рис.2. Распределение трафика, а также значения коэффициента загрузки при решении задачи маршрутизации для сети с многосвязной топологией

Разобьем множество всех вершин топологии на два подмножества E_1 и E_2 (рис.2), так что $E_1 = \{1,2,3,4,5\}$ и $E_2 = \{6,7,8,9\}$. Пусть данные подмножества вершин образуют соответствующие подсети. Рассчитаем коэффициенты максимальной загрузки отдельно для каждой подсети α_1, α_2 в рамках ранее полученного решения задачи маршрутизации.

$$\alpha_1 = \max \frac{\sum X_{ij}^k}{c_{ij}},\ (i,j) \in E_1 \quad \text{и} \quad \alpha_2 = \max \frac{\sum X_{ij}^k}{c_{ij}},\ (i,j) \in E_2 . \qquad (6)$$

Значения коэффициентов α_1 и α_2 представлены на рис.2.

Далее сократим количество каналов, соединяющее выбранные подсети, до двух и до одного, получив двусвязную и односвязную топологию соответственно (рис.3).

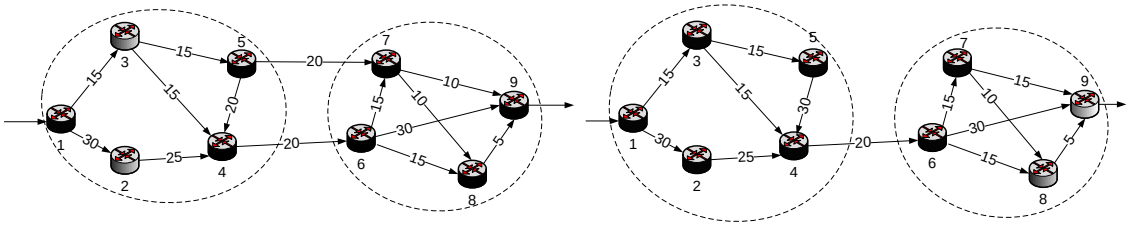


Рис. 3. Рассматриваемая телекоммуникационная сеть с сокращенным количеством каналов между подсетями до двух (а) и до одного (б)

Решим задачу маршрутизации в рамках модели (1)-(5) для полученных сетей, и найдем значения коэффициентов максимальной загрузки α, α_1 и α_2 (табл.1).

Далее в сети рис. 3б) исключим канал 4-6 и рассмотрим две подсети отдельно друг от друга. Значение коэффициента максимальной загрузки отдельно для каждой подсети (соответственно α_1 и α_2) при решении задачи маршрутизации представлено в табл. 1.

Анализируя значения коэффициента максимальной загрузки для первой подсети (α_1) из табл.1, заметим, что при решении задачи маршрутизации значение данного коэффициента для случая двусвязной и односвязной сети ($\alpha_1 = 0.4286$ и $\alpha_1 = 0.4991$ соответственно) больше, чем для случая многосвязной сети и подсети отдельно ($\alpha_1 = 0.3750$ и $\alpha_1 = 0.3750$ соответственно). Аналогичная ситуация наблюдается и со значением коэффициента максимальной загрузки для второй подсети: его значение для случая двусвязной и односвязной сети ($\alpha_1 = 0.4286$ и $\alpha_1 = 0.4898$ соответственно) больше, чем для случая многосвязной сети и второй подсети отдельно ($\alpha_1 = 0.3380$ и $\alpha_1 = 0.3333$ соответственно). Это говорит о том, что значения показателей QoS внутри рассматриваемых подсетей в рамках решения задачи маршрутизации для случая сети с односвязной и двусвязной топологией

хуже, чем для случая с многосвязной топологией и для подсети отдельно. Это происходит из-за присутствия в сети «узкого места» - участка с меньшей пропускной способностью (для двухсвязной сети – это каналы 4-6 и 5-7 (рис.3а); для односвязной сети – это канал 4-6 (рис.3б)). Величина загрузки в этом участке получает наибольшее значение среди значений загрузки на других участках сети ($\alpha = 0.7500$). А это, в свою очередь, препятствует минимизации величины загрузки каналов в подсетях, приводя к их росту. Тем самым ухудшая значения показателей QoS.

Табл.1. Значение коэффициента максимальной загрузки для разных топологий

Значения коэффициента / Топология	α	α_1	α_2
Многосвязная	0.3750	0.3750	0.3380
Двусвязная	0.4286	0.4286	0.4286
Односвязная	0.7500	0.4991	0.4898
Первая подсеть отдельно	-	0.3750	-
Вторая подсеть отдельно	-	-	0.3333

Чтобы предотвратить данную проблему рекомендуется переходить от линейной целевой функции в задаче маршрутизации к квадратичной целевой функции. Это позволит получить более сбалансированное решение, тем самым улучшив значения показателей QoS. Кроме этого, для сетей, представленных соединенным графом, значения показателей QoS будут выше, если решать задачу маршрутизации отдельно для каждой из подсетей.

Выводы

В работе рассматриваются особенности моделирования процессов маршрутизации в рамках модели, которая учитывает технологию балансировки нагрузки (технология Traffic Engineering). Преимущество данной модели заключается в том, что распределение трафика при решении задачи маршрутизации носит сбалансированный характер, что улучшает значение показателей QoS. Однако в результате проведенного исследования был установлен недостаток модели, который состоит в том, что для некоторых топологий значения показателей QoS ухудшаются, в частности и для сетей, представленных соединенным графом. Замечено, что в случае, когда пропускная способность каналов, соединяющих подсети, меньше пропускной способности внутри каждой из подсетей, значения показателей QoS внутри подсетей при решении задачи маршрутизации ниже, чем могли бы обеспечить данные подсети. Это происходит из-за того, что в сети существует «узкое место», т.е. участок с меньшей пропускной способностью. Значение коэффициента загрузки в этом участке достигает наибольшего своего значения и этим препятствует минимизации коэффициента загрузки каналов в подсетях, приводя к их росту и ухудшая значения показателей QoS. Для устранения данного недостатка предложено использовать квадратичную целевую функцию, а также решать задачу маршрутизации отдельно для каждой из подсетей.

Литература:

1. NGN: принципы построения и организации / под ред. Ю.Н.Чернышова.–М.:Эко-Трендз,2008.– 400с.: илл.

2. Y.2001. ITU-T. Recommendation Y.2001: General overview of NGN [Text]/ITU-T.- Geneva, 2004. – 18p.

3. Вегенша, Ш. Качество обслуживания в сетях IP.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 368 с.

4. Y Wang Y., Wang Z. Explicit routing algorithms for Internet Traffic Engineering // Proc. of 8th International Conference on Computer Communications and Networks. Paris, 1999. – P. 582-588.

МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Килячков К.П.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Телекоммуникационных систем, тел. (057)702-13-20
E-mail: kilja@meta.ua

The work discussed the relevance of the use of accessible assessments in telecommunications networks. To receive them calculated the most well-known estimates, and given the comparative data.

Общая характеристика

Современные телекоммуникационные системы характеризуются огромным количеством входящих в них компонент и сложностью математического и программного обеспечения. Повышать эффективность таких систем, можно не только изменяя качество компонент, но и повышая надежность самих систем путем подбора наилучшей структуры. Одной из главных задач исследований в области надежности телекоммуникационных систем - дать процедуру инженерного синтеза этих систем, чтобы повысить возможность проектировать системы, для которых надежность есть наиболее важный аспект. Для разработки сети под определенные задачи актуально получить оценочные характеристики сети При проектировании телекоммуникационных сетей, желательно разработать методы проектирования, которые имея на входе различные характеристики компонентов сети (в том числе и характеристики надежности) и критерии синтеза сети, на выходе дают оптимальную топологию сети. Теория надежности основана на некоторых фактах комбинаторики и теории вероятности. При подробном рассмотрении обнаруживается тесная связь с такими разделами математики, как дискретная оптимизация, теория перколяции, теория случайных графов, теория гиперграфов (семейств конечных множеств), теория матроидов, и т.д. При анализе надежности систем обычно применяются дискретные вероятностные модели надежности из-за неспособности как моделирования механизма ошибок компонент системы (параметры повреждения компонент оцениваются на опытных данных), так и трудности вычисления надежности систем.

Существует два общих основных аспекта теории оценок надежности систем:

1. *Аспект эффективности* - вычисления оценок должно требовать меньших усилий, чем вычисление самой надежности;

2. *Аспект точности* - оценки должны обеспечивать "достаточно хорошее" приближение.

Эти аспекты находятся в известном противопоставлении, поэтому желания быстрого вычисления и высокой точности привели к большому количеству методов оценки характеристик надежности различных монотонных систем.

Необходимость использования оценок

Определение надежности сложных систем, т. е. для которых не существует ограниченного набора математических моделей.

В большинстве моделей компоненты системы могут принимать одно из двух состояний: работоспособное состояние или состояние отказа. Любое из этих состояний данной компоненты есть случайное событие, которое не зависит от состояния других компонент. Проблема анализа надежности системы состоит в следующем: при заданных вероятностях того, что каждая компонента системы работает, вычислить меру надежности системы.

Простейшая модель с двумя состояниями достаточна для рассмотрения мер связности телекоммуникационной сети. В этой модели вероятность *p(e)* исправного состояния компоненты e имеет одну из нескольких возможных интерпретаций. В этом случае состояние компоненты чередуется между работоспособным и отказавшим (и подвергаю-

щимся ремонту). Определение надежности компоненты не влечет за собой рассмотрения ремонта.

Ключевая роль достижимых(предельно возможных) оценок в классе всевозможных оценок характеристик надежности сети состоит в том, что на основе их обобщения возможно построение новых, вообще говоря, уже не достижимых оценок (т.е. достижимые оценки являются порождающими, материнскими оценками).

В контексте достижимых оценок становится понятным и подчиненная роль

-Преобразований, не меняющих значение надежности;

-Преобразований, увеличивающих (уменьшающих) надежность;

-Эффективной вычислимости надежности для некоторых классов рассматриваемых дискретных структур (упаковок, последовательно-параллельных структур, прямых сумм матроидов, полных графов, полных двудольных графов, ациклических орграфов и т.д.). Конструкция структур с экстремальным значением надежности, обычно, связана с преобразованиями , так как последовательность таких преобразований может приводить к экстремальной конструкции. Кроме того, возможна "своевременная" остановка процесса преобразований, когда рассматриваемая структура преобразовалась в структуру, надежность которой может быть вычислена эффективно.

Случайная монотонная система - одна из простейших моделей надежности составных технических систем, в частности, телекоммуникационных сетей. В этой модели предполагается, что работоспособность системы определяется исключительно знанием того, какие компоненты работают (отказали). Надежность системы есть вероятность того, что функционируют все элементы какого-либо набора компонент из указанного семейства таких наборов (математически такое семейство есть семейство попарно не вложимых множеств (клаттер)). Клаттером является совершенная биниальная иерархическая сеть более низкого ранга. Существует целый ряд оценок. Особое место среди них занимают оценки надежности монотонной системы общего вида (с произвольным клаттером и произвольной надежностью компонент).

В свою очередь среди оценок общей монотонной системы ключевое место занимают оценки, которые представляют собой аналитические функции от каких-либо параметров монотонной системы и точные на некоторых классах монотонных систем. Иными словами это достижимые - наилучшие возможные (в терминах используемых параметров) оценки.

Основные виды оценок

Вычисление всех основных характеристик надежности телекоммуникационных сетей - трудная алгоритмическая проблема, что свидетельствует о целесообразности применения их оценок вместо точного вычисления. Существует большое количество различных оценок, изучим их эффективность и пригодность для использования в телекоммуникационной сети. Основные перечислим:

Оценки включения-исключения или оценки Бонферрони получаются из формулы включения-исключения . Отсечением суммы после $J < \kappa$ членов мы получаем верхнюю оценку, когда J - нечетно, и нижнюю оценку, когда J - четно. Весьма положительна простота оценок, которые могут быть рассчитаны в кратчайшее время при сравнительно небольшом количестве членов. Отметим, что оценки Бонферрони требуют знания всех членов клаттера, это вносит значительные коррективы в сферу их применения. Примем что S сумма членов системы, тогда, как A член системы, а p его достижимая надежность.

$$\ldots, S1 - S2 + S3 - S4, S1 - S2 \le R(\mu; p) \le S1, S1 - S2 + S3, \ldots$$

$$St = \sum_{i1 \lhd \ldots \lhd it} P(A_{i_1} \ldots A_{i_t}; p).$$

Упаковочные оценки , основаны на монотонности меры *P,* статистической независимости монотонных событий и соотношении двойственности. Обе оценки, достижимы. С помощью подстановки в различные части равенства, мы можем вычислить нижнюю и верхнюю границы надежности монотонной системы в терминах упаковки членов двойственного клаттера. Достижимость нижней оценки соответствует случаю, когда клаттер μ - упаковка. Достижимость верхней оценки соответствует случаю, когда двойственный клаттер упаковка.

$$R(\mu; p) = 1 - \prod_{j=1}^{t} (1 - p^{A_{ij}}),$$

Недостаточная точность оценок вызывает значительные нарекания. Более подробно остановимся на представителях класса развязочных оценок: развязочные оценки основаны на преобразовании развязывания и том факте, что оно не уменьшает надежность монотонной системы.

Оценки Эзари - Прошана естественно назвать *развязочно-упаковочными* оценками. Это наихудшие развязочные оценки по показателю точности. Поскольку оценки Эзари - Прошана достижимые, то для построения более точных развязочных оценок привлекаются дополнительные понятия. Внимательное рассмотрение оценок Оксли -Уэлша привело к новым, разностно-развязочным оценкам, но они применимы только для изотропного случая и представляют больше математический, нежели практический интерес. Единственной альтернативой разностно-развязочным оценкам до настоящего времени были упаковочные оценки.

Разностно-развязочные оценки являются передовым методом для эффективного оценивания надежности, как монотонных систем общего вида, так и систем с сетевой структурой для {s, t}-надежности и K-терминальной надежности в случае малого \K\. Известно, что для всех известных оценок сравнивая "хорошую" (по точности) и "плохую" оценки, всегда можно построить пример, когда "хорошая" оценка будет хуже "плохой". Поэтому сравнивая работающие кластеры сетей, не оптимизированные для использования сколь угодно эффективных оценок, можно определить слабые места на основании данных работающей топологии. Высокая точность оценок относительно уже известных, перевешивает значительную сложность при исследовании сложных систем с большим количеством членов.

Рассмотрим выбранные оценки на модели сети которая является случайной монотонной системой и представляет собой универсальную модель для расчета параметров надежности системы.

Литература

1. Кривулец В.Г. Об оценке оценок Эзари - Прошана в задачах анализа структурной надёжности сетей связи. *LV научная сессия, посвященная дню радио "Радиотехника, электроника и связь на рубеже тысячелетия". Сб. трудов.* Москва: РНТОРЭС им. А.С. Попова, 2000,стр. 272-275.

2. Кривулец В.Г. Разностно-развязочные оценки надежности монотонной структуры. *XLIV научная конференция МФТИ, посвященная 50-летию создания МФТИ, Сб. трудов, часть I.* Москва-Долгопрудный, 2001, стр. 17.

3. Полесский В.П. Оценки вероятности связности случайного графа. *Проблемы Передачи Информации,* 1990, том 26.

4. Филин Б.П. Методы анализа структурной надёжности сетей связи. М.: Радио и связь, 1988.

ИСПОЛЬЗОВАНИЕ ПОТОКОВЫХ АГЕНТОВ ДЛЯ МОНИТОРИНГА И УПРАВЛЕНИЯ КАЧЕСТВОМ ПОТОКОВОГО ВИДЕО В СЕТЯХ WIMAX

Поповский В. В., Кобрин А. В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем, тел. (057) 702-55-92)
e-mail: tkc@kture.kharkov.ua, факс: (057) 702-13-20

Feedback adaptation has been the basis for many media streaming schemes, whereby the media being sent is adapted in real time according to feedback information about the observed network state and application state. Central to the success of such adaptive schemes, the feedback must: 1) arrive in a timely manner and 2) carry enough information to effect useful adaptation. I show how the introduction of a streaming agent (SA) at the junction of the wired and wireless network can be used to provide useful information in a timely manner for media adaptation

При передаче мультимедийной информации по комбинированным сетям с учетом различных механизмов распространения с различными технологиями, важным является выполнение требований по качеству предоставления мультимедийной информации пользователю.

При этом важными являются такие характеристики: задержка, число потерянных и поврежденных пакетов. Как показывает практика наибольшие потери качественных характеристик происходит на границах операторских сетей и сетей с различными механизмами распространения.

Возникает необходимость установки соответствующих агентов, обеспечивающих мониторинг на том или ином промежутке сети. Вместе с тем от числа и места этих агентов существенно зависит качество мониторинга.

Потоковый агент это агент, который находится на базовой станции на пересечении проводной и беспроводной сети. Агент просматривает и распознает поток, исследуя заголовки RTP. Агент периодически посылает статистические и своевременные обратные сообщения на отправляющий сервер. Статистические обратные связи помогают отправителю проследить проводное состояние сети, что существенно для выполнения надлежащего контроля над перегрузками. С другой стороны, потоковый агент отправляет своевременные обратные сообщения, такие как подтверждение пакетов (ACKs), что говорит отправителю о прибытии каждого пакета к агенту корректно и вовремя.

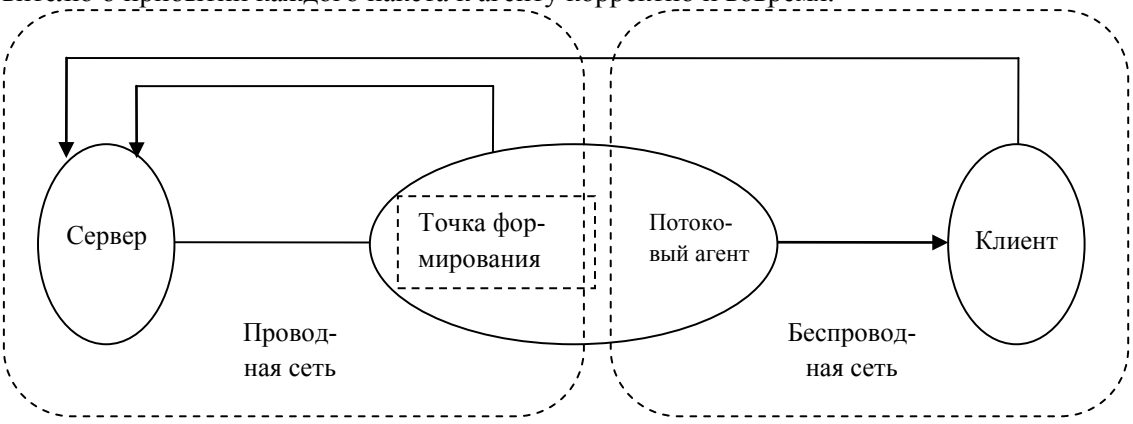


Рис. 1 - Использование потокового агента

Точка формирования находится перед потоковым агентом и ограничивает объем отправляемых сообщений, чтобы он не был больше чем полоса пропускания беспроводной сети, храня пакеты, ожидающие фрагментации и передачи на более низкий уровень. Если состояние беспроводной сети плохое число повторных передач будет расти, застав-

ляя увеличиваться очередь пакетов. Точка формирования реагирует на заполненность очереди, отбрасывая пакеты до прибытия их к агенту.

Преимущество использования потоковых агентов: во-первых, агенты помогает определить место потери пакета, что обеспечивает адекватный контроль над перегрузками; во-вторых, у мобильного клиента типично есть серьезное ограничение мощности из-за ограниченного времени работы аккумулятора и частая отправка служебных сообщений клиентом, нежелательна, так как отправка данных потребляет больше мощности, чем прием; в-третьих, в современных беспроводных сетях типично большая односторонняя задержка, порядка 100 мс, без учета повторных передач, и если потеря произошла в проводной сети повторная передача, может быть выполнена без использования беспроводной сети. Кроме того, можно балансировать между качеством беспроводной связи и задержкой связи, определяя число повторных передач канального уровня во время установки сессии.

Одна из проблем интерактивных медиа потоков в современных сетях это джиттер задержки, который вводится сетевым оборудованием и протоколами. Мы верим, что в будущем будет увеличена пропускная способность и вычислительная мощность компьютеров, но джитер останется проблемой, которую нужно решить. Первая причина этого то, что увеличение полосы пропускания сетевого оборудования будет происходить параллельно с увеличением требований пользователей к качеству предоставления сервисов. Вторая причина, это природа используемых протоколов, таких как TCP протокол, который для каждого пакета предоставляет различную задержку.

Для оптимизации джиттера предложено установить на узел потокового агента систему адаптации джиттера, которая с помощью фильтра Калмана оценивает состояние системы.

За оптимизационные критерии выбраны $\omega_1, \omega_2, \omega_3$, с помощью которых рассчитывается оптимальный буфер $M_{RCV,d}$.

ω_1 – размер буфера должен быть близок к оптимальному значению, минимизация $|M_{RCV} - M_{RCV,d}|$.

ω_2 – скорость воспроизведения должна быть как можно ближе к корректной скорости воспроизведения, минимизация $|M_{PLR} - M_{SNDR}|$.

ω_3 – изменение скорости воспроизведения должно происходить как можно медленнее, минимизация $|\frac{drPLR}{dt}|$.

Все три требования не могут быть удовлетворены в одно и то же время, из-за взаимных конфликтов. Поэтому одна из целей работы, является дать пользователю возможность комбинировать их выполнение.

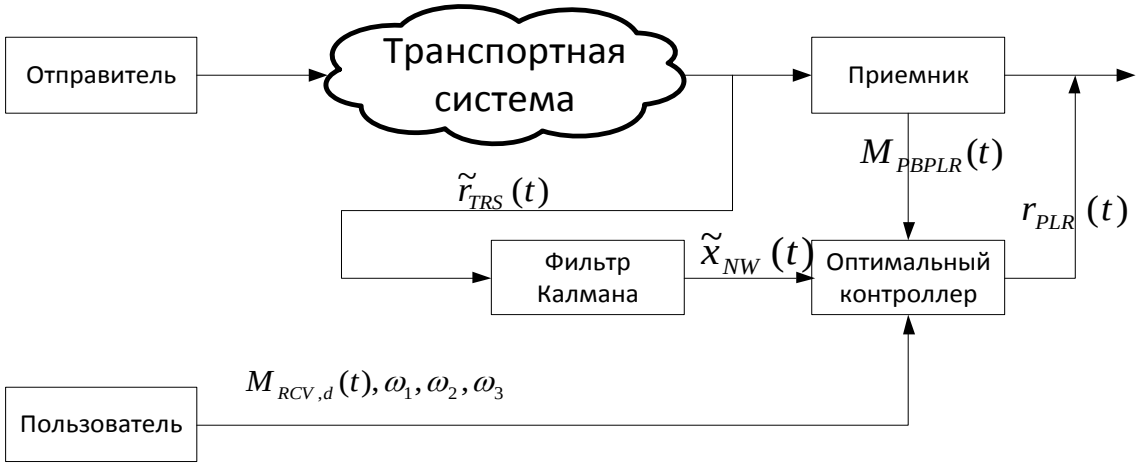


Рис. 2 - Система адаптации джиттера

WiMAX — это сеть беспроводной передачи множеству пользователей различного вида информации: голоса, потокового видео, аудио, обеспечения доступа в Интернет с гарантированным качеством, и др.

Цель технологии WiMAX заключается в том, чтобы предоставить универсальный беспроводный доступ для широкого спектра устройств (рабочих станций, бытовой техники "умного дома", портативных устройств и мобильных телефонов) и их логического объединения - локальных сетей. Надо отметить, что технология имеет ряд преимуществ.

По сравнению с проводными (xDSL, T1), беспроводными или спутниковыми системами сети WiMAX должны позволить операторам и сервис-провайдерам экономически эффективно охватить не только новых потенциальных пользователей, но и расширить спектр информационных и коммуникационных технологий для пользователей, уже имеющих фиксированный (стационарный) доступ.

Стандарт объединяет в себя технологии уровня оператора связи (для объединения многих подсетей и предоставления им доступа к Интернет), а также технологии "последней мили" (конечного отрезка от точки входа в сеть провайдера до компьютера пользователя), что создает универсальность и, как следствие, повышает надёжность системы.

Беспроводные технологии более гибки и, как следствие, более просты в развёртывании, так как по мере необходимости могут масштабироваться.

Простота установки как фактор уменьшения затрат на развертывание сетей в развивающихся странах, малонаселённых или удалённых районах.

Дальность охвата является существенным показателем системы радиосвязи. На данный момент большинство беспроводных технологий широкополосной передачи данных требуют наличия прямой видимости между объектами сети. WiMAX благодаря использованию технологии OFDM создает зоны покрытия в условиях отсутствия прямой видимости от клиентского оборудования до базовой станции, при этом расстояния исчисляются километрами.

Технология WiMAX изначально содержит в себе протокол IP, что позволяет легко и прозрачно интегрировать её в локальные сети.

Технология WiMAX подходит для фиксированных, перемещаемых и подвижных объектов сетей на единой инфраструктуре.

Укрупненно WiMAX сеть состоит из следующих логических объектов:

1) абонентские станции.

2) ASN (Access Service Network) — сеть доступа.

3) CSN (Connectivity Service Network) — сеть обеспечения услуг.

Каждый объект может быть реализован в одном физическом модуле или в нескольких.

ASN-GW, шлюз радио подсети — это логический элемент сети, выполняющий агрегирование (объединение) сигнальных функций, а также, если необходимо, маршрутизацию потоков данных пользователей. ASN-GW может быть связан с другими ASN-GW для обеспечения резервирования и балансировки нагрузки.

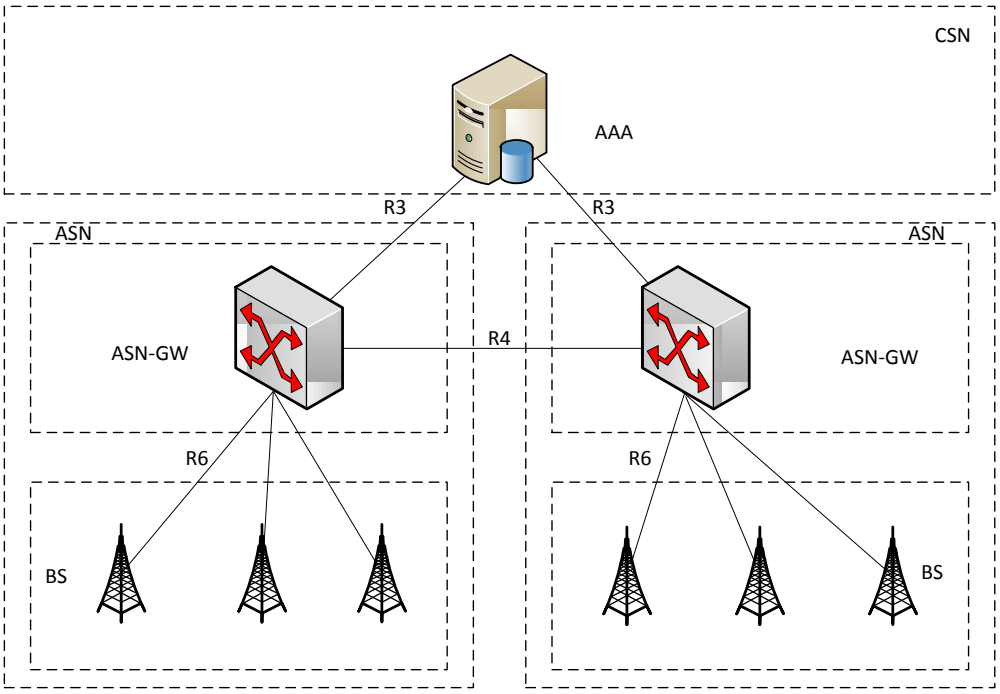


Рис. 3 - Расположение узла ASN-GW в сети Wimax с обозначением интерфейсов

Являясь центральным узлом сети, ASN-GW берёт на себя львиную долю всех функций:

- Маршрутизация
- Управление QoS
- Аккаунтинг
- DHCP
- VPN
- Обеспечение связи с AAA-сервером и подключения MS (мобильная станция) без аутентификации
- Управление текущими сессиями и хранение данных о подключенных MS
- Управление радиоресурсами
- Управление режимами работы мобильной станции (sleep, idle-mode)
- Трассировка интерфейсов и параметров оборудования.

Предложено в роли узла потокового агента использовать узел ASN-GW, в связи с тем, что узел расположен на уровне доступа и имеет широкий функционал, включая работу с потоками.

В течение последний лет увеличился размер передач интерактивных медиа потоков поверх различных сетей и протоколов. И есть несколько причин, почему эта тенденция будет продолжаться в будущем:

• IP телефония становиться домашним инструментом

• Согласно исследованиям компании Nokia в будущем все речевые сообщения будут передаться через беспроводные сети

• Видео камеры также становятся распространенным инструментом общения

• Использование мультимедийных игр и т д

В связи увеличения размера передач интерактивных медиа потоков поверх различных сетей и протоколов актуальность использования потоковых агентов будет расти.

СТОХАСТИЧЕСКАЯ СОТОВАЯ ПОДВИЖНАЯ СВЯЗЬ ИЛИ ЗАДАЧА О ПРЫГАЮЩЕЙ ОБЕЗЬЯНЕ И ЕЕ ПРИМЕНЕНИЯ В ТЕОРИИ СВЯЗИ.

Луценко[1] В.И., Лю Цзяньфен[2], Бабаков М.Ф.[2], Зарицкий В.И.[3]
[1]Институт радиофизики и электроники им. А.Я. Усикова НАН Украины,
61085, Украина, г. Харьков, ул. Ак. Проскуры, 12
[2]Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ», 61085, Украина, г. Харьков, ул. Чкалова, 17,
[3]Академия наук «Прикладная радиоэлектроника»,
проспек Ленина, 14, г. Харьков, 61166, Украина.
тел.: 057-702-17-35, E-mail: enneas@yandex.ru

Possibility of construction of cellular systems with use as virtual base station of equipment of the mobile subscriber is considered. Statistical modeling for an estimation of possibility of a covering of the set area is spent at such principle of the organization of communication.

Введение. Интенсивные поиски и исследования в области разработки систем эффективно использующих выделенный участок спектра частот и высокой пропускной способностью, которые были бы в состоянии обслуживать большое количество абонентов, начались на рубеже 60-70-х годов и привели к созданию территориальных систем с малыми зонами обслуживания, получивших название сотовых систем радиосвязи с подвижными объектами. До недавнего времени при разработке сотовых систем связи с подвижными объектами исходили из детерминистской постановки задачи. Суть ее состояла в том, что вся зона обслуживания делилась на области, обычно шестигранной формы, так называемые соты, в центре которых размещались базовые станции. Небольшая мощность передатчиков в системах малой зоны ответственности (МЗО) и, соответственно, небольшой радиус их действия, допускает организацию повторения частот приема-передачи через 1…2 зоны. Это позволяет реализовать основное достоинство сотовой системы - обеспечить высококачественную радиосвязь большого количества подвижных абонентов (ПА) в условиях ограниченного частотного диапазона.

В последнее время в ряде работ была предложена принципиально иная концепция построения системы связи с подвижными объектами, в соответствии с которой в процесс формирования общего информационного потока вовлекаются отдельные абоненты. Их система связи используется в качестве локальной базовой станции, которой выделяются частоты или коды (при использовании псевдошумового сигнала) в зависимости от их местоположения [1, 2]. Такой подход к организации сотовой связи, с использованием в качестве базовых не станций, располагающихся в фиксированных точках пространства, а стохастических квазибазовых станций представляется достаточно перспективным для снижения затрат на покрытие заданной области пространства связью и рассмотрен в настоящей работе.

Модель псевдосотовой системы. Теоретическая постановка задачи. Пусть в некоторой точке пространства с координатой $\vec{R}_0$ на ветке дерева находится обезьяна. Задана плотность распределения координат расстояний между ветвями $p(\Delta x, \Delta y, \Delta z) \to p(\rho, \theta, \beta)$. Необходимо определить вероятность того, что обезьяне удастся прыжками переместиться в область пространства Θ, ограниченную поверхностью $S(\vec{R})$. Обезьяна может осуществлять прыжки длиной не более l_0.

Физическая интерпретация модели. Одномерный случай. По автобану движется поток автомобилей, плотность распределения расстояний между которыми $p(x)$. Каждый автомобиль принимает информацию от соседнего и ретранслирует ее дальше, добавив в общий поток свою информацию. Дальность действия автомобильных систем связи не превышает l_0. Необходимо оценить вероятность передачи информации по автобану на расстояние L_0. Впервые идея организации такой самоорганизующейся мультиплексной системы связи между транспортными средствами на автобане, которую

назвали CARs-to-CARs система связи, была высказана авторами работ [1, 2]. Ключевая идея построения CARs-to-CARs системы [1, 2] состоит в том, чтобы в системе с кодовым распределением каналов код для каждого транспортного средства ассоциировать не с транспортным средством, а с его текущим положением на автобане. Это позволяет в передаваемом информационном потоке иметь данные не только о информационных сообщениях передаваемых автомоблями, но и о местоположении, а значит и о распределении автомобилей по автобану. В нашей постановке задачи представляет интерес оценка вероятности установления связи на заданное расстояние в зависимости от функции распределения автомобилей по автобану. При этом каждый из автомобилей выступает в качестве виртуальной базовой станции системы подвижносй сотоывой связи.

Двумерный случай. На морской акватории расположены рыболовецкие суда, концентрация которых наиболее велика в районах зон промысла. Плотность распределения их по координатам описывается функцией $p(\Delta x, \Delta y)$. Береговая черта описывается функцией $y(x)$. На берегу в точках с известными координатами $\vec{R}_i$ находятся диспетчерские станции, хотя бы на одну из которых должна быть передана информация с судов. Передача информации осуществляется путем ее ретрансляции судами, расстояние между которыми меньше дальности связи l_0. Необходимо оценить вероятность передачи береговым службам информации с судна, находящегося на удалении R_0.

Аналогичная ситуация имеет место, когда в системе сотов связи ипользуют некоторых из абонентов телефонной сети в качестве псевдобазовых станций. Поступившая на них информация от других абонентов ретранслируется дальше на частотах либо с использованием ортогональных кодов, как это было в одномерном случае [1, 2]. При этом в общий поток дополнительно добавляется собственная информация. При ретрансляции информация передается на частоте, либо с использованием кода, которые задаются местоположением ретранслирующего объекта. Он при этом выполняет функции виртуальной базовой станциии.

Трехмерный случай – рассматривает ситуацию установления связи между летательным аппаратом, находящимся в точке пространства с координатами $\vec{R}_0$ и i-м диспетчерским пунктом, находящимся на земной поверхности в точке с координатами $\vec{R}_i$. Она устанавливается с использованием в качестве ретрансляторов (виртуальных базовых станций) других летательных аппаратов, находящихся в зоне действия его передатчика. Предполагается известной плотность распределения расстояний между летательными аппаратами в пространстве $p(\Delta x, \Delta y, \Delta z)$ и существуют ограничения на дальность действия их радиостанций l_0. При этом сообщение ретранслируется на диспетчерский пункт через j ближайших летательных аппаратов, каждый из которых добавляет в общий поток свою информацию. Для выбора кода передачи собственной информации используются данные о местоположении летательного аппарата, полученные с использованием систем глобальной навигации. При этом каждой точке пространства соответствует свое кодовое слово. Необходимо оценить вероятность установления связи между летательным аппаратом и диспетчерским пунктом.

Оценка вероятности попадания обезьяны в заданную точку пространства. Одномерный случай. Необходимо оценить вероятность того, что обезьяне удастся за $j \in (1, \infty)$ прыжков покрыть расстояние L_0, причем расстояние, покрываемое каждым из прыжков, будет меньше l_0. Эти условия можно записать в виде соотношения:

$$\zeta_{j0} = \sum_{j=1}^{j_0} l_j \geq L_0 \cup l_j \leq l_0,\ j_0 \in (1, \infty) \qquad (1)$$

Задача сводится к нахождению вероятности того, что при количестве прыжков j_0, являющемся случайной величиной удастся покрыть расстояние L_0 при этом каждый из них будет короче l_0.

Применительно к задаче организации одномерной квазисотовой связи между автомобилями на автобане эти условия означают, что для передачи информации с автомобиля на расстояние L_0 необходимо выполнение двух условий:

1. Сумма расстояний между k автомобилями должна быть больше L_0, при $j \in (1, \infty)$

2. Расстояние между соседними автомобилями должно быть меньше l_0.

Двумерный случай. Необходимо оценить вероятность покрытия за $j \in (1, \infty)$ прыжков расстояния L_0. Это означает, что обезьяна должна выпрыгнуть из центра круга на расстояние большее L_0, при этом радиус вектор $\dot{R}_j = R_j \exp i\varphi_j$ будет иметь модуль R_j больший L_0, в то время, как каждый из прыжков будет короче l_0.

Применительно к организации псевдосотовой, например, мобильной телефонной связи это означает, что для передачи информации аюонента на расстояние L_0 необходимо, чтобы абонент, которого дотигло сообщение находился на расстоянии от исходного абонента далее, чем L_0, при этом расстояние между соседними абонентами болжно быть меньше дальности гарантированной связи l_0:

Результаты машинного эксперимента. Для оценки размеров зоны покрытия сотовой связью при использовании стохастического принципа использования в качестве квазибазовой станции аппаратуры абонента был проведен статистический эксперимнт. Моделировалось пространственное распределение абонентов, и оценивалась возможность, используя их аппаратуру, установить связь с базовыми станциями, находящимися на расстоянии L_0. Пространственное распределение расстояний полагалось релеевским, а в двухмерном случае плотность распределения направлений полагалась равномерной. На рис. 1 показаны функции распределения покрываемых расстояний. Величины l_0 и L_0 нормированы относительно среднеквадратичного значения плотности распределения σ. Функции распределения - рис. 1а, в представлены в масштабе лианеризирующем закон распределения Релея. Видно, что как в одномерном случае, так и двухмерном, функции распределения вероятности установления связи удовлетворительно описываются экспоненциальной моделью. Увеличение дальности действия аппаратуры абонента, которая используется для ретрансляции сигналов других абонентов, т.е. в качестве виртуальной базовой станции приводит к резкому возрастанию зоны покрытия (рис. 1 б, г). Наблюдается сильная зависимость зоны покрытия, как от нормированной на среднеквадратичное значение расстояний между станциями распределение дальности связи l_0/σ, так и от заданной вероятности установления связи P. При дальности действия аппаратуры подвижного абонента в несколько раз превышающей расстояние между абонентами удается существенно расширить зону покрытия.

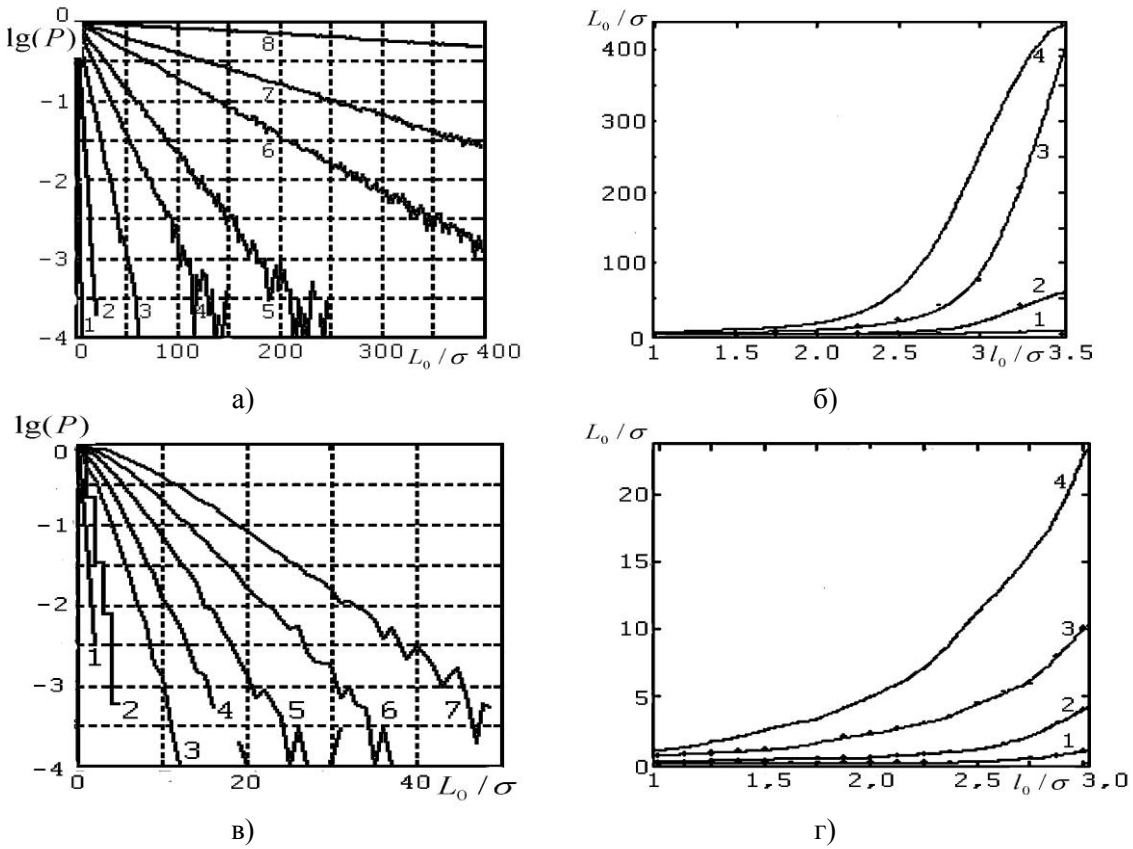


Рис. 1 Статистические характеристики покрываемой зоны: а, б – одномерный случай; в, г – двумерный случай; а, в – вероятность покрытия зоны L_0; а - 1 - l_0=1, 2 - l_0=1.5, 3 - l_0=2, 4 - l_0=2.3, 5 - l_0=2.5, 6 - l_0=2.8, 7 - l_0=3, 8 - l_0=3.5; в - 1 - l_0=1, 2 - l_0=2, 3 - l_0=2.5, 4 - l_0=3, 5 - l_0=3.5, 6 - l_0=4, 7 - l_0=4.5, 8 - l_0=5; б, г - 1 - P=0.99; 2 - P=0.9; 3 - P=0.5; 4 - P=0.1.

Заключение. Рассмотрен новый принцип организации сотовой связи, использующий для передачи сообщений, находящихся в зоне действия абонентов. Их аппаратура используется в качестве псевдобазовой станции, частотное или кодовое распределение каналов которой определяется ее местоположением. Проведенное рассмотрение позволило установить, что использование в качестве квазибазовых станций аппаратуры абонентов позволяет организовать стохастическую сотовую связь и обеспечить существенное увеличение зоны покрытия связью без привлечения дополнительных средств.

Литература:

1. Konstantin Lukin, Valery Scherbakov, Vladimyr Konovalov, Ryan Breed. Dedicated Short-Range Communication System for Vehicle-to-Vehicle Data Transmission on the Basis of Chaotic Waveform codes (DSRC-VVDT). // Proceedings of 16 International Conference on Microwaves, Radar and Wireless Communications – MIKON-2006, Krakow, Poland, May 22 – 24, 2006, Vol. 1, pp. 442 – 445.

2. К.А. Лукин, В.Е. Щербаков, В.М. Коновалов, Д.С. Брид. Метод построения самоорганизующейся системы связи между транспортными средствами на автобане. Радіоелектронні і комп'ютерні системи, №6 (25), 2007, Харків «ХАЇ», с. 238 – 244.

МЕТОД НЕЙРО-НЕЧІТКОГО АКТИВНОГО УПРАВЛІННЯ ПАКЕТНИМИ ЧЕРГАМИ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Польщиков К.О.[1], Здоренко Ю.М.[2]
[1]Донбаська державна машинобудівна академія
84313, Краматорськ, вул. Шкадінова, 72, каф. комп'ютерних інформаційних технологій,
тел. 0503022140, E-mail: konspol@rambler.ru;
[2]Військовий інститут телекомунікацій та інформатизації НТУУ «КПІ»
36000, Полтава, вул. Зіньківська, 44, тел. 0660165793, E-mail: zdor@front.ru

In this work article a method of active control the packet queue of router output port of telecommunication network is offered, which in the process of decision-making about the done early casting-out packet foresees the use of the fuzzy neural systems. Application of method allows to decrease probability of casting-out of packets and middle delay of packets in a router.

1. Обґрунтування актуальності досліджень

Для сучасних телекомунікаційних мереж з комутацією пакетів, характерними явищами є перевантаження, що викликані зростанням інтенсивності трафіку в цих мережах в умовах їхньої обмеженої пропускної здатності. Без реалізації ефективної боротьби з мережними перевантаженнями неможливо забезпечити якісне обслуговування користувачів. Для боротьби з перевантаженнями використовують велику кількість методів, серед яких важливе місце займають методи управління чергами пакетів в маршрутизаторах. Суть активного управління пакетними чергами є у тому, щоб запобігати виникненню перевантажень шляхом відкидання певної частини пакетів, що потрапляють до маршрутизатора до моменту заповнення відповідної канальної черги. Найбільш поширеним методом активного управління чергами є метод випадкового завчасного виявлення перевантаження (Random Early Detection, RED) [1]. Згідно з цим методом рішення про відкидання того чи іншого пакету приймається на основі обчислень середнього розміру черги та імовірності відкидання пакетів. Для обчислення зазначених величин використовуються аналітичні вирази, що містять низку параметрів, значення яких підібрано експериментальним шляхом. Слід зазначити, що ці розрахункові формули є евристичними та, на жаль, не мають достатнього теоретичного обґрунтування. Тому, на практиці використання RED хоча й знижує середню затримку пакетів, проте часто спричиняє більшу кількість втрачених пакетів.

Недосконалість методу RED викликала появу великої кількості його різних модифікацій. Зараз відомі методи адаптивного (Adaptive RED), динамічного (Dynamic RED), стабілізованого (Stabilized RED), потокового (Flow RED), зваженого (Weighted RED) завчасного виявлення перевантаження. Проте усі зазначені удосконалені версії активного управління чергами також мають основний недолік класичного RED: рішення про відкидання пакетів приймається на основі використання досить грубих, наближених моделей. Тому застосування існуючих методів управління чергами в мережах з комутацією пакетів не завжди дозволяє здійснювати ефективну боротьбу з перевантаженнями, що обмежує можливості у забезпеченні якісного обслуговування користувачів. Це спричиняє необхідність розробки нового теоретично обґрунтованого методу управління процесом завчасного відкидання пакетів.

Аналіз результатів наукових досліджень показав, що управління чергами пакетів в маршрутизаторах відбувається в умовах наявності неповної, розмитої, неточної інформації про стан елементів цієї мережі в поточному часі і в майбутньому. Ефективним засобом управління в таких умовах є застосування систем нейро-нечіткого виводу [2].

Доповідь присвячено розв'язанню **актуального науково-технічного завдання**, що полягає у розробці методу нейро-нечіткого активного управління пакетними чергами в телекомунікаційній мережі.

Метою дослідження є зниження втрат пакетів та їхньої середньої затримки у маршрутизаторах за рахунок застосування нейро-нечіткого активного управління пакетними чергами.

2. Суть пропонованого методу

Згідно з пропонованим методом процес активного управління пакетною чергою вихідного порту маршрутизатора є послідовністю періодичних циклів. На рис. 1 зображено фрагмент такої послідовності, у якому поточним є цикл e. По відношенню до нього цикли a, b, c та d є попередніми, а цикл f – наступним.

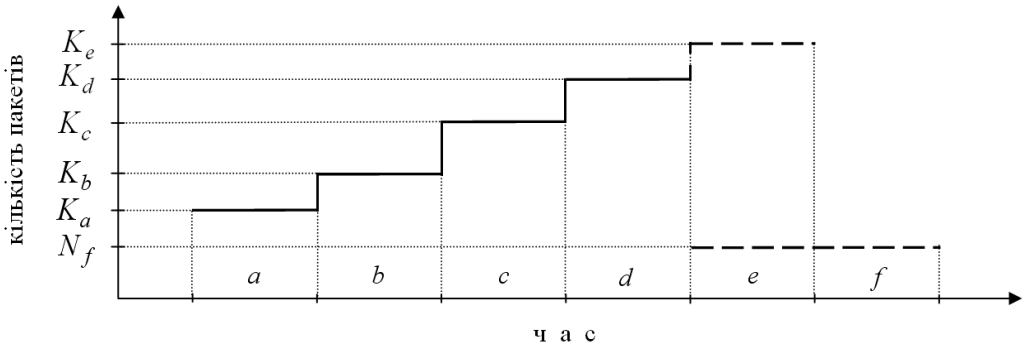


Рис. 1. Фрагмент послідовності циклів процесу активного управління пакетною чергою вихідного порту маршрутизатора.

У вихідний порт маршрутизатора у чотирьох попередніх циклах було спрямовано відповідно K_a, K_b, K_c та K_d пакетів, а у поточному циклі, припустимо, буде спрямовано K_e пакетів. Крім того, припустимо, що при пасивному управлінні чергою вихідного порту маршрутизатора в циклі f буде відкинуто N_f пакетів. Тоді, якщо $K_e \geq N_f$, то для здійснення ідеї активного управління чергою потрібно випадковим чином відкинути у поточному циклі $N_e = N_f$ пакетів, завчасно попередивши цим появу перевантаження у наступному циклі.

Суть методу активного нейро-нечіткого управління пакетною чергою вихідного порту маршрутизатора є у наступному:

1) у кожному циклі виконується підрахунок пакетів, спрямованих у вихідний порт маршрутизатора для передавання по каналу мережі;

2) на початку поточного циклу визначаються значення $\tilde{K}_e$ та $\tilde{N}_f$ – результати нейро-нечіткого прогнозування величин K_e та N_f відповідно (при цьому як вхідні змінні використовуються значення K_a, K_b, K_c та K_d), а потім обчислюється імовірність завчасного відкидання пакетів:

$$p_e = \begin{cases} 1, & \tilde{K}_e < \tilde{N}_f; \\ \dfrac{\tilde{K}_e}{\tilde{N}_f}, & \tilde{K}_e \geq \tilde{N}_f. \end{cases} \qquad (1)$$

3) значення p_e до закінчення поточного циклу використовується для прийняття рішення про випадкове завчасне відкидання пакетів; спрямований у вихідний порт маршрутизатора пакет відкидається при виконанні умови:

$$p_e \geq P, \qquad (2)$$

де P – псевдовипадкове число з рівномірним розподілом в діапазоні [0; 1].

Для одержання значень $\tilde{K}_e$ та $\tilde{N}_f$ пропонований метод передбачає побудову відповідних нейро-нечітких систем.

3. Синтез нейро-нечітких систем

Вище було зазначено, що вхідними змінними нейро-нечіткої системи прогнозування величини $\mathrm{K_e}$ є значення K_a, K_b, K_c та K_d, а вихідною змінною – значення $\tilde{K}_e$. Для одержання шуканого значення вихідної змінної пропонується використовувати один з найбільш поширених на практиці алгоритмів нечіткого виводу – алгоритм Сугено 0-го порядку, який ґрунтується на базі знань, представленій сукупністю нечітких правил:

$$\left\{Якщо\ \left(K_a=\alpha_1^A\right) та\ \left(K_b=\alpha_2^B\right) та\ \left(K_c=\alpha_3^C\right) та\ \left(K_d=\alpha_4^D\right),\ то\ \left(\tilde{K}_e=Y_r\right)\right\}, \tag{3}$$

де α_1^A – терм (нечітка множина) номер A вхідної змінної $\mathrm{K_a}$, $A\in\overline{[1,\mathrm{A_{max}}]}$;

α_2^B – терм номер B вхідної змінної $\mathrm{K_b}$, $B\in\overline{[1,B_{\max}]}$;

α_3^C – терм номер C вхідної змінної $\mathrm{K_c}$, $C\in\overline{[1,C_{\max}]}$;

α_4^D – терм номер D вхідної змінної $\mathrm{K_d}$, $D\in\overline{[1,D_{\max}]}$;

$\mathrm{Y_r}$ – чітке значення індивідуального висновку правила номер $r\in\overline{[1,\rho]}$.

Для побудови нейро-нечіткої системи обрано найпростіший варіант її початкових параметрів: для вхідних змінних обрано по дві функції приналежності ($A_{\max}=B_{\max}=C_{\max}=D_{\max}=2$) трикутної форми. Пропонована система прогнозування величини $\mathrm{K_e}$ структурно складається з чотирьох нейронних шарів, за допомогою яких виконуються наступні процедури нечіткого виводу: фазифікація, агрегування, активізація та дефазифікація.

Перший шар виконує процедуру фазифікації, яка полягає у тому, що для конкретних значень K_a^*, $\mathrm{K_b^*}$, $\mathrm{K_c^*}$ та $\mathrm{K_d^*}$ обчислюються величини $\mu_1\left(K_a^*\right)$, $\mu_2\left(K_a^*\right)$, …, $\mu_{A\max}\left(K_a^*\right)$, $\mu_1\left(K_b^*\right)$, $\mu_2\left(K_b^*\right)$, …, $\mu_{B\max}\left(K_b^*\right)$, $\mu_1\left(K_c^*\right)$, $\mu_2\left(K_c^*\right)$, …, $\mu_{C\max}\left(K_c^*\right)$, $\mu_1\left(K_d^*\right)$, $\mu_2\left(\mathrm{K_d^*}\right)$, …, $\mu_{\mathrm{Dmax}}\left(\mathrm{K_d^*}\right)$ – значення функцій приналежності вхідних змінних відповідним термам.

Другим шаром нейро-нечіткої системи здійснюється процедура агрегування, в процесі якої визначаються ступені істинності умов кожного правила при конкретних значеннях вхідних змінних:

$$\left\{G_r=\mu_A(K_a^*)\wedge\mu_B(K_b^*)\wedge\mu_C(K_c^*)\wedge\mu_D(K_d^*)\right\}. \tag{4}$$

За допомогою третього шару обчислюється сума та зважена сума вихідних сигналів другого шару. При цьому виконується активізація, суть якої в алгоритмі Сугено 0-го порядку полягає у визначенні індивідуальних висновків правил: Y_1, Y_2, …, Y_r, …, Y_ρ.

Четвертий шар реалізує операцію ділення вихідних сигналів третього шару, тобто визначає результат процедури дефазифікації, в результаті якої методом центру тяжіння для одноточкових множин визначається чітке значення вихідної змінної за таким виразом:

$$\tilde{K}_e^*=\frac{\sum\limits_{r=1}^{\rho}Y_rG_r}{\sum\limits_{r=1}^{\rho}G_r}. \tag{5}$$

Для налаштування параметрів функцій приналежності вхідних змінних і значень індивідуальних висновків правил нейро-нечітку систему потрібно навчити відтворювати залежність $K_e=f\left(K_a,K_b,K_c,K_d\right)$. З цією метою шляхом проведення експериментальних досліджень необхідно зібрати дані для нейронного самонавчання у вигляді матриці:

$$\begin{Vmatrix} K_1 & K_2 & K_3 & K_4 & K_5 \\ K_2 & K_3 & K_4 & K_5 & K_6 \\ . & . & . & . & . \\ K_{x-4} & K_{x-3} & K_{x-2} & K_{x-1} & K_x \\ . & . & . & . & . \\ K_{X-4} & K_{X-3} & K_{X-2} & K_{X-1} & K_X \end{Vmatrix}, \quad (6)$$

де K_x – виміряне значення кількості пакетів, спрямованих у вихідний порт маршрутизатора протягом циклу номер x $\left(x \in \left[\overline{1, X}\right]\right)$ при пасивному управлінні відповідною пакетною чергою.

Дані для нейронного самонавчання одержано з використанням моделі пасивного управління пакетною чергою вихідного порту маршрутизатора. Зазначену модель створено у середовищі Simulink системи комп'ютерної математики MATLAB . Адекватність моделі обґрунтовано достатньою збіжністю результатів імітаційного і аналітичного моделювання [3].

4. Результати імітаційного моделювання процесу управління пакетною чергою вихідного порту маршрутизатора.

Для дослідження процесу завчасного відкидання пакетів, що здійснюється згідно з методом RED, використано імітаційну модель, розробці якій присвячено роботу [4]. У середовищі MATLAB+Simulink розроблено також імітаційну модель нейро-нечіткого активного управління пакетною чергою вихідного порту маршрутизатора. Ефективність досліджуваного процесу оцінювалась з урахування показників $t_з$ (середня затримка пакетів у черзі) і $p_в$ (імовірність відкидання пакету, спрямованого до вихідного порту маршрутизатора). У результаті моделювання встановлено, що при використанні нейронечіткого активного управління пакетною чергою середня затримка пакетів у черзі вихідного порту маршрутизатора скорочується на 4% – 10% у порівнянні з використанням методу RED. Крім того, застосування пропонованого методу дозволяє зменшити імовірність відкидання пакетів на 5% – 12%.

5. Висновки

1. Розроблено новий метод активного управління пакетною чергою вихідного порту маршрутизатора телекомунікаційної мережі, який, на відміну від існуючих, в процесі прийняття рішення про завчасне відкидання пакету передбачає використання нейронечітких систем.

2. Застосування зазначеного методу дозволяє на 4% – 10% скоротити середню затримку пакетів у черзі вихідного порту маршрутизатора та на 5% – 12% зменшити імовірність відкидання пакетів.

Література:

1. Floyd S. Jacobson V. Random early detection gateways for congestion avoidance, IEEE/ACM Transactions on networking 1993 – 1 (4), p. 397 – 413.

2. Усков А.А., Кузьмин А.В. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. – М.: Горячая линия – Телеком, 2004. – 143 с.

3. Польщиков К.О., Лаврут О.О., Дружинін С.В. Імітаційна модель управління потоками даних в інформаційній мережі шляхом зміни міжсегментного інтервалу // Радіоелектронні і комп'ютерні системи. – Харків: «ХАІ», 2009. – Вип. 7(41). – С. 304 – 308.

4. Польщиков К.О., Рвачова Н.В. Імітаційна модель управління інтенсивністю вхідного потоку даних в телекомунікаційній мережі // Збірник наукових праць ВІТІ НТУУ «КПІ». – К.: ВІТІ НТУУ «КПІ», 2009. – Вип. 2. – С. 98 – 109.

МЕТОДЫ ПОСЛЕДОВАТЕЛЬНОЙ КОМПЕНСАЦИИ ИСКАЖЕНИЙ В ДРЕВОВИДНЫХ АЛГОРИТМАХ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУПА

Поповский В.В., Тур Б.С., Искандар С.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. системотехники, тел. (057) 702-13-20,
E-mail:bogdan_tur@mail.ru ; факс (057) 702-13-20,

Nowadays Wireless Broadband Networks (WBN) are dynamically developed sphere of science and technology. The given work is devoted to analysis of Random Multiple Access method called Successive Interference Cancellation (SIC), which is widely used in IEEE 802.16 standard. The direction of research is rather up-to-date and its importance is very high.

Общие сведения

Среди различных методов множественного (многостанционного) доступа в беспроводных системах связи наибольшую популярность приобрели методы случайного множественного доступа (СМД). К числу таких относятся алгоритмы АЛОХА, методы двойного экспоненциального отката (Binary Exponential Backoff- BEB), древовидные алгоритмы [1]. Наиболее важной характеристикой этих методов является время разрешения конфликта T_k, наступающего вследствие того, что два или более абонента одновременно претендуют на предоставление ресурса ретранслятора или базовой станции (БС). Показателем скорости разрешения конфликта является отношение [2]:

$$V = \frac{k}{T_k}, \qquad (1)$$

где k - кратность конфликта.

Исторически первым был предложен алгоритм АЛОХА, который с различными модификациями используется до настоящего времени. У этого алгоритма из-за включения механизма выбора случайной задержки при повторной передаче время T_k достаточно велико и в современных широкополосных беспроводных системах типа WiMAX, LTE вместо этих алгоритмов рекомендуется использовать BEB или древовидные алгоритмы, где указанное время в значительной мере детерминируется, а скорость V достигает значений 0,3-0,4.При дополнительных мерах, при использовании последовательной компенсации помех (Successive interference Cancellation - SIC) эта скорость может достичь 0,6 и более [2]. Рассмотрим более подробно процедуру древовидного алгоритма и оценим возможность ее эффективного использования.

Обоснование выбора структуры устройства коррекции принятых сигналов

При выборе структуры устройства коррекции возникает вопрос об ограничениях, в рамках которых может быть решена оптимизационная задача минимизации уровня искажений $\Delta y(t)$. Важным фактором является выбор необходимого числа ветвей корреляции N. Очевидно, должно выполняться условие: $N \geq 2$, что при соответствующем выборе амплитуд и фаз весовых коэффициентов в ветвях коррекции позволит получить взаимную компенсацию искажений. При $N = 2$ искажения отображают ситуацию с плоским фазовым фронтом в элементах пространственного сигнала $x_i(t)$. При $N = 3$ может отображаться нелинейная параболическая форма фазового фронта. Если же приемное устройство реализуется в виде N - элементной антенной решетки, то размер апертуры D необходимо сопоставлять с радиусом пространственной корреляции ρ. Очевидно, если

$D \ll \rho$, то при любой пространственной структуре сигнала $x_i(t)$ фазовый фронт будет восприниматься как плоский. Вместе с тем и при использовании лишь одной приемной антенны, модель статистической структуры многолучевого сигнала должна выбираться исходя из рассмотренных представлений.

Другим ограничением, подлежащим выбору, является период следования тест-сигналов T_T. Данный параметр следует сопоставлять с интервалом корреляции или τ_K случайных изменений сигнала $y(t)$. Очевидно для того, чтобы устройство корреляции успевало компенсировать случайные изменения искажений, период следования T_T должен быть таким, чтобы за это время не произошло заметных изменений ядерных функций $K_i(t)$. Опыт практического использования аналогичных алгоритмов показывает, что допустимые результаты получаются, если этот период выбирать из условий

$$T_T = \frac{\tau_K}{10}, \tag{6}$$

Если же на интервале корреляции τ_k укладывается порядка 100 отсчетных значений, то результаты являются достаточно хорошими, нескомпенсированными остаются менее 1% искажений.

Диапазоны изменений управлений для амплитуд и фаз компенсационных сигналов обычно согласовывают со статистикой канала (Релей, Райс и др.), а сами регуляторы выполняют с использованием квадратурных разложений, что позволяет оставаться в рамках линейных процедур управляющих алгоритмов.

Синтез устройства компенсации искажений сигналов, принятых в многолучевом канале

Весовые коэффициенты обеспечивающие компенсацию указанных искажений, созданных ядерными функциями $K_i(t)$ - образуют вектор $w(t)$ и представляют собой случайные процессы. В качестве математических моделей этих процессов можно использовать дифференциальные уравнения состояния [4]:

$$\frac{dw(t)}{dt} = F(t)w(t) + G(t)\xi(t), \tag{7}$$

где $F(t)$ и $G(t)$ - соответственно: матрицы состояния и генерации, элементы матрицы $F(t)$ суть величины α_{ij} - обратные значения интервалов корреляции многомерного процесса $w(t)$, $\xi(t)$ - порождающий виртуальный гауссов белый шум (ГБШ), со спектральной плотностью мощности $N_\xi(t)$.

Для обычно используемой цифровой реализации процедур оценки и управления уравнения (7) принимает вид:

$$w(k+1) = \Phi(k+1,k)w(k) + G(k)\xi(k), \tag{8}$$

где $\Phi(k+1,k) = \exp\{-\alpha\Delta t\}, \alpha = \frac{1}{\tau_K}$, $\Delta t = T_T$ - шаг дискретизации рекурсивной процедуры (8), $G(k) = \sqrt{\sigma_w^2(1-\exp\{-\alpha\Delta t\})}$.

Для получения оценки оптимального вектора весовых коэффициентов (ВВК) $\hat{w}(k)$ воспользуемся процедурой Калмана-Бьюси (ФКБ) [4]:

$$\hat{w}(k+1) = \Phi(k+1,k)\hat{w}(k) + M(k)[y(k) - y_{\text{н}}(k)], \tag{9}$$

где $y(k) = \hat{w}(k)x(k) + v(k)$, - уравнение наблюдения полезного сигнала на фоне ГБШ $v(k)$ со спектральной плотностью мощности N_v. На рис.3 представлена структурная схема устройства коррекции приемных сигналов.

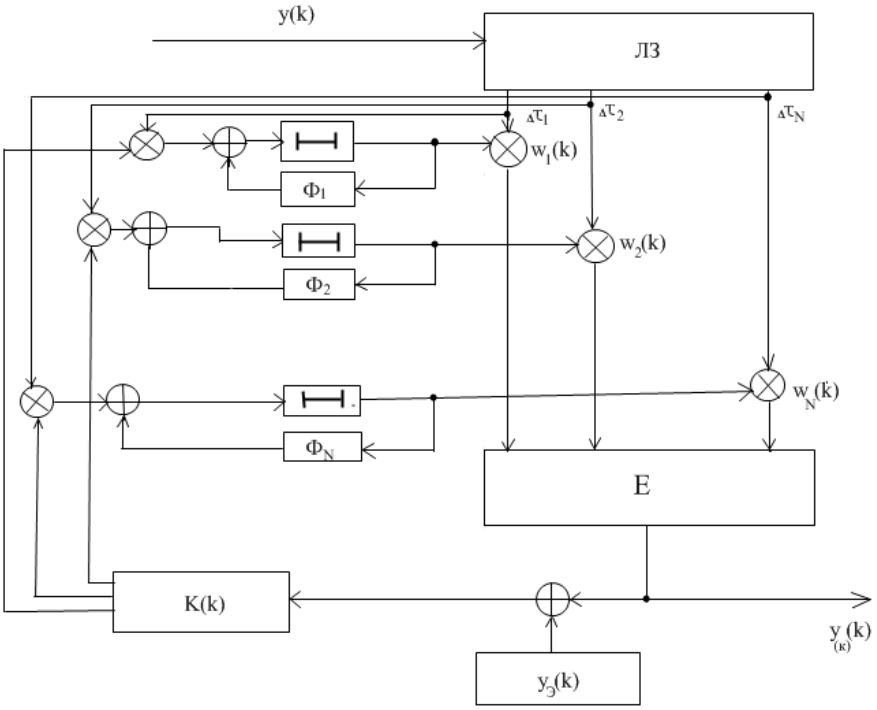


Рис.3-Структурная схема устройства коррекции принятых сигналов

Коэффициент $M(k)$ - является аналогом шаговой постоянной в процедурах Уидроу-Хоффа, которая является оптимальной для ситуации, когда $K_i(k)$ суть случайные величины. В общем же случае, когда $K_i(k)$ - случайные процессы, в соответствии с ФКБ:

$$K(k) = P(k)Y^T(k)N_0^{-1}, \tag{10}$$

где $Y(k)$ - вектор принятых сигналов на выходе линии задержки (ЛЗ), где выводы следуют через временные интервалы $\Delta\tau_i, i = 1,2,3,\ldots,N$. При этом $\sum_{i=1}^{N}\Delta\tau_i = \tau_k$ - интервал когерентности принятого многолучевого сигнала.

Заключение

1. Среди различных методов случайного множественного доступа наибольшим потенциалом по скорости разрешения конфликтов обладают древовидные алгоритмы с использованием последовательной компенсации помех SIC. Потенциальные возможности алгоритмов SIC могут быть реализованы при условии получения идентичности структур

сигналов на соседних слотах, что достигается выбором амплитудно-фазовых выравнивателей.

2.Эффективный алгоритм амплитудно-фазового выравнивания может быть получен, если учтена статистическая структура принимаемых сигналов, с учетом корреляции этих сигналов на соседних слотах, индекс когерентности принимаемых сигналов, что непосредственно определяет величину шага дискретизации для передачи эталонного сигнала и число отводов от линии задержки.

3. Удачной математической моделью многолучевого канала распространения радиосигнала может служить интегро-степенной полином Вольтерра 1-го рода с помощью которого можно адекватно отображать как линейные, так и нелинейные ситуации.

4. Оптимальной процедурой для реализации алгоритма амплитудно-фазового выравнивателя является фильтр Калмана-Бьюси.

Литература:

1.Yu. Y.,Giannakis G.B. High-throughput random access using successive interference cancellation in a tree algorithm. IEEE Transactions Inform. Theory.2007.V.53, № 12, p. 4628-4639.

2. Андреев С.Д., Пустовалов Е.В., Тюрликов А.М. Древовидный алгоритм разрешения конфликта, устойчивый к неполному погашению интерференции. Автоматика и телемеханика. 2009, №3, стр. 78-96.

3. Апарцин А.С. К исследованию устойчивости решений полиномиального уравнения Вольтерра 1 рода. Автоматика и телемеханика 2011, №6, стр. 95-114.

4. Поповский В.В., Олейник В.Ф. Математические основы управления и адаптации в телекоммуникационных системах. Х. СМИТ, 2011- 362с.

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТРАФІКУ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ

В.І. Романчук, О.А. Лаврів, А.В. Поліщук
Національний університет "Львівська політехніка" кафедра "Телекомунікації"
760046, С. Бандери., 12, Львів, Україна, тел. 0 (322) 743382 E-mail Romanchuk@lp.edu.ua

This paper has proposed an analysis of multimedia corporate network traffic. Its statistic and probabilistic properties had been researched.

На сьогодні у розвитку телекомунікаційних мереж відбувається перехід до мультисервісного обслуговування, що суттєво зміщує акценти у архітектурі існуючих корпоративних мереж великих організацій. Корпоративний трафік початку століття – це, здебільшого, перенесення послуги передавання та обміну даними. Такий сервіс не вимагає суттєвого контролю за параметрами якості обслуговування. Необхідним є лише забезпечення низької імовірності втрат інформації в каналі передавання, а також вибір достатньо продуктивних пристроїв обслуговування. Якщо трафік в мережі майже однорідний, то не виникає потреби у залученні додаткових механізмів, що опирались би на властивості та структуру послуг при визначенні способу обслуговування певної інформації. Для того, щоб здійснювати передавання інформації потокового характеру, виникає завдання максимізації мережевого ресурсу (як канального, так і логічного) для конкретного фрагменту даних у конкретний момент часу. Це пояснюється неможливістю повторного отримання помилкового фрагменту інформації, оскільки вона є актуальною лише у призначений для неї інтервал часу.

Ситуація, коли у структурі трафіку останнім часом спостерігається значне тяжіння до використання інтерактивних сервісів та активізації потокових трансляцій у мережі, розрахованій на передавання даних, змушує шукати «слабкі» місця у її структурі та вирішувати завдання оптимального вибору ресурсів пристроїв обслуговування для досягнення очікуваної якості обслуговування.

Для того, щоб підійти до методики розв'язування такого завдання, необхідно провести дослідження часових та імовірнісних параметрів і характеристик реального трафіку корпоративної мережі великої організації, яка з моменту свого впровадження орієнтована на послугу передавання даних, однак із врахуванням зростання потреб користувачів, вимушена обслуговувати мультисервісний трафік.

Самоподібність трафіку мультисервісної мережі та її вплив на прогнозування параметрів пристроїв обслуговування

В теорії аналізу телекомунікаційних мереж достатньо тривалий період загальноприйнятою була концепція, що будь-який пристрій обслуговування може бути описаний засобами систем масового обслуговування та теорії телетрафіку.

Проведений аналіз показав, що так відбувається через невідповідність обраних моделей реальному мережевому трафіку до і після обслуговування. Це, в свою чергу, пояснюється відмінностями у імовірнісних характеристиках випадкових процесів, які прийняті для моделювання реального трафіку.

Для проведення статистично-імовірнісного аналізу трафіку корпоративної мультисервісної мережі використовувались наступні методи дослідження: RS-аналіз для оцінки параметру Херста випадкового процесу, що відображає трафік мультисервісної мережі, оцінка відповідності експериментального розподілу аналітичним відомим розподілам проведена із застосуванням критерію Колмогорова.

Метод RS-аналізу відображається наступною послідовністю кроків:

Визначається математичне сподівання випадкового ряду $X_k\,(k=1..N)$:

$$M_N = \frac{1}{N}\sum_{k=1}^{N} X_k \qquad (1)$$

Визначається дисперсія вибірки:

$$S_N^2 = \frac{1}{N}\sum_{k=1}^{N}(X_k - M)^2 \ . \qquad (2)$$

Визначається інтегральне відхилення:

$$D_j = \sum_{k=1}^{j} X_k - jM, \ \mathrm{j} \in [1;\mathrm{N}] \ . \qquad (3)$$

Визначається рознесення випадкового процесу:

$$R_N = \max_{1\le j\le N} D_j - \min_{1\le j\le N} D_j \ . \qquad (4)$$

З встановленого Херстом співвідношення:

$$\frac{R}{S} \approx \left(\frac{N}{2}\right)^H \ , \qquad (5)$$

визначається параметр Херста *H*:

$$H = \frac{\log\left(\frac{R}{S}\right)}{\log\left(\frac{N}{2}\right)} . \qquad (6)$$

Аналіз характеристик трафіку корпоративної мережі та доведення неможливості його адекватного моделювання відомими імовірнісними розподілами

В роботі проведено аналіз трафіку мультисервісної мережі великої організації. Протягом 541 хвилини велося спостереження за інтенсивністю вхідного і вихідного трафіку агрегуючого маршрутизатора. Було зафіксовано значення кількості поступлених пакетів з інтервалом 1 хв.

Спершу було проаналізовано трафік від одного абонента при завантаженні файлу із фіксованим значенням швидкості з'єднання (рис. 1). Виходячи із RS-методу оцінки параметру Херста, визначено, що даний параметр для такого випадкового процесу становить 0,58. Це означає, що даний процес схильний до персистентності і можна очікувати, що при агрегації декількох таких процесів згадана тенденція буде збільшуватись, що буде доведено нижче на прикладі аналізу трафіку агрегуючого маршрутизатора.

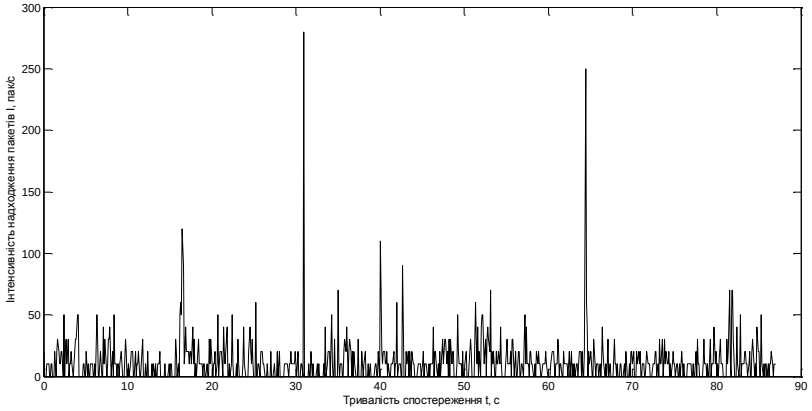


Рис. 1.Інтенсивність трафіку від одного абонента при завантаженні файлу зі швидкістю з'єднання 512 кбіт/с

На рис. 2 наведено трафік, що проходить через агрегуючий маршрутизатор. Штриховою лінією показано вихідний трафік, а суцільною вхідний. На графіку можна спостерігати, що пік-фактор даного процесу значний, що дозволяє зробити припущення про те, що коефіцієнт Херста близький до 1.

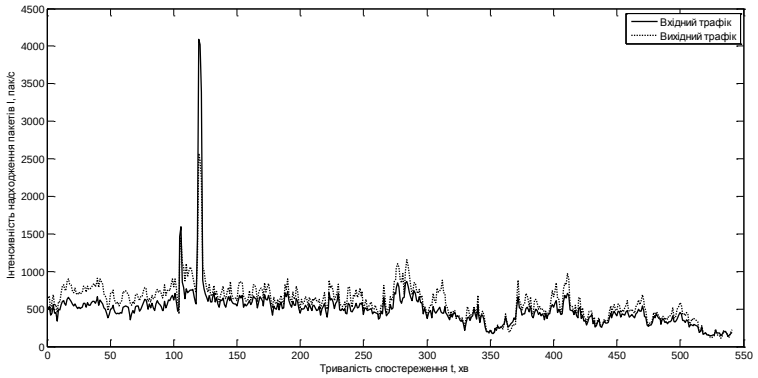


Рис. 2. Інтенсивність агрегованого трафіку корпоративної мультисервісної мережі

На рис. 3 і 4 запропоновано імовірнісно-статистичний аналіз вхідного і вихідного трафіку та проведено підбір аналітичного розподілу імовірностей.

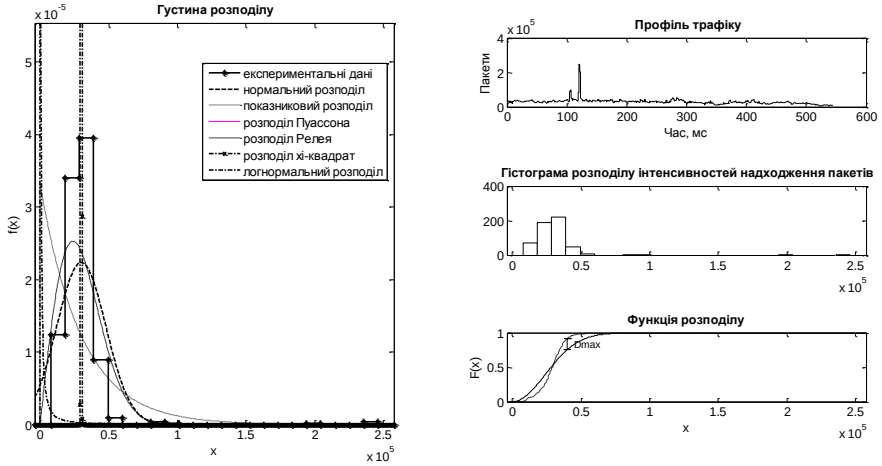


Рис. 3. Імовірнісно-статистичний аналіз вхідного трафіку

Результати проведених статистичних досліджень: об'єм вибірки n=541, число степенів свободи f=n-1=540, xmin=8109, xmax=245727, кількість інтервалів k=23, ширина інтервалу h=10331,217, вибіркові параметри розподілу: математичне очікування Mx=30064.553, середньоквадратичне відхилення Sx=17853.044, дисперсія Dx=318731179.87, асиметрія Ax=8.1444271, ексцес Ex=89.7885207, варіація Vx=0.5938237.

Табл. 1 Рівні значущості і деякі параметри розподілів

p0	p	t(1-p/2,f)	chi2(1-p/2,f)	chi2(p/2,f)
0.9000	0.1000	1.64768	595.16833	487.10527
0.9600	0.0400	2.05872	609.61842	474.67087
0.9900	0.0100	2.58496	628.40237	459.10785
0.9990	0.0010	3.30863	654.72840	438.36749

Виражено параметри гіпотетичних розподілів через статистичні параметри експериментального розподілу: нормальний розподіл: mx=30064.5526802; sx=17853.0439945, показниковий розподіл: lam=0.0000333, розподіл Пуассона: L=30064.5526802, релеєвський розподіл: sig=23988.0424110, хі-квадрат: Xi2=30064.5526802, логнормальний: Mu=0.5211728; Si=4.4249134

Вибираємо рівень значущості для критерію Колмогорова p=0.30. Найбільш підходящий – розподіл Релея. Максимальна різниця Dmax=0.16562 досягається при x=40012. Статистика Колмогорова $\lambda = 3.85223$. Квантиль розподілу Колмогорова $\lambda(0.70)=0.97306$. Розподіл підібрано неправильно, так як $\lambda > \lambda(1\text{-p})$.

Параметр Херста вхідного трафіку 0,837.

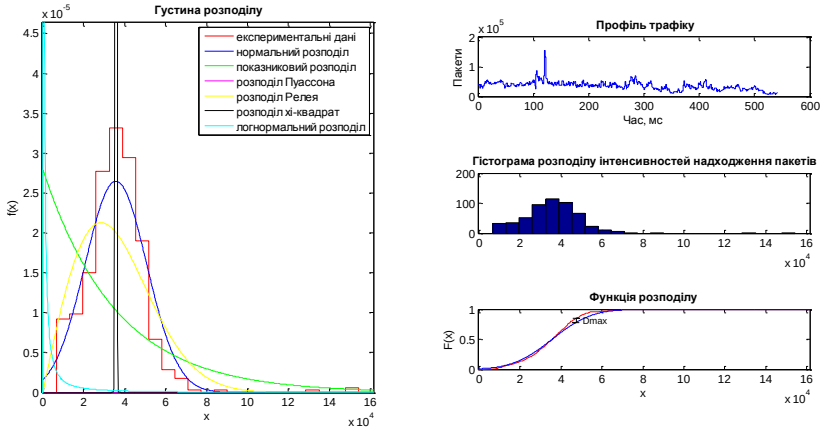


Рис. 4. Імовірнісно-статистичний аналіз вихідного трафіку

Результати проведених статистичних досліджень: об'єм вибірки n=541, число степенів свободи f=n-1=540, xmin=6817, xmax=154189, число інтервалів k=23, ширина інтервалу h=6407.478, вибіркові параметри розподілу, математичне очікування Mx=35723.675, середньоквадратичне відхилення Sx=15068.627, дисперсія Dx=227063523.475, Асиметрія Ax=2.1395800, ексцес Ex=14.7511545, варіація Vx=0.4218107.

Табл. 2 Рівні значущості і деякі параметри розподілів

p0	p	t(1-p/2,f)	chi2(1-p/2,f)	chi2(p/2,f)
0.9000	0.1000	1.64768	595.16833	487.10527
0.9600	0.0400	2.05872	609.61842	474.67087
0.9900	0.0100	2.58496	628.40237	459.10785
0.9990	0.0010	3.30863	654.72840	438.36749

Виражено параметри гіпотетичних розподілів через статистичні параметри експериментального розподілу: нормальний розподіл: mx=35723.6746765; sx=15068.6271264, показниковий розподіл: lam=0.0000280, розподіл Пуассона: L=35723.6746765, Релеєвський розподіл: sig=28503.3684795, хі-квадрат: Xi2=35723.6746765, логнормальний: Mu=0.8631987; Si=4.3864268.

Вибираємо рівень значущості для критерію Колмогорова p=0.30. Найбільш підходящий – нормальний розподіл. Максимальна різниця Dmax=0.07037 досягається при x=47355. Статистика Колмогорова λ=1.63669. Квантиль розподілу Колмогорова $\lambda(0.70)$= 0.97306. Розподіл підібрано неправильно, так як $\lambda > \lambda(1\text{-p})$. Параметр Херста вихідного трафіку 0,907. В роботі розглянуто основні тенденції розвитку корпоративних мереж зв'язку та проведено аналіз трафіку сучасної корпоративної мережі великої організації. На основі проведених досліджень доведено, що агрегований трафік мультисервісної мережі є само подібним з параметром Херста, близьким до однини ці, що свідчить про неможливість точної апроксимації такого випадкового процесу аналітичними розподілами імовірностей. Дане припущення перевірене на основі проведено підбору аналітичного розподілу за критерієм Колмогорова. Найбільш близьким для вхідного трафіку виявився розподіл Релея, а для вихідного – нормальний розподіл. Однак для жодного з цих розподілів не виконана умова критерію Колмогорова, тому найбільш придатними для аналітичного моделювання трафіку мультисервісних корпоративних мереж можна вважати самоподібні процеси.

Література:

1. Ложковский А.Г. Исследование системы обслуживания с ожиданием и рекурентным потоком вызовов // Наукові праці ОНАЗ ім. О.С. Попова. – 2004. – № 2. – С. 56–59. 2. Лаврів О.А. Моделювання та дослідження параметрів QoS в системі розподілу інформації з самоподібним вхідним потоком і обслуговуванням за порядком черги. Матеріали науково-практичної конференції «Проблеми телекомунікацій – 2011». – 2011 р.

ИССЛЕДОВАНИЕ ОДНОПУТЕВОЙ МАРШРУТИЗАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ БАЛАНСИРОВКИ НАГРУЗКИ НА СЕТЬ

Семеняка М.В., Лемешко А.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. телекоммуникационных систем и сетей, E-mail: maxisemen@gmail.com; тел. (057) 372-67-04

The given work is devoted to the research of the possibility using single path routing to provide load balancing in the network. Distribution of the traffic is determined by channel utilization in case of multiple traffic flows entering the network.

Под однопутевой маршрутизацией понимается такая процедура выбора маршрутов, при которой для передачи данных от узла-источника узлу-адресату используется единственный маршрут. Очевидно, что в общем случае многопутевая маршрутизация является предпочтительней, так как она более полно использует ресурсы сети передачи данных, однако фиксированная маршрутизация намного проще для реализации и в ряде случаев (например, при низкой загрузке сети) при ее использовании качество функционирования сети может оказаться очень близким к варианту с реализацией многопутевой маршрутизации.

Целью данного исследования является анализ результатов распределения трафика однопутевой моделью маршрутизации, в случае, когда на вход сети поступает множество потоков.

Топология исследуемой сети с пропускными способностями каналов (Мбит/с) представлены на рисунке.

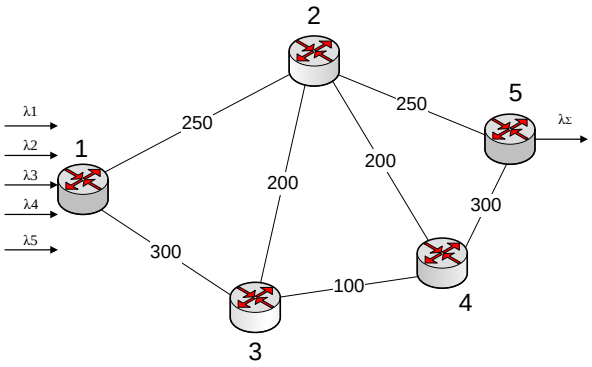


Рис.1 – Топология исследуемой сети с пятью входящими потоками

Суммарная пропускная способность сети составляет 550 Мбит/с. Возможные пути следования потоков трафика: путь №1: узлы 1-2-5, путь №2: узлы 1-3-4-5, путь №3: узлы 1-3-2-4-5, путь №4: узлы 1-2-4-5, путь №5: узлы 1-3-2-5.

Для предотвращения потери пакетов на сетевых узлах и в сети в целом, необходимо обеспечить выполнение условий сохранения потока:

$$\begin{cases} \sum\limits_{j:(i,j)\in E} X_{ij}^{k} - \sum\limits_{j:(j,i)\in E} X_{ji}^{k} = 0, \;\; k \in K,\; i \neq s_k,\; t_k, \\ \sum\limits_{j:(i,j)\in E} X_{ij}^{k} - \sum\limits_{j:(j,i)\in E} X_{ji}^{k} = 1, \;\; k \in K,\; i = s_k, \\ \sum\limits_{j:(i,j)\in E} X_{ij}^{k} - \sum\limits_{j:(j,i)\in E} X_{ji}^{k} = -1, \;\; k \in K, i = t_k. \end{cases} \quad (1)$$

Кроме этого, необходимо обеспечить выполнение условий предотвращения перегрузки в каналах сети:

$$\sum_{k\in K} d_k X_{ij}^{k} \le c_{ij}, \quad (2)$$

где d_k – интенсивность k-го трафика в канале ij, c_{ij} – пропускная способность канала связи. В соответствии с физикой решаемой задачи на переменные X_{ij}^k накладываются следующие ограничения:

$$X_{ij}^k \in (0, 1). \tag{3}$$

Целевая функция имеет вид:

$$\sum_{(i,j)\in E} \frac{10^8}{c_{i,j}} \cdot X_{ij}^k \to \min. \tag{4}$$

В результате проведенного аналитического моделирования получена зависимость средней задержки доставки пакетов от поступающей в сеть нагрузки представлена на рисунке 2. Из данного графика видно, что модель однопутевой маршрутизации обеспечивает низкие показатели средней задержки ($\tau_{cp} \le 0.1$ с) в области низких нагрузок на сеть ($\rho = 0 \div 0.4$) для всех входящих трафиков.

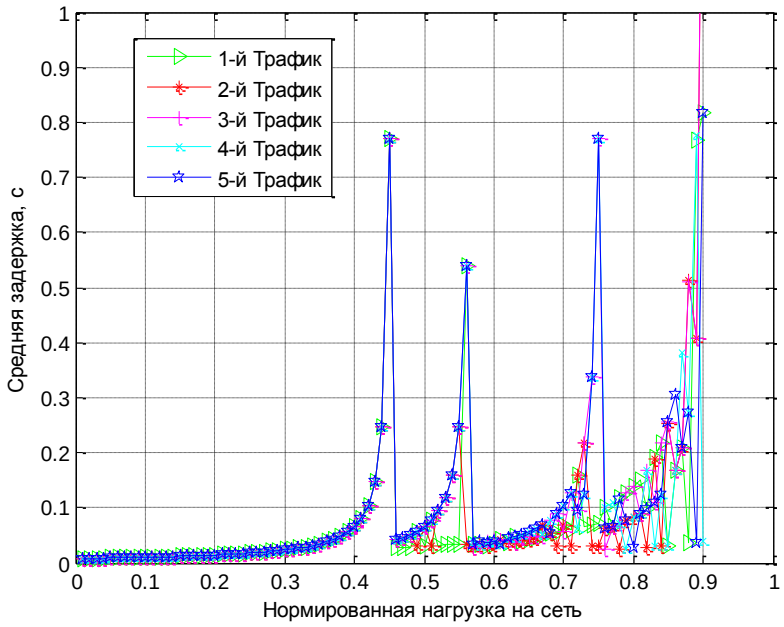


Рис. 2 – Зависимость средней задержки доставки пакетов от нормированной нагрузки на сеть

Распределение трафика происходит по пути с наименьшей стоимостью. В результате переполнения данного пути алгоритм маршрутизации направляет один из трафиков по пути с большей стоимостью, тем самым вызывая скачкообразное изменение показателя средней задержки. В результате переполнения и этого пути механизм однопутевой маршрутизации перенаправляет один из потоков в следующий свободный путь, вызывая тем самым резкое изменение показателя средней задержки. Такое скачкообразное изменение средней задержки негативно сказывается на качестве услуг, чувствительных к джиттеру.

Для устранения данного недостатка предложено изменить накладываемое ограничение на переменные (2), предотвращая полную загрузку каналов связи:

$$\sum_{k\in K} d_k X_{ij}^k \le c_{ij} \cdot 0.95, \tag{5}$$

В случае использования ограничения (5) каналы загружаются на 95% своей пропускной способности, наблюдается уменьшение пиков колебания средней задержки, как показано на рисунке 3:

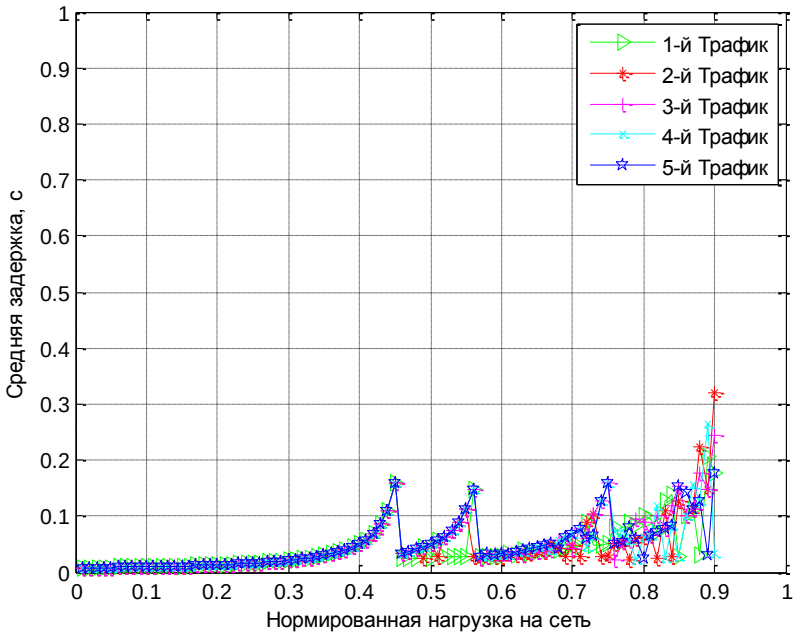


Рис.3 – Зависимость средней задержки доставки пакетов от нормированной нагрузки на сеть с ограничением на загрузку канала

В результате проведенных исследований мы видим, что однопутевая маршрутизация способна обеспечить балансировку нагрузки на сеть в случае, когда в сеть поступает множество потоков малой интенсивности (по отношению к максимальной пропускной способности сети). Потоки распределяются изначально по пути с наименьшей стоимостью, после переполнения которого, направляются по путям с большей метрикой. В силу особенностей однопутевой маршрутизации балансировка нагрузки может осуществляться распределением количества трафиков, направленных по пути, а не их долями, как в задаче многопутевой маршрутизации. То есть чем больше потоков малой интенсивности на входе в сеть, тем эффективнее можно управлять загрузкой сети в рамках решения задачи однопутевой маршрутизации, алгоритмы которой намного проще, нежели в случае многопутевой маршрутизации. Недогружая каналы связи мы обеспечиваем минимальные показатели средней задержки ($\tau_{cp} \le 0.2$ с) почти на всей области абонентской нагрузки ($\rho = 0 \div 0.9$).

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЧУТЛИВОСТІ ФІЛЬТРУ КАЛМАНА-Б'ЮСІ ПРИ НЕСТАЦІОНАРНОМУ ТРАФІКУ

Сокол Г.В.
Військовий інститут телекомунікацій та інформатизації національного технічного університету України "КПІ"
36009, Полтава, вул. Зіньківська, 44, каф. Військових телекомунікаційних мереж та захисту інформації, тел. (0532) 53-18-45, 097-999-18-90

Consider the Kalman filter sensitivity study, I bet to deviations of the selected model parameters. The method of analytical studies show that mismatch parameters of the selected model and parameters of the filter can lead to significant losses as a treatment or loss of stability processing procedures.

Розглянемо дослідження чутливості фільтру Калмана-Б'юсі (ФКБ) до відхилень параметрів вибраної моделі. Методом аналітичного дослідження показано, що неспівпадання параметрів вибраної моделі та параметрів фільтру можуть привести до значних втрат якості обробки або до втрати стійкості процедури обробки.

Дослідження впливу відхилень параметрів дискретного ФКБ від вибраної моделі (чутливість ФКБ) проведені на макеті, який включає модель спостереження, модель оцінки та модель обробки. Структурна схема машинного експерименту представлена на рис.1.

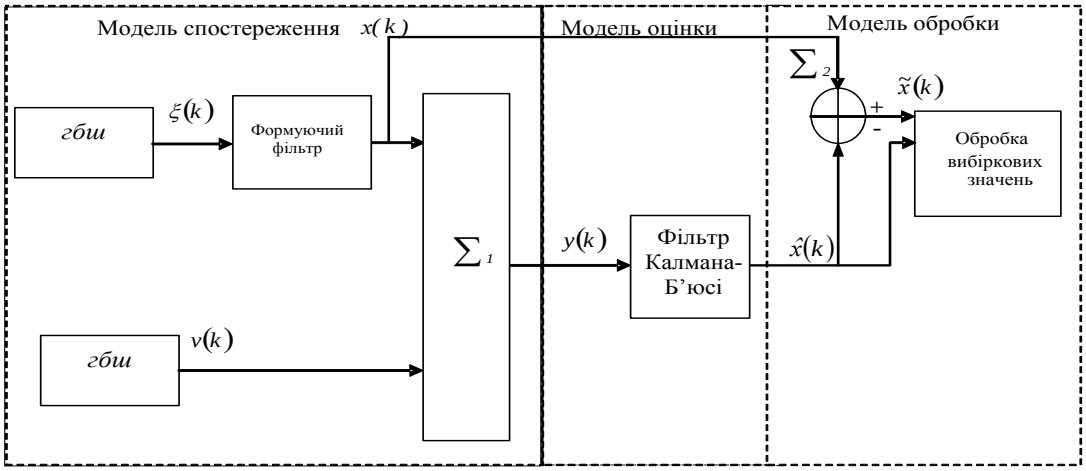


Рис.1. Структурна схема машинного експерименту

Дана схема машинного експерименту дозволяє вибирати ті або інші параметри моделі процесу, що оцінюється $x(k)$ і моделі шуму спостереження $N_v(k)$ як в стаціонарному стані, так і в нестаціонарному. Окремі генератори шумів $\xi(k)$ та $v(k)$ є стандартними процедурами формування з вибором відповідних значень спектральної щільності потужностей $N_v(k)$ і $N_\xi(k)$. Коректність вибраних параметрів моделей контролюється шляхом отримання вибіркових оцінок цих параметрів.

Ефективність фільтру в нестаціонарних умовах проаналізована на модернізованій моделі спостереження. У рівняння спостереження була введена адитивна добавка, що відображає зміну рівня і швидкості зміни цих нестаціонарностей. Враховуючи те, що зміни трафіку є результатом множинних дій на навантаження мережі, вибрана модель синусоїдальної нестаціонарності

$$y(k) = H(k)x(k) + C\sin(l\,kT/\tau_{кор}) + v(k), \qquad (1)$$

де l - множник, який змінює період нестаціонарних дій, C - змінює амплітуду нестаціонарності, $T/\tau_{кор}$ - відношення інтервалів між кроками дискретизації T до інтервалу кореляції $\tau_{кор}$.

Розглянемо ситуацію для різних випадків періодів T_s нестаціонарних змін. Коли ці зміни стають сумірними з часом встановлення процесу $T_s = 5\Delta t$, при більш повільнішій зміні нестаціонарності $T/\tau_{кор} = 25$ і, $T/\tau_{кор} = 500$. Суть впливу нестаціонарної компоненти при швидкій зміні полягає в тому, що сталий процес оцінки не встигає наступати. Таким чином фільтр працює постійно, ніби в перехідному режимі.

При більш повільній зміні вибіркові значення апостеріорних дисперсій вже мало відрізняються від результатів дії звичайного стаціонарного процесу. Таким чином при плавних змінах стаціонарної компоненти процесу, що спостережується достатньої точності оцінки можна добитися лише за рахунок скорочення кроку дискретизації.

Розглянемо також впливи процесів із стрибкоподібною нестаціонарною зміною параметрів. Для цього в рівнянні (1), $\sin(lkT/\tau_{кор}) = 1$, а значення змін C будуть меандром з періодом 100 кроків дискретизації з різними значеннями амплітуди l. На рис.2 та рис.3 представлені вибіркові значення оцінок апостеріорних дисперсій залежно від числа кроків дискретизації. Наведені на рис.2. і рис.3 графіки для кроку дискретизації $T/\tau_{кор} = 0{,}1$ і значення C відповідно $C_1 = 5$ та $C_2 = 10$. Обчислення вибіркової дисперсії проводиться методом усереднювання по десяти незалежних реалізаціях $x(k)$.

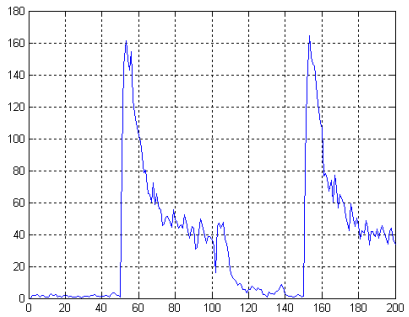


Рис. 2. Графік вибіркової дисперсії при $T/\tau_{кор} = 0{,}001; C_1 = 10$

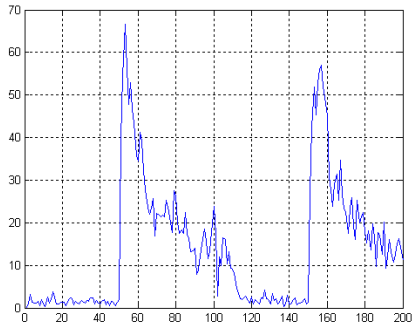


Рис. 3. Графік вибіркової дисперсії при $T/\tau_{кор} = 0{,}001; C_2 = 5$

З графіків видно, що нестаціонарність у вигляді імпульсного перепаду призводить до різкого збільшення значень апостеріорної дисперсії. Це значення перевищує в 50 і більше разів стаціонарний стан. Перехідний процес, що утворюється в наслідок появи нестаціонарного імпульсу, продовжується 100-150 кроків. Таке зростання значень апостеріорної дисперсії призводить до відповідних похибок в управлінні. Характерним є те, що при зникненні нестаціонарного імпульсу реакція фільтру менш значима, ніж при його появі. Таким чином скорочення кроку дискретизації дозволяє відстежувати нестаціонарні зміни, що є важливим чинником, який забезпечує стійке функціонування алгоритмів оцінки та управління.

Література: 1. *Тихонов В. И.* Оптимальный прием сигналов. М.: Радио и связь, 1983, 387с. **2.** *Поповский В.В.* Модель управления реструкторизацией телекоммуникационной сети. //Всеукр. меж. ведом. научн-техн. ст. “Радиотехника”. Вып.138, 2004, стр. 25-32. **3.** *Абдельхамид Зугбар, Звягольская Г.В., Селевко С.Н.* Разработка математической модели состояния нестационарной телекоммуникационной системы //Всеукр. меж. ведом. научн-техн. ст. “Радиотехника”. Вып.141, 2005, стр. 1-3. **4.** *Звягольская Г.В., Селевко С.Н.* Оценка состояния нестационарной телекоммуникационной системы. //Всеукр. меж. ведом. научн-техн. ст. “Радиотехника”. Вып.141, 2005, стр. 1-9. **5.** *Поповский В.В., Сокол Г.В.* Анализ качества оптимальных процедур управления сетевыми элементами и сетями в нестационарных условиях.//Всеукр. меж. ведом. научн-техн. ст. “Радиотехника”. Вып.151, 2007, стр. 6-15.

АНАЛИЗ МОДЕЛИ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ И ДАННЫХ

Поповская Е.О.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр.Ленина, 14. каф. Телекоммуникационных систем
Тел.(057)702-13-20, E-mail: tkc@kture.kharkov.ua

We probed the non-stationary model of simultaneous transmission of real-time services and delay tolerant services. We were got results allowing to determine quality of transmission and border of stability of treatment of macro packages.

Современные телекоммуникационные сети строятся таким образом, что на узлы обработки поступают различные информационные потоки: речь, видео, данные, каждый из которых требует специфических методов передачи. В силу ограниченности сетевых ресурсов, возникает необходимость минимизации потерь каждого из потоков. Проанализируем характер указанных потерь. Будем считать, что на обработку поступает пуассоновский поток заявок, содержащий заявки реального времени, обладающих интенсивностью λ_p и интенсивностью их обслуживания μ_p,поток данных имеет параметры соответственно λ_d и μ_d. Трафик реального времени имеет абсолютный приоритет и ограничивается только пропускной способностью системы, прекращая при необходимости трафик данных.

Для передачи данных, поступающих в виде x-макропакетов, используется свободный канальный ресурс. При отсутствии такового, в отличие от трафика реального времени, оставшиеся макропакеты занимают свободные места в буфере. Среднее число макропакетов, содержащихся в одной заявке:

$$n_g = \sum_{x=1}^{C+Q} xP(x), \quad (1)$$

где C-скорость передачи, выраженная в единицах канального ресурса, Q-объем буфера в единицах макропакетов.

В силу марковости процесса обслуживания, исследование данного процесса можно проводить в предположении его стационарности. Определим вероятность состояния процесса обслуживания заявок:

$$p(n_{p1}, n_{p2}, \dots, n_{pn}, n_g), \quad (2)$$

где $n_{pi}, i = 1,2, \dots, n$-число канального ресурса связанного с выполнением i-заявки трафика реального времени. Данная вероятность может интерпретироваться, как доля времени пребывания системы в состоянии с n_pзаявками i-го потока на передачу трафика реального времени и n_gмакропакетами, находящимися на передаче или в очереди.

Определим потери трафика реального времени и данных. Вероятность потерянных заявок этого трафика:

$$\pi_r = \sum_s p(n_{p1}, n_{p2}, \dots, n_{pn}, n_g), \quad (3)$$

где S-состояния, при которых отсутствует свободный канальный ресурс для передачи данного трафика. Эти состояния удовлетворяют условию $n_p + i > C$.

Среднее число канального ресурса, расходуемого на передачу трафика реального времени:

$$m_p = \sum_s p(n_{p1}, n_{p2}, \dots, n_{pn}, n_g)\, n_p. \quad (4)$$

Потеря трафика данных, передаваемого вне реального времени, состоит из следующих компонент:

-потерь макропакетов, происшедших вследствие отсутствия свободного ресурса и занятости всех мест в очереди π_c;

-потерь макропакетов, вытесненных из обслуживания поступившей приоритетной заявкой трафика реального времени и не нашедших свободных мест в очереди π_b;

-потерь макропакетов из-за превышения времени ожидания в буфере π_d;

Все эти потери определим как отношение интенсивности соответствующих событий к интенсивности поступления макропакетов на передачу. Это позволяет интерпретировать показатели потерь π_c, π_b, π_d как соответствующие вероятности при стремлении числа событий к пределу. Поскольку указанные вероятности – независимы, то общая вероятность потерь макропакетов определяется в виде:

$$\pi_м^{(-)} = \pi_c + \pi_b + \pi_d. \quad (5)$$

Отсюда вероятность успешной доставки макропакетов определяется как дополнение к (5):

$$\pi_м^{(+)} = 1 - \pi_c - \pi_b - \pi_d. \quad (6)$$

Доля определения среднего времени нахождения макропакета в ожидании на передачу воспользуемся формулой Литтла. Это время:

$$T_м = \frac{m_{k+}\, m_d}{\lambda_g n_g (1-\pi_c)}, \quad (7)$$

где m_k, m_d- среднее значение соответственно: единиц канального ресурса, выделяемого для передачи макропакетов и мест в очереди, занятых макропакетами.

Выводы

1.В предположении пуассоновского входного потока заявок получены вероятностные характеристики мультисервисной системы при передаче трафика реального времени и трафика данных. Данные характеристики позволяют формировать показатели качества обслуживания различных сервисов.

2.Получена зависимость среднего числа макропакетов, находящихся в очереди, от интенсивности поступающего трафика данных при его стремлении к предельному значению. При стремлении λ_gк предельному значению среднее число макропакетов в очереди резко увеличивается. Одновременно обслуживающая система переходит в неустойчивый, критический режим.

3.Исследована зависимость вероятности потерянных макропакетов от размера буфера и от импульсного характера поступления макропакетов. Результаты показывают, что импульсный характер поступления макропакетов приводит к значительному росту потерь по сравнению со сглаженным трафиком. Вместе с тем, наличие буфера демпфирует импульсный характер трафика и ведет к уменьшению потерь.

МЕТОД МАКСИМІЗАЦІЇ КОРИСНОСТІ МОБІЛЬНОЇ РАДІОМЕРЕЖІ НА ОСНОВІ ПОКАЗНИКІВ СПРИЙНЯТТЯ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ

Стрюк О.Ю.
Військовий інститут телекомунікацій та інформатизації НТУУ «КПІ»
01011, м. Київ, вул. Московська, буд. 45/1
E – mail: strjuk@rambler.ru

Presented the analyses of perceived quality of service (PQoS) as the objective function of network management. The objective function for PQoS maximization in Ad Hoc Wireless Network is defined. Presents an algorithm of the bundwise allocation in the Ad Hoc Wireless Network.

Вступ. Мобільні радіомережі (Ad Hoc Wireless Networks) – це новий перспективний принцип побудови широкосмугових радіомереж, відмінною особливістю якого є самоорганізація архітектури мережі, що забезпечує реалізацію наступних можливостей:

- використання безпроводових транспортних каналів при побудові мережі за топологією «кожен з кожним»;
- масштабування мережі (зміна площі зони покриття і щільності інформаційного забезпечення) у режимі самоорганізації;
- стійкість мережі до втрати (відмови) окремих елементів;
- зменшення вартості розгортання мережі.

Незважаючи на великий потенціал мобільних радіомереж (МР), та наявні приклади практичного втілення Ad Hoc технологій у проектах побудови безпроводових мереж залишається ряд проблем, що перешкоджають їх широкому розповсюдженню. Одним з найбільш критичних факторів, які впливають на розвиток МР, є складність забезпечення для кожного з користувачів МР заданого рівня якості обслуговування (QoS, Quality of Service) – визначеної у рекомендації ITU – T P.800 як «сукупний ефект характеристик мережного сервісу, який визначає ступінь задоволеності споживача даного сервісу». Забезпечення QoS у МР потребує розробки і впровадження спеціалізованих механізмів і протоколів оперативного керування радіомережами [1].

Обгрунтування вибору сприйняття якості обслуговування як інтегрального показника якості обслуговування. Протягом останніх десяти років була розроблена концептуальна модель координаційної - крос-рівневої (cross-layer) архітектури систем оперативного керування радіомережами [2]. Основні труднощі при побудові координаційної архітектури керування радіомережею – це визначення необхідних параметрів, які будуть використовуватись між рівнями OSI та функціями керування, які дозволяють отримати користувальницьку та (або) мережеву, зонову оптимізацію.

Однією із прикладних задач мережного керування, пов'язаних із забезпеченням QoS, при вирішенні якої використовується крос-рівневий підхід, є задача максимізації корисності мережі (network utility maximization). Вперше задача максимізації корисності мережі сформульована у роботі F.Kelly [3]. Задача максимізації корисності МР, яка складається з E – ресурсних елементів, і в якій створено F – інформаційних потоків, полягає у пошуку такого вектору розподілу ресурсів МР, який задовольняє (1)

$$\mathrm{x}^{*} = \arg \max_{\{x_f\} \in \Omega} \left(\sum_{f \in F} U_f\left(x_f\right) \right) \qquad (1)$$

за умови

$$\mathrm{R} \times \mathrm{x} \le \mathrm{C}, \quad \mathrm{x} \ge 0,$$

де x_f - ресурси мережі, виділені інформаційному потоку f;

$U_f(\{x_f\})$ – значення функції корисності для інформаційного потоку f при виділенні йому x_f ресурсів мережі;

Ω - множина можливих варіантів розподілу ресурсів між інформаційними потоками у мережі;

$\mathrm{R} = (R_{ef})_{|E|\times|F|}$ - матриця розподілу ресурсів елементів мережі між інформаційними потоками у мережі;

$\mathrm{x} = (x_f,\ f \in F)$- вектор ресурсів, які виділяються інформаційним потокам.

$\mathrm{C} = (C_e, e \in E)$ – вектор місткостей ресурсних елементів мережі.

У якості інтегрального показника при оцінюванні оптимальності координаційного керування у радіомережі, безпосередньо пов'язаного з її основним призначенням – забезпеченням передавання інформації із заданою якістю, що враховує як вплив параметрів мережі, так і вплив прикладного програмного забезпечення, - може бути використане сприйняття користувачем якості інформаційної послуги [4].

Сприйняття якості обслуговування (PQoS - perceived quality of service) – це оцінка якості інформаційного сервісу з точки зору сприйняття користувачем як споживачем послуг даного сервісу. Протягом останніх років були розроблені та пройшли міжнародну верифікацію методи об'єктивного оцінювання PQoS для більшості класів інформаційних служб. Наявність об'єктивних методів оцінювання PQoS дозволяє автоматизувати процедуру визначення PQoS як величини, залежної від широкого спектру показників мережі. Для кожної з функціонуючих у мережі інформаційних служб можуть бути визначені значення багатовимірного масиву значень PQoS - $\{q_i\}$, залежні від виділених ресурсів, параметрів мережі, з урахуванням функціональності прикладного програмного забезпечення (кінцевого абонентського обладнання), яке реалізовує дану послугу

$$\{q_i\} = F(\{R_i\}, \{p\}, \{E_i\}), \qquad (2)$$

де q_i - значення PQoS за шкалою MOS для інформаційної служби i, $i \in 1,..,m$;

m – кількість інформаційних служб, які функціонують у мережі;

$\{R_i\}$– множина значень ресурсів мережі, що виділені інформаційній службі i;

$\{p\}$ - множина показників, які характеризують мережу;

$\{E_i\}$ – множина факторів, що відображають вплив на PQoS особливостей реалізації прикладного програмного забезпечення, і (або) кінцевого абонентського обладнання.

Постановка задачі координаційної оптимізації для забезпечення максимізації корисності МР на основі показників PQoS. Основними причинами зменшення рівня QoS у МР є обмеженість радіоресурсу, нестабільність радіоліній і мобільність абонентів. Найбільш вагомим ресурсом МР є пропускна спроможність радіоінтерфейсів вузлів мережі [5], тому оптимізаційна задача, рішення якої пропонується, зосереджена на максимізації повного рівня PQoS у МР за рахунок керування розподілом пропускної спроможності, кодування аудіовізуальних даних зі зміною швидкістю і з урахуванням рівня завадостійкості каналів між мережними пристроями. Вирішення запропонованої задачі забезпечує підвищення ефективності використання радіоресурсу МР.

Початкові припущення. Оптимізаційна задача вирішується, виходячи із припущення про реалізацію в технології побудови радіомережі наступних методів забезпечення інформаційного обміну і керування мережею:

- наявність механізмів класифікації, маршрутизації та відокремленої обробки інформаційних потоків, керування чергами, планування передавання;

- детермінований доступ до радіоканалу з можливістю виділення кожному інформаційному потоку певного значення пропускної спроможності з дискретністю ΔR;

- наявність зворотного службового зв'язку між мобільними абонентами з можливістю отримання інформації про рівень завадостійкості радіоканалу на приймальній стороні;

- можливість транскодування аудіовізуальних даних - зміни в реальному часі швидкості кодування та (або) формату представлення даних базовою станцією і абонентськими пристроями.

Аналіз наведених припущень показує, що всі зазначені механізми, крім транскодування, реалізовані в сучасних технологіях побудови МР [6]. Сучасні методи кодування

аудіовізуальних даних передбачають можливість кодування зі змінною швидкістю без істотної зміни формату представлення даних, що створює умови для здійснення операції транскодування в реальному часі в кінцевих та ретрансляційних вузлах мережі [7].

Вихідні дані. При вирішенні оптимізаційної задачі використовуються наступні вихідні дані: m- кількість вузлів у мобільній радіомережі; R - значення пропускної спроможності радіоінтерфейсів вузлів МР, біт\с; Δr – шаг зміни смуги пропускання, яка може виділятись для інформаційних потоків – ресурсний елемент, біт\с; k – кількість інформаційних потоків, які конкурують за доступ; способи кодування інформації в інформаційних потоках; маршрути проходження інформаційних потоків у МР; p_i – середня імовірність втрати пакету для кожного інформаційного потоку, $i \in 1,..,k$; масив значень PQoS по шкалі MOS в залежності від швидкості потоку імовірності втрати пакету для кожного з інформаційних потоків та обраного способу кодування (характеристик прикладної реалізації послуги)

$$\{q_i(r_i, p_i, E_i)\} = \{q_i(\Delta r, p_i, E_i),\ q_i(2\Delta r, p_i, E_i),\ \ldots,\ q_{i,}(B_i\Delta r, P_i, E_i)\},$$

де $B_i = \lfloor R_i^{max}/\Delta r \rfloor$;

R_i^{max} – максимально необхідна смуга пропускання для інформаційного потоку i, біт\с.

Необхідно – знайти такий вектор розподілу пропускної спроможності між інформаційними потоками у МР, при якому виконується

$$\mathrm{r}^* = \arg \max_{\{r_i\} \in \Omega} \left(\sum_{i=1}^{k} q_i\left(r_i, p_{i,}, E_i\right) \right) \tag{2}$$

за умови

$$\Delta \mathrm{R} \times \mathrm{r} \le \mathrm{C},$$

де $\mathrm{r}^* = \left(r_i, i = 1,\ldots,k\right)$ – вектор розподілу пропускної спроможності між інформаційними потоками, який забезпечує вирішення задачі (2);

Ω – множина можливих значень вектору розподілу пропускної спроможності між k – інформаційними потоками, при дискретності зміни пропускної спроможності Δr;

$\Delta \mathrm{R} = \left(\Delta R_{ji}\right)_{|m+1| \times |k|}$ - матриця розподілу пропускної спроможності радіоінтерфейсів вузлів МР між інформаційними потоками;

$\mathrm{C} = (R_j, j = 1,\ldots,m+1)$ – вектор пропускної спроможності радіоінтерфейсів вузлів МР.

Для вирішення оптимізаційної задачі (2) пропонується використовувати алгоритм, який базується на пошуку максимальної кліки у графі МР, найближчим прототипом якого є алгоритм запропонований у [8].

Алгоритм координаційної оптимізації для забезпечення максимізації корисності МР на основі показників PQoS ініціалізується у випадку необхідності перерозподілу ресурсів МР при початку (закінченні) сеансу зв'язку, або з заданою періодичністю, яка, згідно умови стохастичної стійкості алгоритмів керування розподілом ресурсів мережі, має відповідати співвідношенню:

$$T_r \approx T_c < T_s, \tag{3}$$

де T_r – середній час, необхідний для здійснення розподілу ресурсів;

T_c – інтервал кореляції зміни параметрів мережі;

T_s – середня тривалість сеансів зв'язку.

Результатами виконання алгоритму є вектор розподілу пропускної спроможності між інформаційними потоками, який забезпечує вирішення задачі (2), та матриця розподілу пропускної спроможності радіоінтерфейсів вузлів МР між інформаційними потоками.

Для експериментальної перевірки ефективності використання запропонованого методу із використанням системи комп'ютерної математики Matlab створена математична модель алгоритму максимізації корисності МР на основі показників PQoS.

Результати математичного моделювання показують, що максимізація корисності мережі на основі показників PQoS дозволяє досягти 20 - 30 % переваги у порівнянні із значеннями PQoS, яких дозволяє досягти управління розподілом ресурсів мережі на основі пріоритетності аудіовізуального трафіку, і 5 - 10 % переваги у порівнянні із значеннями PQoS, яких дозволяє досягти управління розподілом ресурсів мережі на основі значень функції корисності.

Висновки. У доповіді доведена можливість і перспективність використання значення сприйняття якості обслуговування в якості показника в задачах мережного керування. Запропонований метод координаційної зонової оптимізації максимізації корисності МР на основі показників PQoS. Запропонований метод відрізняється від відомих використанням у якості цільової функції оптимізації – PQoS, залежної від пропускної спроможності, рівня завадостійкості та способу реалізації інформаційної послуги. Результати, яких дозволяє досягти запропонований метод, перевищують результати стандартних та відомих перспективних методів забезпечення максимізації корисності МР. Під час подальших досліджень передбачається розширення переліку ресурсів радіомережі, керування якими забезпечує вирішення задачі забезпечення максимізації корисності мобільної радіомережі.

Література:

1. Миночкин А.И. Управление качеством обслуживания в мобильных радиосетях / А.И. Миночкин, В.А. Романюк // Зв'язок. – 2005. – № 8. – С. 17 – 23.

2. Романюк В.А. Архітектура системи оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2009. - №3. – С. 70 – 76.

3. Kelly F. Charging and rate control for elastic traffic / F. Kelly // European Transactions on Telecommunications. – 1997. - №8 – P. 33–37.

4. Батлер Ю.В. О качестве услуг в IP – сетях / Ю.В. Батлер, В.Ф. Михайлов // Зв'язок. – 2006. – №6. – С. 2 – 6.

5. Resource management in wireless networking / edited by M. Cardei, I. Cardei, D-Z. Du– Springer, 2005. – 716 p.

6. Advances in Wireless Ad Hoc and Sensor Networks / edited by X. Cheng and D. Li. Springer, 2008. – 316 p.

7. Multimedia Transcoding in Mobile and Wireless Networks / edited by M. Ashraf, A. Ibrahim - IGI Global, 2009. – 439 p.

8. Xue Y. Optimal resource allocation in wireless ad hoc networks: a price-based approach / Y. Xue, L. Baochun, K. Nahrstedt // IEEE Transactions on Mobile Computing. – 2006. – Vol. 5. – Is. 4. – P. 347 – 364.

ТРЕБОВАНИЯ К ПЕРСПЕКТИВНЫМ СРЕДСТВАМ КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ ПЕРЕГРУЗОК В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Старкова Е.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: Elena_Starkova@ukr.net

The given work is devoted to the problems of congestion control and congestion avoidance in networks. It is noted that the most common means of congestion avoidance are Active Queue Management (AQM) algorithms, implemented on the routers. AQM algorithms have been designed to be able to actively control the average queue length in routers supporting TCP traffic, and thus to be able to prevent congestion and resulting packet loss as much as possible. The basic drawbacks of these algorithms are indicated and the requirements that they must satisfy are formulated.

Современные телекоммуникационные системы (ТКС) характеризуются неуклонным ростом количества пользователей, предоставляемых услуг и разработкой и усовершенствованием различных сетевых технологий. Тенденции развития ТКС указывают на внедрение и развертывание концепции сетей следующего поколения Next Generation Network (NGN) [1], отличительной особенностью которых является предоставление широкого спектра услуг, включая услуги в реальном времени и услуги доставки информации, в том числе мультимедийные услуги, через единую инфраструктуру. При этом возрастают и требования, которые предъявляются к качеству обслуживания предоставляемых услуг, регламентируемых в различных международных и местных стандартах, например, ITU-T. При этом эффективность телекоммуникационных сетей во многом зависит от результативности решения задач управления сетевыми ресурсами. К таким средствам относятся протоколы маршрутизации, алгоритмы профилирования трафика, дисциплины обслуживания и ограничения очередей, алгоритмы явного уведомления о перегрузках, а также механизмы контроля перегрузок, заложенные в протокол транспортного уровня TCP.

Немаловажную роль играют механизмы контроля и предотвращения перегрузок, которые могут быть классифицированы различными способами и по различным признакам. Одна из основных классификаций основана на том, где именно реализован механизм: на оконечных (Primal, end-system-based, source-based, TCP-friendly protocols) или на промежуточных устройствах сети (Dual, router-based). Примерами первых являются различные механизмы борьбы с перегрузками, заложенные в протокол TCP, отвечающий за надежную доставку пакетов получателю - Rate Adaptation Protocol (RAP), Loss-Delay Based Adaptation Algorithm (LDA), Inverse-Increase/Additive-Decrease (IIAD).

Однако протокол TCP обнаруживает перегрузку после того, как пакет был отброшен из очереди. Ситуация постоянной загруженности очередей крайне нежелательна, поскольку это существенно увеличивает задержку доставки пакетов получателю. Следовательно, с учетом постоянно увеличивающихся скоростей передачи в сетях все более существенной становится необходимость использования механизмов, позволяющих удерживать производительность на высоком уровне, при этом сохраняя размер очереди минимальным насколько это возможно. Для того, чтобы выполнить данное требование, протокол TCP в процессе борьбы с перегрузками зачастую полагается на результат работы дисциплин ограничения очередей, реализуемых на промежуточных устройствах – маршрутизаторах. Такое решение было реализовано исходя из того факта, что обнаружение перегрузки может быть осуществлено более эффективно именно на самом маршрутизаторе. Маршрутизатор может достаточно четко разграничивать задержки распространения и продолжительные задержки пакетов в очереди. Только у маршрутизатора есть целостное представление об изменении состояния очереди во времени.

Наибольшее распространение среди дисциплин ограничения очередей получили AQM-алгоритмы [2-5], к числу которых относятся Random Early Detection (RED) и мно-

жество его модификаций – Weighted RED, Adaptive-RED (ARED), Fair Random Early Detection (FRED), Balanced RED (BRED), Stabilized RED (SRED), Double Slope Random Early Detection (DSRED). Согласно принципам работы подобных алгоритмов для предотвращения перегрузки сети используется превентивный подход, согласно которому вместо ожидания фактического переполнения очереди, отбрасывание пакетов начинается с ненулевой вероятностью, когда средний размер очереди превысит определенное минимальное пороговое значение. Основными целями AQM-алгоритмов являются [2-5]:

1. Обеспечение механизма заблаговременного обнаружения сетевых перегрузок, который начинает отбрасывание пакетов из очереди на маршрутизаторе до того, как перегрузка существенно повлияет на производительность сети. При этом существенность этого влияния зависит от параметров Quality of Service (QoS), требуемых при доставке пакетов того или иного трафика.
2. Уменьшение количества потерь пакетов, возникающих вследствие переполнения буферного пространства маршрутизаторов, что достигается за счет поддержки величины среднего значения очереди достаточно малой, следовательно, оставляя место для временных всплесков.
3. Поддержка интерактивных сервисов, критичных к задержке, поскольку гарантия небольшой величины среднего значения очереди способствует малым задержкам из конца в конец.
4. Предотвращение случаев блокировки (lock-out) потоков с низкой скоростью передачи и пульсирующих потоков и гарантия справедливого обслуживания различных типов трафика.

Однако проведенный анализ показал, что основными недостатками AQM-алгоритмов является

- отсутствие согласованности решения задач контроля и предотвращения перегрузок при управлении трафиком из конца в конец и на промежуточных устройствах (с результатами работы протоколов маршрутизации, протоколов управления трафиком на транспортном уровне);
- отсутствие у большинства AQM-алгоритмов возможностей адаптироваться к различным интенсивностям трафика и другим параметрам сети;
- чувствительность к количеству источников/потоков, претендующих на сетевые ресурсы;
- концентрация внимания лишь на одном аспекте проблемы (например, решение задачи по обеспечению справедливости обслуживания различных типов трафика, по уменьшению сложности реализации или вычислительных затрат);
- отсутствие ограничений для агрессивных, неадаптиивных потоков (например, использующих протокол UDP для транспортировки), что имеет негативное влияние на TCP-потоки, уменьшающие интенсивность передачи при обнаружении потери пакета;
- в основе этих алгоритмов зачастую лежат эвристические схемы обслуживания очередей, которые являются причиной низкой производительности соединений и увеличения значения задержка/джиттер.

Перечисленные недостатки алгоритмов и механизмов управления трафиком являются факторами, которые приводят к неустойчивости функционирования ТКС вследствие потерь пакетов данных и колебаний интенсивности трафика. Такие последствия становятся очевидными, поскольку реакцией на потери пакетов являются их повторная передача в рамках TCP-сеансов (отсюда возникновение эффекта глобальной синхронизации (global synchronization), для борьбы с которым на сегодняшний день существует лишь алгоритм RED).

Принимая во внимание вышеперечисленные недостатки можно сформулировать следующие требования к перспективным AQM-алгоритмам:

- учет требований по задержке и производительности одновременно. Некоторые AQM-алгоритмы могут удовлетворять требованиям отдельных типов трафика, однако эти

алгоритмы слишком сложно реализуемы и неприменимы в условиях высокой загруженности, что влечет высокие вычислительные затраты;

- учет особенностей широковещательного и многоадресного трафика, игнорирование которых приводит к низкой эффективности использования пропускной способности и низкому качеству получаемой услуги;
- учет различных сетевых параметров и условий (например, уровень загруженности). В основном современные AQM-алгоритмы используют настройку интенсивности отбрасывания пакетов для борьбы с проблемой перегрузки сети, не принимая во внимание другие сетевые параметры и условия (например, уровень загруженности);
- адаптивность к постоянно меняющимся условиям функционирования сети, что снизит необходимость в административной настройке большого количества параметров;
- использование математических моделей отбрасывания пакетов, закладываемых в основу алгоритма и позволяющих более эффективно реагировать на перегрузки, особенно в условиях высокой загруженности сети.

Таким образом, в виду стремительного развития телекоммуникационных технологий, гетеродинности трафика, расширения перечня услуг и ужесточения требований к их качеству немаловажным аспектом является обеспечение эффективного функционирования сети. Это достигается за счет использования различных средств управления сетевыми ресурсами, в том числе алгоритмов и механизмов контроля и предотвращения перегрузок, к которым относятся алгоритмы активного управления очередями AQM. Несмотря на существование множества подобных алгоритмов [2-5], наибольшее распространение среди которых получил алгоритм раннего обнаружения перегрузок RED, практика показывает ряд присущих им недостатков, которые приводят к неэффективному использованию сетевых ресурсов, потерям пакетов и снижению производительности сети. Среди прочего к таким последствиям приводят несовершенство математических зависимостей для расчета вероятности отбрасывания пакетов, которые лежат в основе работы AQM-алгоритмов. Следовательно, актуальной является задача пересмотра и усовершенствования математических моделей отбрасывания пакетов, более точно отражающих процессы функционирования сети с целью недопущения перегрузок при сохранении относительной простоты реализации алгоритма.

Литература:

1. Бакланов И. Г. NGN: принципы построения и организации / И. Г. Бакланов; под ред. Ю. Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с.

2. G. Thiruchelvi A Survey On Active Queue Management Mechanisms / G. Thiruchelvi, J. Raja // IJCSNS International Journal of Computer Science and Network Security. – 2008. – Vol. 8, №. 12. – Pp. 130 – 145.

3. M. Lestas Queue length based Internet congestion control / M. Lestas, A. Pitsillides, P. Ioannou and G. Hadjipollas // IEEE International Conference on Networking, Sensing and Control. – 2007. – Pp. 584 – 589.

4. I-Shyan Hwang QoS-Aware Active Queue Management for Multimedia Services over the Internet / I-Shyan Hwang, Bor-Jiunn Hwang, Pen-Ming Chang, Cheng-Yu Wang // Proceedings of the International MultiConference of Engineers and Computer Scientists, IMECS 2010. – 2010. – Vol II. – Pp. 774 – 779.

5. G.F.Ali Ahammed Analyzing the Performance of Active Queue Management Algorithms / G.F.Ali Ahammed, Reshma Banu // International journal of Computer Networks & Communications (IJCNC). – 2010. – Vol.2, No.2. – Pp. 36 – 55.

УПРАВЛЕНИЕ НАЗНАЧЕНИЕМ ДЛИН ВОЛН СВЕТОВЫМ МАРШРУТАМ В СЕТЯХ DWDM

Агеев Д.В., Переверзев А.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. ТКС, тел. (057) 702-13-06,
E-mail: tks@kture.kharkov.ua ; факс (057) 702-11-13

The technology of wavelength division multiplexing provides the most scalable and cost-effective way to increase the capacity of fiber-optic channels than technology that does not use multiplexing streams of fiber-optic channels. In addition to the methods described above, there is a method for solving RWA based on the use of optical converters, they can be used to change the wavelength of the light route, thus greatly increasing network capacity, but the cost of building such a network is also growing. The proposed method takes into account the distribution of wavelengths FWM nonlinear phenomenon by introducing additional constraints: the total input power, the use of the frequency plan with a distance between the frequencies of wavelengths

Развитие современных мультисервисных телекоммуникационых систем характеризуется предоставлением большого числа сервисов, что приводит к увеличению объема передаваемого трафика. Для передачи большого объема трафика между сетями используют транспортные сети. Большой объем передаваемого трафика выдвигает требование к транспортной сети по обеспечению больших скоростей, по этой причины современных транспортные сети строятся на основе технологии волоконно-оптических сетей DWDM. DWDM относиться к сетям маршрутизации длин волн, где передача трафика между узлами сети происходит через световой маршрут. Световой маршрут – это оптическое соединение точка – точка использующие определенную длину волны вдоль всего маршрута передачи потока.

Технология мультиплексирования по длине волны позволяет получить наиболее масштабируемый и рентабельный способ увеличение пропускной способности волоконно-оптических каналов, чем технология, которая не использует мультиплексирование потоков в волоконно-оптических каналов. Среди задач, которые необходимо решить при построении транспортной сети на основе технологии DWDM, есть задача распределения длин волн.

Цель данной работы является повышение качества передаваемых услуг в полно-оптических сетях DWDM (без использования оптических конверторов) за счет уменьшения числа коллизий.

При использовании сетей на основе технологии DWDM основными задачами управления являются: маршрутизация и назначения длин волн световым маршрутам (RWA). Основные методы решения задачи RWA приведены ниже:

– Статическое распределение;

– Динамическое распределение;

Статическое распределение применяется при условии, что назначенный порядок длин волн световым маршрутам и распределения световых маршрутов не изменяются или изменяются редко (единицы изменения месяцы).

Динамическое распределение применяется при условии, что назначенный порядок длин волн световым маршрутам и распределения световых маршрутов изменяются довольно часто (единицы изменения минуты).

Кроме методов приведенных выше, есть метод решения задач RWA основанный на применении оптических конверторов, с их помощью можно изменять длину волны в световом маршруте, вследствие чего значительно расширяется пропускная способность сети, однако стоимость построения такой сети так же растет.

Решение задачи RWA можно разделить на две подзадачи: задача маршрутизации и задача назначения длин волн этим маршрутам. Эта работа посвящена методу назначения длин волн световым маршрутам, при котором уменьшается количество коллизий.

В данной работе рассматривается метод статического распределения при решении задачи RWA. Решения задачи распределения использованных длин волн в сети на основе технологии WDM были рассмотрены в работах [1, 2, 3]. Однако все эти работы имели общие ключевые недостатки:

–не учитывается необходимое расстояние между длинами волн;

–не ограничивается количество длин волн согласно частотному плану;

–не учитываются нелинейное явление четырехволнового смешивания (ЧВС).

ЧВС – явление, возникающее при передачи трех или более световых сигналов w_i, w_j и w_k, распространяющихся по одному волокну, возникают паразитные сигналы, которые приводят к коллизиям с полезным передаваемым сигналом. Длину волны, на которой возникают паразитные сигналы можно определить с помощью выражения:

$$w_{ijk} = w_i + w_j - w_k \quad (1)$$

Последствием ЧВС является появление побочных сигналов, некоторые из которых могут соответствовать частотам рабочих каналов, которое может привести к росту ошибок и ухудшению эффективности системы DWDM. Приведем способы уменьшения влияния ЧВС:

–уменьшение мощности оптического сигнала в канале DWDM;

–увеличение частотного расстояния между длинами волн, использующихся в одном волокне.

Из работы [4] получим значение допустимого предела мощности появления ЧВС суммарной от мощности накачки. Для удобства расчета необходимо получить граничное значение в виде мощности входного сигнала. Используя работу [3] выведем формулу зависимости мощности накачки от суммарной мощности сигнала.

$$P_p = P_{вх} \cdot G / E_q \quad (2)$$

где P_p – мощность накачки, $P_{вх}$ – входная мощность сигнала, G– коэффициент усиления усилителя, E_q – квантовая эффективность излучателя.

На основании выражения(1,2) можно получить выражения допустимого значения мощности:

$$P_d = P_p \cdot E_q / G \quad (3)$$

Ограничение на суммарную мощность входного сигнала:

$$\sum_{k \in K} \sum_{\lambda \in \Lambda} P_0 \cdot \alpha_p \cdot L_e \cdot \alpha_e \cdot x_{ke}^{\lambda} \le P_d, \quad (4)$$

где k – соединение между парой источник-получатель, λ – длина волны, e – канал связи, P_0 – начальная мощность сигнала, L_e – длина волокна, α_e – затухание в волокне, α_p – затухание, вносимое оптическими разъемами,

$x_{ke}^{\lambda} = \begin{cases} 1, \text{если используется в } e \text{ канале связи длина волны } \lambda \text{ при k соединении;} \\ 0, \text{иначе.} \end{cases}$

Введем ограничение на использование частотного плана с растоянием между частотами длин волн в 100 ГГц:

$$M \cdot y_e \ge \sum_{k \in K} \sum_{\lambda \in \Lambda} x_{ke}^{\lambda}, e \in E, \quad (5)$$

где M – количество каналов частотного плана (в нашем случае 40);

где $y_e = \begin{cases} 1, \text{если используется } e \text{ канал связи;} \\ 0, \text{иначе.} \end{cases}$

Существует ряд методов назначения длин волн маршрутам. Описание методов назначения длин волн при выборе световых путей приведены в работе [1]. Наиболее распространенными являются метод First-fit и Random.

Суть метода Random заключается в том, что при передачи трафика от отправителя к получателю используемая длина волны назначается случайным образом.

Метод First-fit реализуется предварительным определением порядка длин волн, при передачи трафика от отправителя к получателю используемая длина волны назначается, с самым низким индексом.

Недостатком метода Fitst-fit является неравномерное использование заданного частотного диапазона длин волн при назначении световым маршрутам, статистические данные исследования приведены ниже.

Поэтому рассмотрим метод ”Гибридный”. Опишем алгоритм метода: на первой итерации равномерно распределяются длины волн с шагом между частотами 3; на второй итерации с шагом 7; на третьей с шагом 11; на четвертой итерации с шагом 13; на следующей итерации случайным образом выбираются длины волн. Таким образом, предложенный метод исключает недостаток метода First-fit. Метод “Гибридный” является объединением предыдущих методов: при не большом количестве необходимых длин волн метод ведет себя как First-fit только с изменяющимся шагом между частотами длин волн; при большом количестве необходимых длин волн небольшое количество длин волн выбирается методом First-fit с изменяющимся шагом между частотами длин волн, а остальная часть с помощью метода Random.

Проведем сравнение этих методов на заданных топологиях оптической сети по параметру количества коллизий между полезным сигналом и сигналами-помехами возникающими при явлении ЧВС.

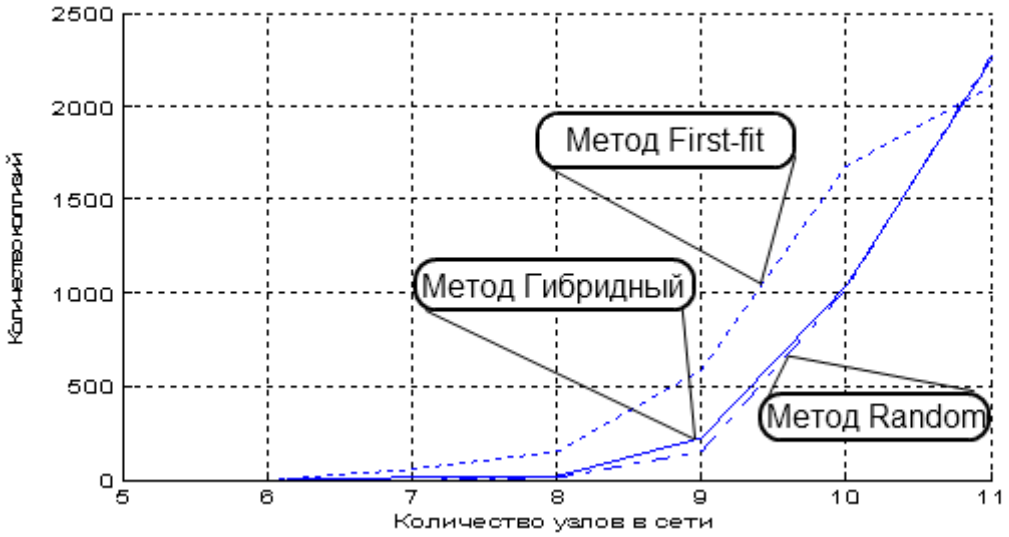


Рис. 1 Зависимость количества коллизий от числа узлов сети для различных методов

Таблица 1

Количество узлов в топологии сети	Количество коллизий		
	Метод First-fit	Метод Random	Метод “Гибридный”
7	52	0	8
8	152	8	16
9	592	148	220
10	1680	1020	1032
11	2112	2280	2256

На рис.1 показан анализ зависимости методов назначения длин волн световым маршрутам от количества узлов в сети и числа коллизий между полезным сигналом и сигналами-помехами.

Из результатов анализа таблицы 1 видно, что метод Random обеспечивает более равномерное загрузку выделенного диапазона длин волн и как следствие более равномерное расстояние между использованными длинами волн. Но при числе узлов более 10, это преимущество теряется, все три метода показывают близкие результаты однако, методы First-fit и ”Гибридный” обеспечивает меньшее количество коллизий. Это можно объяснить тем, что задействовано большое количество длин волн из заданного диапазона поэтому метод Random не эффективно применять.

В результате проведенного в работе исследования можно сделать вывод, что ранее известные методы решения задачи управления распределения длин волн использующихся в транспортной сети на основе технологии DWDM имеют общий недостаток – не учитывалось нелинейного явления четырехволнового смешивания.

Предложенный метод распределения длин волн учитывает нелинейное явление ЧВС за счет введения дополнительных ограничений: на суммарную мощность входного сигнала; на использование частотного плана с растоянием между частотами длин волн в 100 ГГц. Так же был проведен сравнительный анализ методов назначения длин волн световым маршрута: First-fit, Random, ”Гибридный” предложенный по параметру – количество коллизий. В ходе которого можно сделать вывод, что эффективнее использовать предложенный метод ”Гибридный” чем существующие методы, так как, при небольших размерностях топологий сети он эффективнее чем First-Fit, а при больших размерностях лучше чем Random по критерию количества коллизий.

Литература: 1. *Ramaswami, R.* Routing and wavelength assigment in all-optical networks / R. Ramaswami, K.N. Sivarajan // IEEE/ACM Transaction on Networking. 1995. 5(3). P.489-501.

2. *Baroni,* S. On the number of wavelengths in arbitrarily-connected wavelength-routed optical networks/ S. Baroni, P. Bayvel, R.J. Gibbens // Optical Society of America/TOPS. 1998. 20. P. 195-204.

3. *Mauricio, G. C.* Handbook of Optimization in Telecommunications. New York:Springer Science + Business Media, 2006. 1120 p.

4.Агравал Г. Нелинейная волоконная оптика. – М.: Мир Год,1996.– 324 с..

ПОСТРОЕНИЕ МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ МЕТОДОВ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ И УЧЕТОМ ТРЕБОВАНИЙ СПЕЦИФИКАЦИЙ MUSE

Игнатенко А.А., Агеев Д.В., Хайдара Абдалла
Харьковский Национальный Университет Радиоэлектроники
61166, Украина, г.Харьков, пр. Ленина 14, каф. ТКС, тел (057) 702-13-20
E-mail:sanitarium@ukr.net

This thesis provides an overview of the approaches to the design of modern multiservice telecommunication systems. It contains the analysis of a wide range of problems which need to be solved in order to design the networks meeting the given criteria. Network design using integer programming methods is considered in the thesis. It also outlines the recommendations proposed in the framework of Muse project. The most important of these recommendations are pointed out and considered.

Концепция сети связи следующего поколения (NGN) предполагает построение сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений. Для этого необходимо обеспечить реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

Мультисервисные сети представляют собой самостоятельный класс сетей, строящихся на основе концепции NGN, на базе которых может быть осуществлено предоставление широкого набора как традиционных, так и новых услуг.

Процесс проектирования мультисервисных сетей предполагает решение некоторого множества оптимизационных задач для обеспечения заданных требований к топологии проектируемой сети, ее пропускной способности, значений задержки, джиттера и т.д. Для решения этих задач, могут применяться широкий спектр различных алгоритмов и методов оптимизации.

В частности, для решения широкого спектра задач, возникающих при проектировании сети, могут использоваться методы линейного частично-целочисленного программирования. Данные методы могут использоваться для решения разных типов задач, таких как минимизация стоимости многопродуктового потока, проектирование сетей с ограниченной пропускной способностью, расчет загрузки сети, построение сети с учетом ограничивающих условий топологии и/или маршрутизации и т.д.

Общая задача оптимизации может быть формализована в виде задачи минимизации $c^T x$ при условии что $Ax \geq b$ и $x \in Z_+^n$. Здесь Z_+^n описывает множество неотрицательных целочисленных точек. Проблема сводится к нахождению оптимального решения x^*. Для решения сложных задач целочисленного программирования используются так называемые релаксации, то есть упрощение задачи, которое приводит к появлению нижнего предела оптимальной целевой функции. Нижний предел может использоваться в сочетании с верхним пределом. Данный метод позволяет проводить оценку качества полученного решения.

Хорошим решением для реализации релаксаций является применение метода ветвей и границ. В его основе лежит идея последовательного разбиения множества допустимых решений на подмножества. На каждом шаге метода элементы разбиения подвергаются проверке для выяснения, содержит ли данное подмножество оптимальное решение. Проверка осуществляется посредством вычисления оценки снизу для целевой функции на данном подмножестве. Если оценка снизу не меньше *рекорда* — наилучшего из найденных решений, то подмножество может быть отброшено. Проверяемое подмножество может быть отброшено еще и в том случае, когда в нем удается найти наилучшее решение. Если значение целевой функции на найденном решении меньше рекорда, то

происходит смена рекорда. По окончанию работы алгоритма рекорд является результатом его работы.

Данный метод в комбинации с Лагранжевой релаксацией можно, применять, к примеру, при проектировании колец первичной сети SDH, а также для оптимального выбора путей при доставке multicast-трафика.

Однако, кроме математического аппарата, построение любой сложной системы предполагает наличие некоторых методик и рекомендаций, стандартизирующих процесс проектирования и регламентирующих значение тех или иных параметров элементов системы. На сегодняшний день не существует единого общепризнанного стандарта для проектирования и построения мультисервисных сетей, однако авторы данного доклада считают целесообразным использовать в качестве такого стандарта набор рекомендаций, сформулированных в наборе документов проекта MUSE (Multi-Service Access Everywhere).

Основная идея MUSE заключается в создании некоей стандартизирующей базы. Эта база должна иметь набор технических рекомендаций для проектирования и построения мультисервисной сети, которая характеризовалась бы низкой стоимостью и возможностью доступа с применением любой технологии, что предоставляло бы пользователю повсеместный доступ к широкополосным сервисам.

Одним из важнейших вопросов, затронутых в MUSE, является мультиплексирование доступа. Подробно описаны требования к аппаратной части и структурные схемы размещения мультиплексоров доступа. Отдельно рассмотрены шлюзы TVoIP так как услуги IP-телевидения также должны предоставляться мультисервисной сетью.

Кроме того, MUSE выделяет основные требования к приложениям. Термин *nomadism* в описаниях MUSE следует понимать как независимость от типа линии связи и местоположения абонента. Требования пользователя к сети расписаны в виде набора параметров QoS, для которых приведены допустимые численные значения. Так, требование пользователя «доступность сети» формализовано в таких параметрах QoS как вероятность блокировки, время установки соединения и т.д. Приведены требования к полосе пропускания для разного вида трафика. Также приведены требования к безопасности, к именованию и адресации в сети, к типу коммутации виртуальных каналов в зависимости от типа потоков.

Однако MUSE не ограничивается лишь техническими рекомендациями. Подробно описана бизнес-модель распределения сетевых функций и требования симметричности или асимметричности канала в зависимости от вида сервиса. В данной бизнес-модели четко регламентированы функции каждого участника процесса для обеспечения вышеперечисленных требований.

Проект MUSE представляет собой продуманный и планомерный подход к проектированию мультисервисных сетей следующего поколения. Использование рекомендаций MUSE, на наш взгляд, поможет облегчить и упорядочить работы по проектированию и построению таких сетей.

Литература:

1. D A1.2 - Network Requirements for multi-service access. A. Elizondo Ermingol, G. Gallizo Rueda, Telefónica I+D, Emilio Vargas, 6 – 28043 Madrid, SPAIN.

2. DTF1.1 – Reference Models for a European Multi-service Access Network. Peter Adams, BT peter.f.adams@bt.com

3. Мультисервисные сети следующего поколения: потребности рынка, принципы, мониторинг. Дмитрий Чижиков, IKSMEDIA.RU.

РЕКУРСИВНАЯ ПОТОКОВАЯ МОДЕЛЬ MPLS

Овчинников К.А, Руккас К.М., Горюнов А.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: vonhaimek@gmail.com ; факс (057) 702-13-20

The given work is devoted to the modeling of modern telecommunication systems. Flow modeling problems has been described. A new flow model for MPLS with losses and delays has been suggested.

Современные телекоммуникационные системы (ТКС), активно развивающиеся на протяжении последних 20 лет, представляют собой сложные распределенные системы, функционирующие на множестве протоколов и использующие различные технологии. Распространенные технологии и протоколы создавались в различные промежутки времени для обеспечения различных задач, что породило проблему совместимости этих сетей. Для решения задачи совместимости была разработана технология коммутации по меткам MPLS (Multiprotocol Label Switching), обеспечивающая общую транспортную среду для одновременной передачи трафика IP (Internet Protocol), ATM (Asynchronous Transport Mode), Frame Relay. Второй, не менее важной и актуальной задачей, которая ставится перед современными ТКС, является передача трафика с обеспечением заданных параметров QoS (Quality of Service, качество обслуживания), в первую очередь, времени доставки и вероятности потери пакета, обусловленных особенностями мультимедийного трафика. Важно понимать, что гарантии качества могут предоставляться только в случае сквозной маршрутизации с резервированием ресурсов вдоль пути, в остальных случаях речь идет лишь о некотором вероятностном показателе. Из вышесказанного следует, что наиболее распространенная технология IP с маршрутизацией hop-by-hop (от узла к узлу) не способна обеспечивать требования QoS в полной мере, что обуславливается, в первую очередь, отсутствием необходимых механизмов в самом протоколе. Возникновение технологии MPLS совпало с кризисом поиска методов обеспечения QoS в IP, что послужило причиной расширения возможностей MPLS как транспортной сети в сторону механизмов гарантирования качества обслуживания и TE (Traffic Engineering, управление трафиком). Таким образом, технология MPLS представляется перспективным направлением развития современных ТКС.

Разработка методов обеспечения QoS и TE неразрывно связана с моделированием поведения ТКС, что позволяет провести апробацию алгоритмов управления с помощью машинного эксперимента, предшествующего этапу разработки оборудования и ПО (программного обеспечения). На сегодняшний день можно выделить два основных направления развития моделей ТКС: потоковые модели, имитирующие поступление потока трафика с заданными требованиями на узел ТКС, и пакетные модели, рассматривающие потоки информации как совокупность пакетов данных различного размера и с различными требованиями к передаче. Ни один из данных подходов не позволяет в полной мере отразить особенности поведения ТКС: исходя из особенностей подхода, потоковые модели чаще всего используются для моделирования поведения сети, а пакетные – для моделирования узлов связи. В данной работе предлагается адаптация потоковой модели для технологии MPLS, а разработка модели отдельного узла является направлением дальнейших исследований.

Постановка задачи потоковой модели и ее формализация приведены в [1]. Для существующих потоковых моделей характерны следующие недостатки:

- статичность (решение задачи в фиксированный момент времени);
- отсутствие потерь (предполагается, что размер БЗУ на узлах неограничен);
- отсутствие задержки пакетов в очереди (следует из предыдущего).

Данные недостатки были учтены при разработке потоковой модели для MPLS.

Пусть сеть задана графом $G=(V,E)$, где V – множество узлов сети (vertices, вершины), E – множество каналов между ними (edges, дуги). Исходя из особенностей MPLS, все множество узлов разбивается на два подмножества: $V^+=\{V_i^+, i=\overline{1,n_{LER}}\}$, множество граничных маршрутизаторов (LER, Label Edge Router), составляющих периферию сети и реализующих основной интеллект сети, и $V^-=\{V_i^-, i=\overline{1,n_{LSR}}\}$, множество коммутаторов меток (LSR, Label Switching Router), составляющих ядро сети и выполняющих исключительно задачу коммутации по меткам. При разбиении на подмножество должно выполняться условие:

$$\begin{cases} V^+ \cup V^- = V \\ V^+ \cap V^- = \varnothing \end{cases} \quad (1)$$

В свою очередь, каждый элемент множества V^+ может являться и источником трафика s (source), и получателем d (destination). Под источником трафика понимается, что на данный маршрутизатор поступает трафик от смежной сети (IP, MPLS, ATM или др.) и он должен быть доставлен на узел-получатель, также являющийся точкой соприкосновения со смежными сетями. Будем рассматривать случай, когда каждый граничный маршрутизатор LER является одновременно источником и получателем. LER не может являться получателем трафика, поступившего на него из смежной сети.

Предположим, что в каждый момент $k \in K$ (K – множество событий) на один из граничных маршрутизаторов поступает трафик интенсивностью $\lambda(k)$, относящийся к одному из классов обслуживания $q \in Q$ (в MPLS на маркировку класса обслуживания отводится 3 бита, т.о. возможно всего 8 классов). Каждому классу обслуживания соответствуют значения максимально допустимой задержки τ_q (delay) и максимально допустимого процента потерь l_q (losses). Если количество классов обслуживания трафика, поддерживаемых смежной сетью, не равно 8, то необходимо дополнительно указать правила преобразования классов. Каждому трафику ставится в соответствие пара (s,d), указывающая, на какой узел поступает трафик и через какой узел трафик покидает сеть. Вероятность того, что в один и тот же момент k на два и более граничных маршрутизаторов поступит новый поток трафика, принимается равной 0. Таким образом, через $\lambda_{(s,d)}^{q}(k)$ обозначим, что на k-м шаге на граничный маршрутизатор s поступает трафик интенсивностью λ, относящийся к q-му классу обслуживания, который необходимо доставить на узел d не превышая заданных максимально допустимых значений задержки τ_q и потерь l_q.

Важной подзадачей данной модели является описание механизма высвобождения занятых трафиком сетевых ресурсов при окончании передачи данного трафика. В реальных сетях это происходит на основе данных, поступающих от протокола маршрутизации, поддерживающего сообщения о доступной полосе пропускания (например, CSPF), либо на основе заголовков пакетов, указывающих на окончание сессии передачи. Для моделирования этого процесса введем дополнительную переменную $\varepsilon_{(s,d)}^{q,k_0}(k)=\{0,1\}$, указывающую, что на k-м шаге на граничный маршрутизатор s перестал поступать трафик класса q ($\varepsilon=1$), который был принят на обслуживание в момент k_0 и должен был передаваться на узел d. Таким образом, данная переменная содержит все необходимые данные для определения сетевых ресурсов, подлежащих высвобождению.

Каждый узел сети на k-м шаге характеризуется:

- производительностью μ;
- коэффициентом потерь $P_j^{q,(s,d)}(k) \in P$;

• средним временем ожидания пакета в очереди $T_j^{q,(s,d)}(k) \in T$.

Переменная $P_j^{q,(s,d)}(k)$, $j = \overline{1,|V|}$, равна % потерь на узле трафика с классом обслуживания q, маршрутизируемого между узлами (s,d) на шаге k, $|V|$ – мощность множества V или же количество узлов (маршрутизаторов). Предполагается, что вероятностью искажения пакета в тракте передачи можно пренебречь и потери происходят исключительно на узлах сети из-за переполнения запоминающего устройства (ЗУ). На величину потерь накладывается следующее ограничение:

$$0 \le P_j^{q,(s,d)}(k), \quad \sum_j^{|V|} P_j^{q,(s,d)}(k) \le l_q \qquad \text{для всех узлов сети } j = \overline{1,|V|}. \tag{2}$$

Таким образом, из ограничения (2) следует, что суммарные потери для трафика $\lambda_{(s,d)}^q(k)$, маршрутизируемого на k-м шаге, не должны превышать максимально допустимого значения для данного класса обслуживания l_q. В реальных сетях потери определяются как отношение количества отброшенных пакетов к количеству поступивших на обслуживание, пакеты имеют различный размер (в зависимости от технологии), вероятность потери является функцией от размера буфера, размера пакета и длины очереди, а требования к обеспечению вероятности потери пакета определяются собственно вероятностью. Поскольку в терминах потоковой модели невозможно задать указанные параметры (т.к. она оперирует потоками, а не пакетами), данные параметры могут быть отражены лишь косвенно через перманентные потери в объеме передаваемого трафика на узлах сети. Значение $P_j^{q,(s,d)}(k)$ подлежит минимизации.

Ограничения, накладываемые на время задержки, аналогичны:

$$0 \le T_j^{q,(s,d)}(k), \quad \sum_j^{|V|} T_j^{q,(s,d)}(k) \le \tau_q \qquad \text{для всех узлов сети } j = \overline{1,|V|}, \tag{3}$$

где $T_j^{q,(s,d)}(k)$ – среднее время ожидания пакета класса обслуживания q в очереди на узле j, следующего из узла s в узел d. Выполнение данного ограничения способствует тому, что время доставки пакетов не превысит максимально допустимого значения для заданного класса обслуживания τ_q. Определение времени доставки пакета в общем виде является нетривиальной задачей и детально рассмотрено в [2].

Каждый тракт передачи между узлами сети на k-м шаге характеризуется:

• доступной пропускной способностью $\varphi_{ij}^q(k)$;

• стоимостью использования $\omega_{ij} \in \Omega$.

Предполагается, что вся доступная пропускная способность разделена между классами обслуживания, деление задано административно, и на протяжение всего времени модели остается неизменным. Доля пропускной способности Φ_{ij}, выделяемой для q-го класса обслуживания в канале (i, j) задана в виде β_{ij}^q и удовлетворяет условиям:

$$0 \le \beta_{ij}^q, \quad \sum_q^Q \beta_{ij}^q \le 1 \qquad \text{для всех каналов сети } i, j = \overline{1,|V|}. \tag{4}$$

В рамках подхода, используемого потоковыми моделями, необходимо для каждого вновь поступившего трафика определить один либо множество маршрутов до узла-получателя. В качестве переменных в потоковых моделях выступают маршрутные переменные $x_{ij}^{q,(s,d)}(k)$, которые характеризуют интенсивность трафика $\lambda_{(s,d)}^q(k)$ между узлами i и j на шаге k, $(i, j) \in E$. На основании результатов решения оптимизационной задачи в рамках потоковой модели по маршрутным переменным определяется множество

путей коммутации меток (LSP, Label Switching Path) между узлами (s,d), а также доля трафика $x_{ij}^{q,(s,d)}(k)$, которая будет передана по каждому из каналов пути. Возможен и альтернативный подход, в котором считается, что множество путей между граничными маршрутизаторами известно заранее и задача оптимизации сводится к выбору таких LSP для передачи трафика, которые минимизируют некоторую целевую функцию α. В общем случае $\alpha = f(P,T,Q,\Omega)$.

Поскольку задача распределения потоков по сети будет решаться во времени, значение свободной полосы будет варьироваться, и для каждого нового потока их необходимо рассчитывать заново, на основании результатов, полученных на предыдущем шаге, а доля трафика в канале, в свою очередь, не должна превышать доступную пропускную способность:

$$x_{ij}^{q,(s,d)}(k) \le \varphi_{ij}^{q}(k) \text{ для всех } i,j=\overline{1,|V|}, \tag{5}$$

где $\varphi_{ij}^{q}(k) = \varphi_{ij}^{q}(k-1) - x_{ij}^{q,(s,d)}(k-1) + \varepsilon_{(s,d)}^{q,k_0} * x_{ij}^{q,(s,d)}(k_0)$ рассчитывается для всех $q=\overline{1,Q}$.

В начальный момент значение $\varphi_{ij}^{q}(0) = \beta_{ij}^{q} * \Phi_{ij}$, $q=\overline{1,Q}$, $i,j=\overline{1,|V|}$.

Для корректной работы модели необходимо указать ограничения, которые обеспечивают поиск решений исключительно в допустимой области значений. Рассмотрим ограничение, обеспечивающее выполнение условия сохранения потока:

$$\begin{cases} \sum\limits_{j:(i,j)\in E} x_{ij}^{q,(s,d)}(k) + P_i^{q,(s,d)}(k) = \lambda_{(s,d)}^{q}(k) & i = V_s^+; \\ \sum\limits_{j:(i,j)\in E} x_{ij}^{q,(s,d)}(k) - \sum\limits_{j:(j,i)\in E} x_{ij}^{q,(s,d)}(k) + P_i^{q,(s,d)}(k) = 0 & i \ne V_s^+, i \ne V_d^+; \\ \sum\limits_{j:(j,i)\in E} x_{ij}^{q,(s,d)}(k) + \sum\limits_{j}^{|V|} P_j^{q,(s,d)}(k) = \lambda_{(s,d)}^{q}(k) & i = V_d^+. \end{cases} \tag{6}$$

Физический смысл маршрутной переменной накладывает ограничение вида:

$$0 \le x_{ij}^{q,(s,d)}(k) \le \lambda_{(s,d)}^{q}(k). \tag{7}$$

В то же время для обеспечения универсальности условия (5) необходимо, чтобы на каждом шаге маршрутные переменные, не участвующие в вычислении, определялись как:

$$x_{ij}^{m,(s,d)}(k) = 0, \quad \text{для всех } m \ne q,\ m=\overline{1,Q},\ i,j=\overline{1,|V|} \tag{8}$$

Результатом решения оптимизационной задачи на каждом шаге выступают вектор распределения трафика $\vec{x}(k)$, вектор потерь $\vec{P}(k)$ и вектор задержек $\vec{T}(k)$. Чтобы уйти от многокритериальности, все переменные можно включить в один искомый вектор $\vec{X}(k)$.

В данной работе предложена рекурсивная потоковая модель MPLS, описывающая поведение ТКС во времени. При составлении модели были максимально учтены такие параметры, как потеря пакетов и среднее время ожидания пакета в очереди, роль которых в предыдущих потоковых моделях не рассматривалась. Направлением развития данной работы служит разработка рекурсивной модели узла MPLS, а также обоснование выбора целевой функции.

Литература: 1. Лемешко А.В., Ахмад М. Хайнлайн Многоуровневое управление трафиком в сети MPLS-DiffServ на основе координационного принципа прогнозирования взаимодействий, Проблемы Телекоммуникаций №1(1) 2010, стр. 35-44; 2. Лосев Ю.И., Шматков С.И, Руккас К.М., Щебенюк В.С. Математическая модель процесса информационного обмена при многопутевой передаче, Системи управління, навігації та зв'язку Київ 2010 випуск №1(13) стор. 205-209; 3. Handbook of optimization in telecommunication, Edited by M. G.C. Resende, P. M. Pardalos, Springer Science + Business Media, Inc, 2006, 1134p.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТЕХНОЛОГИЙ MPLS И GMPLS

Горюнов А.А., Руккас К.М., Овчинников К.А.
Харьковский национальный университет радиоэлектроники
(61166, г. Харьков, пр. Ленина,14, каф. ТКС)
e-mail: sqrt-avers@mail.ru

Multi-Protocol Label Switching (MPLS) provides a mechanism for forwarding packets for any network protocol. Since then its capabilities have expanded massively, for example to support service creation (VPNs), traffic engineering, network convergence, and increased resiliency. MPLS similarly uses IP addresses, either IPv4 or IPv6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs). Generalized Multiprotocol Label Switching (GMPLS) enhances MPLS architecture by the complete separation of the control and data planes of various networking layers.

1 Введение в технологию MPLS

MPLS (Multiprotocol Label Switching — многопротокольная коммутация по меткам) представляет собой механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток. MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети. Так же данная технология позволяет инкапсулировать различные протоколы передачи данных. MPLS является масштабируемым и независимым от каких-либо протоколов механизмом передачи данных. Основным преимуществом MPLS является независимость от особенностей технологий канального уровня, таких как ATM, Frame Relay, SONET/SDH или Ethernet и отсутствия необходимости поддержания нескольких сетей второго уровня, необходимых для передачи различного рода трафика. По виду коммутации MPLS относится к сетям с коммутацией пакетов.

Технология MPLS основана на обработке заголовка MPLS, добавляемого к каждому пакету данных. Заголовок MPLS может состоять из одной или нескольких "меток". Несколько записей (меток) в заголовке MPLS называются стеком меток (рис.1).

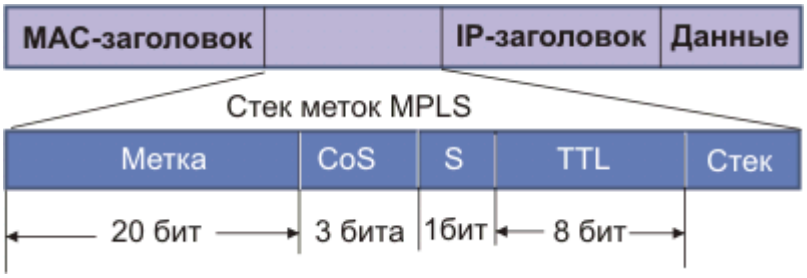


Рис. 1 – Стек меток MPLS

В MPLS маршрутизаторе пакет с MPLS меткой коммутируется на следующий порт после поиска метки в таблице коммутации вместо поиска в таблице маршрутизации. Как упоминалось выше, при разработке MPLS, поиск меток и коммутация по меткам выполнялись быстрее, чем поиск в таблице маршрутизации или RIB (Routing Information Base — информационная база маршрутизации), так как коммутация может быть выполнена непосредственно на коммутационной фабрике вместо центрального процессора. Маршрутизаторы, расположенные на входе или выходе MPLS сети называются LER (Label Edge Router - граничный маршрутизатор). LER на входе в MPLS сеть добавляют метку MPLS к пакету данных, а LER на выходе из MPLS сети удаляет метку MPLS из пакета данных. Маршрутизаторы, выполняющие маршрутизацию пакетов данных, основываясь только на значении метки, называются LSR (Label Switching Router — коммутирующий маршрутизатор). В некоторых случаях пакет данных, поступивший на порт LER, уже может содержать метку, тогда новый LER добавляет вторую метку в пакет данных. Мет-

ки между LER и LSR распределяются с помощью LDP (Label Distribution Protocol - протокол распределения меток). Для того чтобы получить полную картину MPLS сети LSR постоянно обмениваются метками и информацией о каждом соседнем узле, используя стандартную процедуру. Виртуальные каналы (туннели), называемые LSP (Label Switch Path - Пути коммутации меток) устанавливаются для решения различных задач, например для организации виртуальных частных сетей, или для передачи трафика через MPLS сеть по указанному туннелю. Во многом LSP ничем не отличается от PVC в сетях ATM или Frame Relay за исключением того, что LSP не зависят от особенностей технологий канального уровня. Существует два стандартных протокола управления туннелями в MPLS сети: LDP и RSVP-TE, расширение RSVP (Resource Reservation Protocol — протокола резервирования сетевых ресурсов) для оптимизации и управления трафиком. Также существуют расширения протокола BGP, способные управлять виртуальными каналами в MPLS сети. Заголовок MPLS не указывает тип данных, передаваемых в MPLS туннеле. В случае, если возникает необходимость передать два различных типа трафика между двумя маршрутизаторами так, чтобы они по-разному обрабатывались маршрутизаторами ядра сети MPLS, необходимо установить два различных MPLS туннеля для каждого типа трафика.

2 Сравнительная характеристика MPLS с GMPLS

GMPLS (Generic Multiprotocol Label Switching - Обобщенный MPLS) отличается от традиционного MPLS тем, что он поддерживает много типов коммутации, TDM - волоконную коммутацию. Изначально на базе MPLS была разработана технология MPλS (Multiprotocol Wavelength Switching - многопротокольная коммутация по длине волны), затем её доработали и создали GMPLS. Поддержка дополнительных видов коммутации вынуждает обобщенный протокол MPLS расширить некоторые базовые функции MPLS и, в некоторых случаях добавить определенные функции. Эти изменения и добавления оказывают влияние на то, как осуществляются запросы и транспортировка меток, как пересылаются сообщения об ошибках и как выполняется синхронизация на входе и на выходе. В традиционном управлении трафиком MPLS TE, каналы, через которые проходит LSP, могут содержать сегменты с разной кодировкой меток. Обобщенный MPLS осуществляет расширение функциональности путем включения каналов, где метка кодируется как временной домен, длина волны, или позиция в физическом пространстве. Также как и в традиционном MPLS TE, где не все LSR могут распознавать границы IP-пакетов (напр., ATM-LSR) при переадресации, обобщенный MPLS включает в себя поддержку LSR, которые не распознают границ IP-пакетов. В традиционном MPLS TE LSP, который транспортирует IP, должен начинаться и завершаться в маршрутизаторе. Обобщенный MPLS требует, чтобы LSP начинался и завершался в LSR того же типа. Кроме того, в обобщенном MPLS тип данных, который транспортируется через LSP, может включать в себя SONET/SDH, GE или 10Гбитный Ethernet. Эти изменения традиционного MPLS отражаются в механизме запроса и переноса меток. Другим базовым отличием традиционного и не-PSC типа обобщенного LSP MPLS, является то, что полоса пропускания, выделяется для LSP дискретными порциями. Заметим, что использование FA (Forwarding Adjacencies), предоставляет механизм, который может улучшить использование полосы пропускания, когда выделение полосы осуществляется дискретным образом, а также механизм агрегирования состояния переадресации, что может сократить требуемое число меток. Обобщенный MPLS допускает возможность предложения метки вышестоящим узлом. Это предложение может быть отвергнуто нижестоящим узлом, за счет увеличения времени установления LSP. Предлагаемая метка представляет ценность, когда LSP устанавливается через определенное оптическое оборудование, где конфигурирование системы коммутации может быть долгим. Если метки и, следовательно, оптическая система коммутации сконфигурированы в обратном порядке (норма), может потребоваться задержать сообщение MAPPING/Resv на десятки миллисекунд на один шаг, для того чтобы установить маршрут переадресации. Предлагаемая метка может быть полезной также при

восстановлении в случае отказа узла. Обобщенный MPLS расширяет понятие ограничения диапазона меток, которые могут быть выбраны нижестоящим узлом. В обобщенном MPLS, входной или другой вышестоящий узел может ввести ограничения на метки, которые могут быть использованы в LSP. Эта особенность пришла из оптической области, где бывают случаи, когда длины волн, используемые в пределах маршрута, должны быть ограничены узким диапазоном или даже одной длиной волны. В то время как традиционный трафик, формируемый MPLS является однонаправленным, обобщенный MPLS поддерживает установление двунаправленных LSP. Необходимость двунаправленных LSP вызвана не-PSC приложениями. Существует много причин, зачем нужны такие LSP, в частности конкуренция за ресурсы при формировании LSP с привлечением разных сигнальных сессий, и упрощение процедур восстановления при ошибках в случае не-PSC. Двунаправленные LSP имеют также преимущества малой задержки установления канала и малого числа сообщений при реализации этого процесса. Обобщенный MPLS поддерживает специфические метки для специальных интерфейсов, поддерживает также специальные механизмы RSVP для быстрого уведомления об ошибках. Обобщенный MPLS формализует возможное разделение каналов управления и данных. Такая поддержка особенно важна для поддержки технологий, где управление трафиком не может осуществляться в рамках информационного потока. Обобщенный MPLS также позволяет использование параметров, специфических для сигнальной технологии. Для расширения области применения MPLS в сферу оптики и временных доменов, необходимо несколько новых форм меток. Эти новые формы меток называются "обобщенными метками" (рис. 2). Обобщенная метка содержит достаточно информации, чтобы позволить принимающему узлу программировать коммутацию вне зависимости от типа этого соединения. Заметим, что, так как узлы, посылающие и принимающие новые формы меток, знают, какой тип канала они используют, обобщенная метка не содержит поля тип, вместо этого предполагается, что узлы знают из контекста, какие метки следует ожидать.

Рис. 2 – Метки GMPLS

Обобщенная метка расширяет функциональность традиционной метки, допуская представление не только меток, которые транспортируются соответствующими информационными пакетами, но также меток, которые идентифицируют временные домены, длины волн, или пространственное мультиплексирование по положению. Например, обобщенная метка может содержать данные, которые представляют (a) одно волокно из пучка, (b) один волновой диапазон в волокне, (c) одну длину волны из диапазона (или волокна), или (d) набор временных доменов для заданной длины волны (или волокна). Метка может также нести данные о базовой метке MPLS, метке Frame Relay, или метке ATM (VCI/VPI). Обобщенная метка не идентифицирует класс, к которому принадлежит метка. Это определяется возможностями мультиплексирования канала, где используется метка. Обобщенная метка несет в себе лишь метку одного уровня, т.е., она не является неиерархическим объектом. Когда требуется несколько уровней меток (LSP внутри LSP), каждый LSP должен быть сформирован отдельно. Каждый TLV-объект обобщенной метки несет в себе параметр метки переменной длины. В контексте коммутации по диапазонам длин волн метка имеет формат (рис. 3):

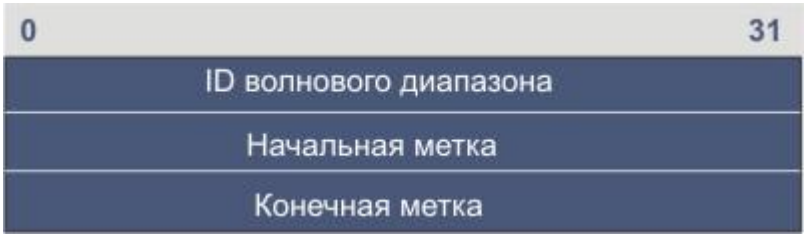


Рис. 3 – Метки MPλS

Таблица 1 – Сравнение MPLS и GMPLS

MPLS	GMPLS
1. Отсутствие возможности использования оптической коммутации. 2. Меньшая функциональность, ограниченная возможными видами коммутций. 3. Трафик, формируемый MPLS является однонаправленным.	1. Поддержка дополнительных видов коммутаций (TDM и т.д.). 2. Расширенное количество базовых функций как следствие использования дополнительных видов коммутаций. 3. Метка кодируется как временной домен, длина волны, или позиция в физическом пространстве 4. Полоса пропускания, выделяется для LSP дискретными порциями. 5. GMPLS расширяет понятие ограничения диапазона меток. 6. Трафик, формируемый GMPLS является двунаправленным.

Выводы:

Такие недостатки в MPLS как отсутствие возможности организации связи по оптике или включение в действующую сеть таких популярных систем как DWDM дали повод для доработки и создания технологии GMPLS. Отдельные достоинства и недостатки приведены в таблице 1. Однако у этих технологий есть один общий недостаток (с точки зрения безопасности) - он может применяться только для связи "сеть - сеть" и не применим для соединения с отдельными узлами. Есть и второй недостаток - данные разных пользователей хоть и не смешиваются, но все-таки к ним можно получить доступ, прослушивая сетевой трафик. Кроме того, провайдер, предлагающий услуги MPLS будет иметь доступ ко всей передаваемой информации.

Литература:

1. Вивек Олвейн – Структура и реализация современной технологии MPLS. – Cisco Press; 2004. – 480с.

2. Гольдштейн А.Б., Гольдштейн Б.С.. Технология и протоколы MPLS. — СПб.: БХВ – Санкт-Петербург, 2005. — 304 с.

3. Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V. и G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

4. Berger, L., Editor "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

5. Ashwood-Smith, P. и L. Berger, Editors, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions", RFC 3472, January 2003

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ СИСТЕМ УПРАВЛЕНИЯ МУЛЬТИСЕВИСНЫМИ СЕТЯМИ

Дуравкин Е.В., Копытова Е.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: duravkin_evgen@mail.ru, koputova@mail.ru

In this article is offered a web-oriented architecture of distributed management of the network. This architecture makes reduction of processing time with intensity of incoming flow of requests more then intensity of service is possible.

Введение

В настоящее время в телекоммуникационной сфере наблюдается интенсивное расширение перечня предоставляемых услуг и внедрение новых технологий передачи данных. В связи с этим особую актуальность приобретают задачи повышения эффективности систем управления в телекоммуникационных сетях с целью обеспечения заданного качества обслуживания пользователей при предоставлении услуг.

На сегодняшний день существуют несколько реализаций концепции управления телекоммуникационными системами TMN [1]: SNMP [2], CMIP [2] и т.д.. Однако в настоящее время данные технологии не позволяют в полной мере решать возложенные на них задачи управления и обеспечение заданного качества обслуживания. В первую очередь это связанно с повышением разнородности как аппаратного, так и программного обеспечения внедряемого для реализации новых услуг в телекоммуникационных сетях.

На смену указанным технологиям приходят CORBA [3,5], SOA [4,5], WBEM и т.д.

Основная часть

Структура распределенного управления инфокоммуникационной сетью на базе CORBA представлена на рис.1.

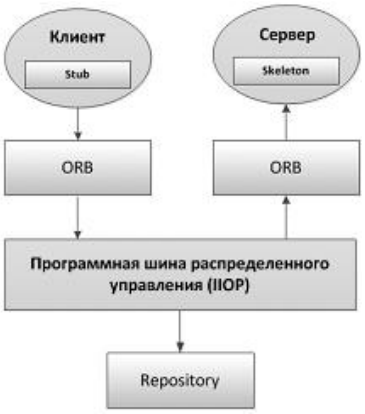


Рис. 1 – Структура распределенного управления сетью на базе CORBA

Внедрение технологии управления CORBA, основанной на идее открытого распределенного управления, позволяет гибко обеспечить взаимодействие территориально распределенных компонентов системы управления. Необходимо отметить ориентированность данной технологии на программно-реализуемые компоненты распределенной системы управления, что несколько сужает ее область применения. Одним из основных недостатков данной технологии является то, что с увеличением числа взаимодействующих объектов (перечня предоставляемых услуг) резко повышается сложность реализации IIOP.

Альтернативной технологией управления является сервис-ориентированная архитектура (SOA) (рис.2).

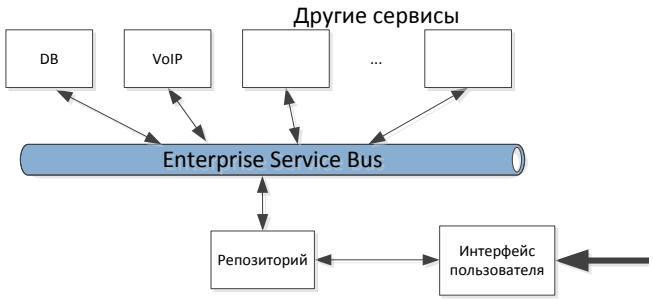


Рисунок 2 — Структура распределенного управления сетью на базе SOA

Основной задачей технологии SOA является интеграция разнородных услуг предоставляемых телекоммуникационной сетью. В основе технологии лежит использование единой транспортной среды (ESB). Следовательно, производительность системы при использовании такой архитектуры во многом определяется производительностью транспортной среды. Во многих случаях добиться высокой производительности такой системы достаточно тяжело как раз в силу разнородности обслуживаемых сервисов.

Повышение производительности SOA систем предполагается несколькими способами:

- за счет улучшения характеристик ESB;
- за счет объединения предоставляемых сервисов в группы и выделением отдельных транспортных подсистем для каждой из групп.

Дальнейшим развитием технологии SOA является веб-ориентированная технология управления распределенными системами WBEM (Web-based Enterprise Management). В основе WBEM лежит идея использования общей информационной модели (Common Information Model, CIM). На рисунке 3 представлена практическая реализация архитектуры управления мультисервисной сетью на базе технологии WBEM.

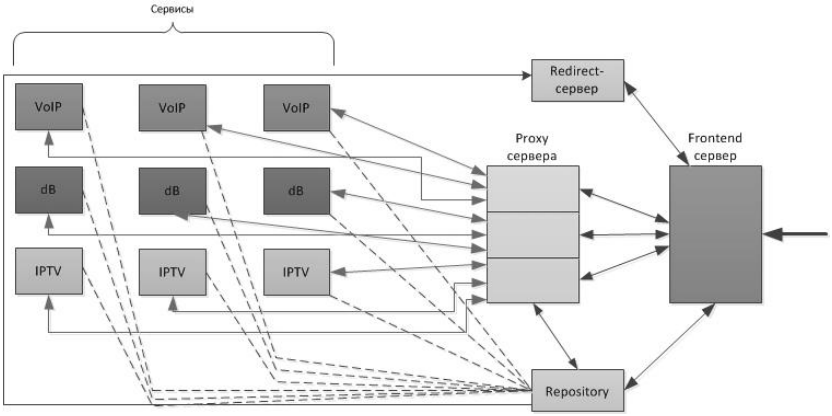


Рис. 3 — Структура распределенного управления сетью на базе предложенной web-ориентированной архитектуры

Сравнительная оценка производительности систем управления мультисервисной сетью реализованных по технологиям CORBA, SOA, WBEM приведена на рисунке 4. Анализируемые системы были исследованы на предмет зависимости времени обработки запроса пользователя на получение случайной (из числа поддерживаемых) услуги от интенсивности поступающих запросов (время реакции сети).

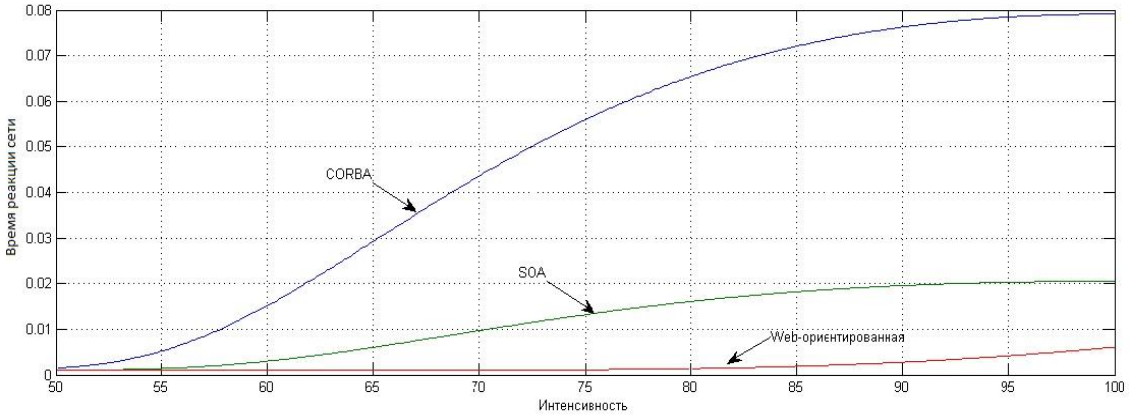


Рис. 4. График зависимости времени реакции сети от интенсивности поступающих запросов

Выводы

Анализ полученных результатов показал, что характер зависимости времени реакции сети от интенсивности входящего потока определяется архитектурными особенностями используемой системы управления. При анализе результатов подтверждается тот факт, что при значении интенсивности входящего потока заявок превышающем интенсивность обслуживания, увеличение времени реакции сети оказывается значительно более быстрым для архитектуры CORBA, чем для SOA и WBEM архитектур. Это объясняется особенностями информационных связей в IIOP, которую используют системы управления CORBA. В системе управления, использующей архитектуру WBEM выигрыш (в сравнении с остальными) достигается за счет распараллеливания процесса обслуживания заявок, в соответствии с типом услуги. При поступлении запроса выполняется перенаправление его на соответствующий proxy-сервер, управляющий группой серверов, предоставляющих услугу запрашиваемого типа. Таким образом, можно сделать вывод о целесообразности использования WBEM архитектуры для высоконагруженных мультисевисных сетей..

Литература:

1.ITU-T Recommendation M.3010. Principles for a telecommunications management network.

2. Поповский В.В., Олейник В.Ф. Математические основы управления и адаптации в телекоммуникационных системах – Х.: СМИТ, 2011 - 362 с.

3. Common Object Request Broker Architecture (CORBA) Specification, Version 3.1 Part 1: CORBA Interfaces

4. Компас в мире сервис-ориентированной архитектуры (SOA): ценность для бизнеса, планирование и план развития предприятия / [Биберштейн Н., Боуз С., Джонс К. и др.]. – М.: КУДИЦ-ПРЕСС, 2007. –256 с.

5. Е.А. Копытова. Анализ технологий построения распределенных управляющих систем/ Е.А. Копытова // Радиотехника. – 2009. – Вып.159. – С.249-261.

ОБЗОР И КЛАССИФИКАЦИЯ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Евдокименко М.А., Ахмед Хассан Абед
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. ТКС, тел. (057) 702-13-20,
E-mail: gogolevam@gmail.com ; факс (057) 702-11-13\

One of the promising areas of wireless networks is a research and development used in these algorithms and routing protocols. After analyzing the existing solutions have been put forward demands for improvements to existing and developing new routing protocols for wireless networks.

Введение

На сегодняшний день в связи с созданием мультисервисных сетей, беспроводные сети представляют собой наилучшее решение для организации доступа по совокупности показателей быстроты и стоимости развертывания, простоте подключения пользователей и степени зависимости от окружающих условий. Но, несмотря на интенсивное развитие и применение беспроводных сетей, существует ряд недостатков касательно невысокой пропускной способности и качества обслуживания (Quality of Service, QoS). Поэтому, исходя из широкой области применения беспроводных сетей, классификации их архитектур, классов и режимов существует достаточно обширная классификация алгоритмов и протоколов маршрутизации, направленных именно на повышение качества обслуживания. А ввиду отсутствия фиксированной структуры беспроводной сети, а также фиксированных пропускных способностей, основной задачей маршрутизации в отличие от проводных сетей является решение задачи структурно-функционального синтеза.

В связи с этим, одним из перспективных направлений развития беспроводных сетей является исследование и усовершенствование применяемых в них алгоритмов и протоколов маршрутизации.

Классификация протоколов маршрутизации в беспроводных сетях

Протоколы маршрутизации, используемые в беспроводных сетях, основаны на традиционных алгоритмах маршрутизации, таких как дистанционно-векторный алгоритм маршрутизации и маршрутизация с учетом состояния связей. Однако ограниченные ресурсы беспроводных сетей сделали проектирование надежных и эффективных алгоритмов маршрутизации достаточно сложной задачей, т.к. они должны не только эффективно использовать ресурсы, но и быть хорошо адаптированы к изменениям размера сети, совместимости беспроводных устройств, плотности трафика, к выведению узлов из строя и т.д. На сегодняшний день, исходя из специфики построения беспроводных сетей, их высокой динамичности и ограниченности ресурсов, что в целом приводит к ухудшению показателей качества обслуживания, существует обширная классификация протоколов маршрутизации. И в зависимости от сложившейся ситуации реализуются различные алгоритмы маршрутизации, такие как проактивная и реактивная маршрутизация, маршрутизация в зависимости от географического местоположения, гибридная, иерархическая и т. д.

Но если проводить сравнительный анализ наиболее используемых методов маршрутизации, то результаты [2] показывают, что наиболее эффективными для использования в беспроводных сетях являются реактивные протоколы, которые инициируют запрос о формировании (расчета) маршрута по требованию. Такие протоколы сохраняют пропускную способность беспроводной среды и экономят запас энергии батарей мобильных терминалов. С другой стороны для обеспечения качества обслуживания заслуживает внимания подход, основанный на реализации принципов многопутевой (multipath routing) и потоково-ориентированной маршрутизации (flow-based routing). Потоково-ориентированные алгоритмы маршрутизации могут применяться в высоко-

динамичной сети, в которой существует ряд узлов, которые менее подвижны, чем все остальные. В таком случае трафик в основном обрабатывается этими малоподвижными узлами. Таким образом, может быть улучшено нахождение маршрута и для реактивных, и для проактивных алгоритмов маршрутизации. Однако в начале работы сети такой подход не дает хороших результатов, так как нет никаких ранее собранных данных, системе нужно время для сбора необходимой статистики. Главная особенность, отличающая протоколы потоково-ориентированной маршрутизации от других протоколов маршрутизации, это то, что данные протоколы поддерживают множественные маршруты к каждому искомому узлу, а не единственный маршрут. А недостатком данного вида маршрутизации являются большие временные затраты при установлении нескольких маршрутов

Если рассматривать беспроводные сети большой размерности и с высокой мобильностью узлов, то проактивные алгоритмы применяться не могут. Это связано с большим объемом служебной информации для поддержания маршрутов и медленной реакцией на изменение топологии сети. Однако их можно взять за основу для создания новых алгоритмов, более приспособленных к динамически изменяющимся сетям.

Попытка структурировать динамически изменяющуюся сеть путем объединения узлов в кластеры на базе использования иерархической маршрутизации тоже не принесла ожидаемых результатов. Т.к. clusterheads (так называемые «главные узлы» в кластере) и шлюзы занимаются маршрутизацией и координированием, они легко могут стать узким местом сети из-за того, что нагрузка на эти узлы будет намного больше, чем на обычные, и это приведет к быстрому расходованию энергии и отключению этих устройств из-за недостатка энергии.

Гибридная маршрутизация имеет свойства как дистанционно-векторных алгоритмов маршрутизации так и маршрутизации по состоянию каналов и, сочетая в себе достоинства проактивной и реактивной маршрутизации, в целом является более эффективной.

Следует отметить, что алгоритмы и методы маршрутизации, используемые в беспроводных сетях (FSR, OLSR, AODV и др.) [3] основаны преимущественно на моделях поиска кратчайшего пути на графовом представлении сети. Эти модели, как правило, не учитывают возможность перегрузки радиоканала, доступность полосы пропускания, ограниченность энергетического ресурса сетевого узла. Несмотря на широкое распространение графовых моделей маршрутизации, положенных в основу большинства существующих маршрутизирующих протоколов, на практике все более востребованы именно потоковые модели маршрутизации, которые, с одной стороны, учитывают потоковый характер современного, преимущественно мультимедийного трафика (видео, речь и др.), а с другой стороны, более адаптированы под решение задач

В настоящее время существует множество моделей, которые используются в проводных сетях. В объединенных сетях задачу обеспечения QoS рассматривают на макроуровне, то есть на уровне взаимодействия составляющих локальных сетей. Сетевая структура на макроуровне изменяется относительно редко, что так же позволяет использовать известные методы. Однако в беспроводных сетях маршрутизация и обеспечение требуемого QoS, основываются на динамической природе этих сетей, что предопределяет использование динамических алгоритмов обеспечения QoS. Существующие модели QoS неприемлемы для использования в мобильных сетях Ad Hoc и необходима их адаптация для использования в таких сетях.

Исходя из этого, несмотря на разнообразие протоколов и алгоритмов маршрутизации в беспроводных сетях, ни один из них не является самодостаточным. Поэтому, возникает задача разработки и исследования новых подходов решения задачи маршрутизации в беспроводных сетях, повышающих эффективность передачи данных с обеспечением требуемого различными приложениями уровня качества обслуживания.

Таким образом, к протоколам маршрутизации в беспроводных сетях сформулированы специальные требования (рис. 1).

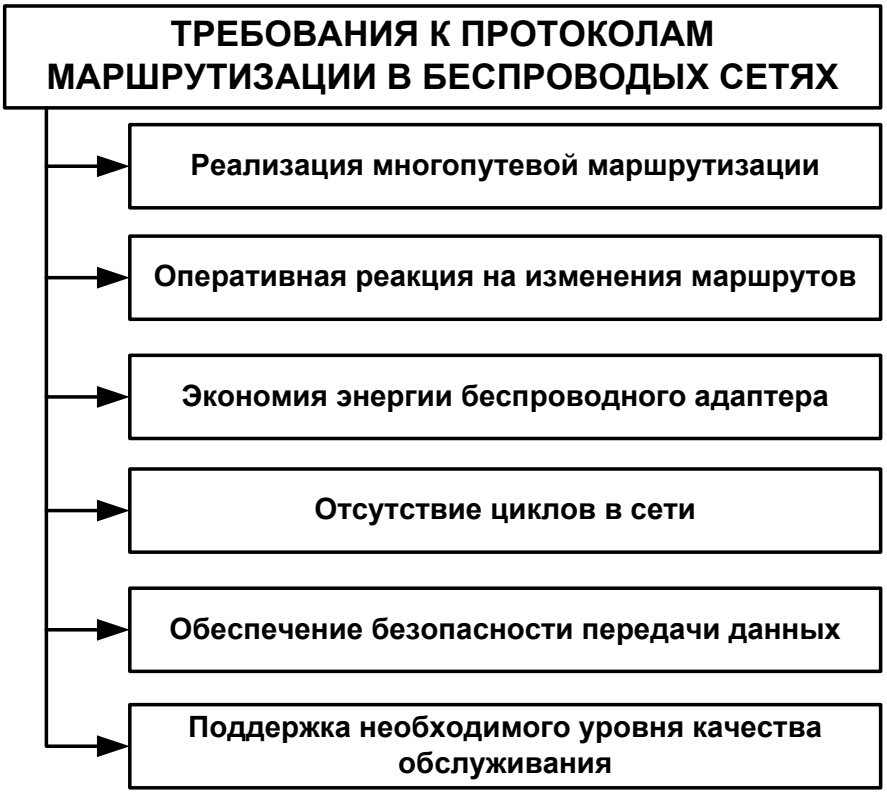


Рис. 1. Требования к протоколам маршрутизации в беспроводных сетях

Выводы

На данном этапе развития беспроводных сетей, в силу ряда достоинств наиболее используемые считаются следующие виды маршрутизации: реактивная, проактивная и иерархическая. Однако в беспроводных сетях маршрутизация и обеспечение требуемого QoS, основываются на динамической природе этих сетей, что предопределяет использование динамических алгоритмов обеспечения QoS. Исходя из этого, в работе были выдвинуты требования для усовершенствования существующих и разработки новых протоколов маршрутизации

Литература:

1. Йоганн. Ш. Мобильные коммуникации.// Пер. с англ. Издательский дом Вильямс. – 2002. – С. 384

2. Das S. R., Perkins C. E., and Royer E. Performance comparison of two on-demand routing protocols for Ad Hoc networks. // IEEE Conference on Computer Communications. – 2000. – P.3-12 .

3. Поповский В.В., Лемешко А.В., Мельникова Л.И., Андрушко Д.В. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника. – 2005.– Том.4. Вып. № 4. – С. 372-38.

4. Лемешко А.В., Гоголева М.А. Потоково-ориентированная модель многопутевой маршрутизации в телекоммуникационной сети // Вісник Державного університету інформаційно-комунікаційних технологій. – 2008. – Том 6 (2). – С. 162-170.2.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПОТОКОВОЙ МАРШРУТИЗАЦИИ

Карпин Н.Б, Ткаченко В.М.
Харьковский национальный университет радиоэлектроники
61170, Харьков, пр. Ленина, каф. ТКС, тел.(057) 702-13-20
E-mail: nkarpin@yandex.ru, тел. (0572) 67-64-07

One of the most important means of ensuring quality of service and traffic is routing. The basis for all technologies and routing protocols are mathematical routing models. In a scientific paper analyzes three mathematical models for single-threaded and multi-threaded cases. Based on the results of research formulated the basic guidelines for choosing a particular model.

Введение.

Обеспечение необходимого уровня качества обслуживания (QoS) является приоритетной задачей в современных телекоммуникационных системах (ТКС). При этомодним из важнейших средств обеспечения качества обслуживания и управления трафиком есть маршрутизация. Основу большинства технологий и протоколов маршрутизации составляют соответствующие математические модели, поэтому важно при создании маршрутизирующих протоколов и смежных средств обеспечения QoS выбрать такую модель, которая бы, с одной стороны, наиболее полно и адекватно описывала моделируемый процесс, а с другой, не приводила к чрезмерному усложнению процесса ее анализа и исследования, обеспечив получение искомых результатов с приемлемой точностью.

Ввиду большого количества существующих и с разной степенью успеха применяемых моделей маршрутизации в настоящем докладе предлагаются результаты сравнительного анализа ряда основных потовых моделей (М1÷М3), на основе которых сделаны важные выводы и рекомендации по поводу перспектив их дальнейшего использования.

Описание моделей маршрутизации.

Модель многопутевой маршрутизации М1 была представлена системой линейных алгебраических уравнений, описывающих условие сохранения потока в узлах сети, а также условиями-ограничениями по предотвращению перегрузки каналов связи ТКС. При этом количество искомых маршрутных переменных ($N_{пер}$) для полносвязной структуры ТКС определялось с помощью следующих выражений:

- при обслуживании одного трафика между одной парой узлов $N_{пер} = m \cdot (m-1)$,

- при обслуживании множества трафиков ($m \cdot (m-1)$), т.е. при обслуживании по одному трафику, но уже между каждой парой узлов, $N_{пер} = m \cdot (m-1) \cdot m \cdot (m-1)$, где m – количество узлов ТКС.

Модель М2 также представлена системой линейных алгебраических уравнений. Имеет те же ограничения, что и модель М1. В отличие от модели М1 имеет трехиндексные искомые переменные. Формулы расчета количества переменных:

- для одного трафика – $N_{пер} = m \cdot (m-1)$;

- для $m \cdot (m-1)$ трафиков – $N_{пер} = m \cdot (m-1) \cdot (m-1)$.

Модель М3, предложенная Р. Галагером, представлена системой нелинейных уравнений. В ней реализованы те же ограничения, что и в предыдущих моделях. Формулы для расчета количества маршрутных переменных:

- для одного трафика – $N_{пер} = m \cdot (m-1) + m$;

- для $m \cdot (m-1)$ трафиков – $N_{пер} = m \cdot (m-1) \cdot (m-1) + m \cdot (m-1)$.

Исследование описанных моделей.

На рис.1а представлены зависимости количества маршрутных переменных от количества узлов при наличии одного трафика в сети, на рис. 1б – при наличии $m \cdot (m-1)$ трафиков в сети.

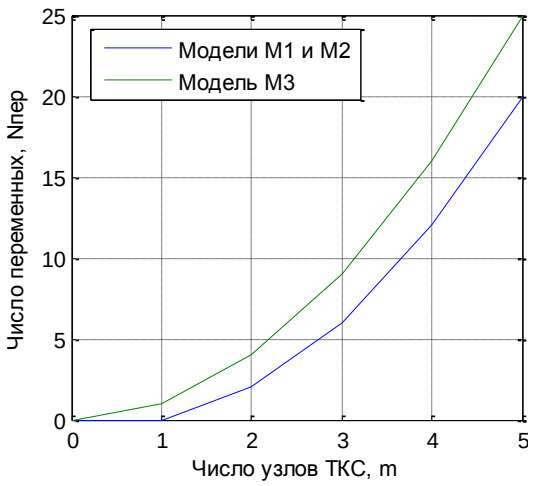


Рис. 1а

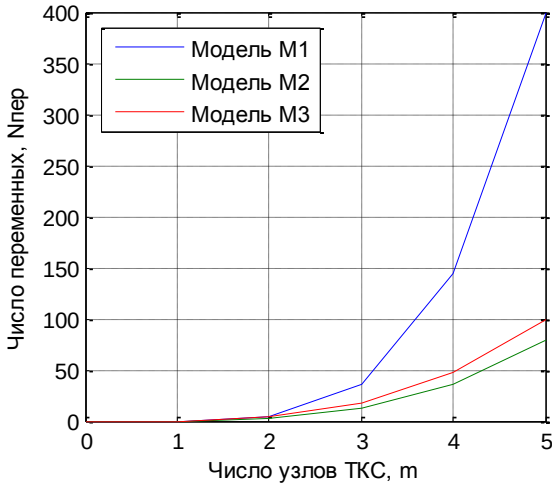


Рис. 1б

Выводы

По результатам анализа были сделаны следующие выводы:

- в ходе маршрутизации одного трафика между одной парой узловв ТКС все три модели давали одинаковый результат с точки зрения характера распределения интенсивности трафика по каналам связи сети. Однако модель М3 была более сложной в исследовании, т.к. была нелинейной и обладала большей размерностью (сложностью);

- в ходе маршрутизации по одному трафику между всеми парами узлов ТКС модель М2 обладала меньшей сложностью, чем модели М1 и М3 при обеспечении той же адекватности описания процесса маршрутизации в ТКС.

В этой связи, целесообразной представляется использование модели М2 при моделировании процессов многопутевой маршрутизации множества трафиков, передаваемого между множеством узлов в сети.

ПРОЦЕДУРА ОЦЕНКИ RTT СЕГМЕНТА В СЕТИ НА ОСНОВЕ ЗАШУМЛЕННЫХ НАБЛЮДЕНИЙ

Андрушко Юрий Владимирович
Харьковский национальный университет радиоэлектроники
61000, г.Харьков, пр. Ленина 14, каф. ТКС, тел. (057) 702-13-20,
e-mail: ya@kture.kharkov.ua

Article is dedicated to overview approaches of RTT estimation in different versions of TCP protocol and proposed procedure based on noisy observations.

Основная задача протокола TCP – гарантировать доставку данных от источника к получателю, причем, протокол гарантирует так же прием данных в той последовательности, в которой они были отправлены. Для решения задачи гарантированной доставки, протокол использует механизм подтверждения полученных данных приемной стороной. Стоит отметить, что в зависимости от версии протокола TCP механизмы подтверждения, роста и уменьшения окна, реакции на потерянные данные и их повторной пересылки могут отличаться. Так, к примеру, в «классической» версии протокола Tahoe TCP определены процедуры «аддитивного увеличения/мультипликативного уменьшения» и механизм медленного старта [1].

Склонность протокола TCP версии Tahoe к пониженному использованию полосы пропускания и подверженность к незначительным потерям привела к появлению новых версий протокола как стандартизированных, таких как Reno TCP [2] и Vegas TCP [3], так и перспективных, таких как FAST, H-TCP, Hybla, BIC. Основное отличие реализаций протокола – введение новых или модернизация старых механизмов определения, предотвращения перегрузки и начала соединения.

Безотносительно используемого версией протокола математического аппарата, основной характеристикой сети между отправителем и получателем, а так же ее загруженности является время кругового обращения в сети (Round Trip Time, RTT). Процедуры и методы оценки RTT, а так же их точность непосредственно влияют на использование полосы пропускания протоколом TCP. Для описания функционирования протокола при межсетевом взаимодействии можно рассмотреть пару «RTT-характеристики канала». Особенностью этих показателей является то, что они ненаблюдаемы, и кроме этого, изменяются с течением времени и взаимозависимы друг от друга. Наиболее адекватно процесс передачи может быть представлен в виде случайной марковской последовательности. При построении марковской модели процесса передачи данных по сети связи, сам процесс можно описать двумя параметрами – состоянием сети и временем кругового обращения пакета. Можно предположить, что сеть и ее каналы могут находиться в двух состояниях – свободном и загруженном. Так, в свободном состоянии сеть характеризуется низкими показателями RTT и вероятности сброса пакета, а в загруженном – возрастает как задержка, так и вероятность сброса пакета или его искажения. В таком случае динамику сети связи можно описать с помощью марковской цепи q_t с возможными состояниями:

$q_t = e_1$ - отсутствие потерь при свободном канале

$q_t = e_2$ - потеря при свободном канале

$q_t = e_3$ - отсутствие потерь при загруженном канале

$q_t = e_4$ - потеря при загруженном канале

Состояние вероятности марковской цепи q_t можно представить в виде матрицы:

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{pmatrix},$$

где P_{ij} - вероятность наступления события.

Значения элементов матрицы могут быть различны и зависят от ряда факторов, таких как топология сети, объем передаваемых данных, тип трафика и т.д. Вне зависимости от конкретных значений, в матрице должно соблюдаться условие $\sum_{j=1}^{4} P_{ij} = 1$. В результате экспериментальных исследований и имитационного моделирования, получены состояния марковской цепи, которые могут быть описаны следующей матрицей:

$$P = \begin{pmatrix} 0.92 & 0.05 & 0.03 & 0 \\ 0.4 & 0.4 & 0.2 & 0 \\ 0.08 & 0 & 0.77 & 0.15 \\ 0 & 0 & 0.4 & 0.6 \end{pmatrix}$$

Проанализировав значения параметров, можно видеть, что самым стабильным состоянием является $q_t = e_1 (P_{11} = 0{,}92)$, то есть ситуация когда сеть не загружена и нет потерь. Однако даже в этом состоянии, хоть и с низкой долей вероятности, возможна потеря пакета, а следовательно, переход в состояние $q_{t+1} = e_2, P_{12} = 0{,}05$. Кроме этого так же возможна ситуация перехода в загруженное состояние $q_{t+1} = e_3, P_{13} = 0{,}03$. В случае потери пакета при свободном канале (состояние $q_t = e_2$) с большой долей вероятности $(P_{21} + P_{22} = 0{,}8)$, цепь останется в незагруженном состоянии $q_{t+1} = e_1$, если потеря пакета не повторится, или $q_{t+1} = e_2$, если повторится. Так же возможен переход (с вероятностью $P_{23} = 0{,}2$) в загруженное состояние $q_{t+1} = e_3$. В случае когда сеть загружена $q_t = e_3$, чаще происходят потери пакетов $q_{t+1} = e_4$ $P_{34} = 0{,}15$, тем не менее достаточно вероятно ($P_{33} = 0{,}77$), что на следующем шаге потерь не будет $q_{t+1} = e_3$., так же с вероятностью $P_{31} = 0{,}08$ канал может освободиться $\theta_{t+1} = e_1$. Повышенная вероятность блокирования трафика и повторных потерь в состоянии $q_t = e_4$ моделирует явление «коллапса», связанное с потерей нескольких пакетов сразу. Такая ситуация зачастую встречается в тривиальных механизмах активного управления очередями, таких как DropTail. Динамику марковской цепи q_t можно описать в виде рекуррентного уравнения:

$$q_t = P_t^* q_{t-1} + \Delta Q_t^q \qquad (1)$$

где P - постоянная матрица перехода с начальным состоянием p_0, что означает, что в начальный момент времени канал не загружен.

Если обозначить RTT как Y_t, его динамику можно описать с помощью дискретного марковского процесса:

$$Y_t = \lambda_t^* \left(I - diag\ q_t\right) \theta_{t-1} Y_{t-1} + \mu^* S_t \theta_{t-1} + \Delta M_t^Y, \qquad (2)$$

где λ – вектор, состоящий из диагональных элементов матрицы переходных вероятностей;

I – индикаторная функция;

q – вектор вероятностей скачка процесса Y без смены состояния θ;

θ – марковская цепь;

Y – входной случайный процесс;

μ – стохастическая мера;

S – конечное число состояний $\{e_1, \ldots, e_N\}$ цепи θ;

M – мартингал.

Данный процесс порожден марковской цепью q_t и последовательностями $\{V_t\}$ и $\{X_t\}$. Порождающую последовательность индикаторов скачков без смены состояния марковской цепи $\{V_t\}$ можно задать следующим вектором вероятностей

$p_t = p = (0{,}05;0{,}05;0{,}05;0{,}05;)^*$. На практике это означает, что в моменты времени $t_k^{//}$ отличные от моментов переходов состояния марковской цепи q_t, значение времени кругового обращения может измениться с вероятностью $p_i = 0{,}05$ вне зависимости от состояния цепи q_t и времени. Кроме этого, предполагается, что распределение RTT остается таким же, как и на предыдущем шаге.

В качестве закона распределения времени кругового обращения в случае загруженного канала, можно выбрать логарифмически нормальное распределение $\psi_1(y)$, для которого $m_\eta = 5$, $\sigma = 0{,}5$ рис. 1, 1. В случае свободного канала, распределение RTT описывается логарифмически нормальным распределением $\psi_2(y)$ с соответствующими параметрами $m_\eta = 2$, $\sigma = 1$ рис. 2.1, 2.

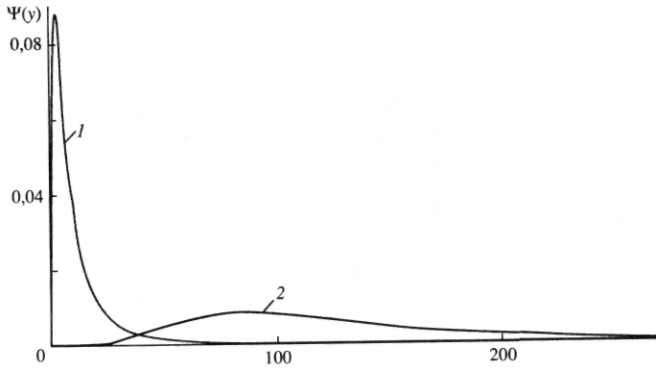


Рис. 1. Плотность распределения RTT

Таким образом, $\{X_t\}$ может быть представлен как последовательность независимых одинаково распределенных четырехмерных векторов с составляющими $x_t^1, x_t^2 \sim \psi_1(y)$ для незагруженных состояний сети $q_t \in \{e_1, e_2\}$ и $x_t^3, x_t^4 \sim \psi_2(y)$ - для загруженных ($q_t \in \{e_3, e_4\}$).

В дополнение к уравнениям состояния (1) и (2) необходимо так же рассмотреть наблюдаемый процесс потери пакетов:

$$\eta_t = A_t^* \theta_{t-1}, \tag{3}$$

где A = (0,1,0,1).

В уравнении наблюдения (3) учтено, что наблюдения являются незашумленными. При этом $\eta_t = 1$ в случае потери пакета или $\eta_t = 0$ если потерь нет.

Можно также предположить, что в моменты, когда потери пакетов отсутствуют, возможны измерения RTT с некоторым шумом:

$$\xi_t = (e_1 + e_3)^* \theta_{t-1} Y_{t-1} + \varepsilon_t, \tag{4}$$

где ε_t - последовательность одинаково распределенных ошибок измерения, распределенных по логарифмически нормальному закону с параметрами $m_\eta = 0, \sigma = 1.$

Задача оптимального оценивания в реальном времени вектора зависимости RTT от состояния канала ($\overline{Y}_t = \left(\theta_t^*, Y_t\right)^*$) по доступным наблюдениям $\{\eta_t, \xi_t\}$ является частой задачей оптимальной нелинейной фильтрации марковских процессов. Для сравнения – в стандартном протоколе TCP [1] для оценки значения RTT используется алгоритм стохастической аппроксимации:

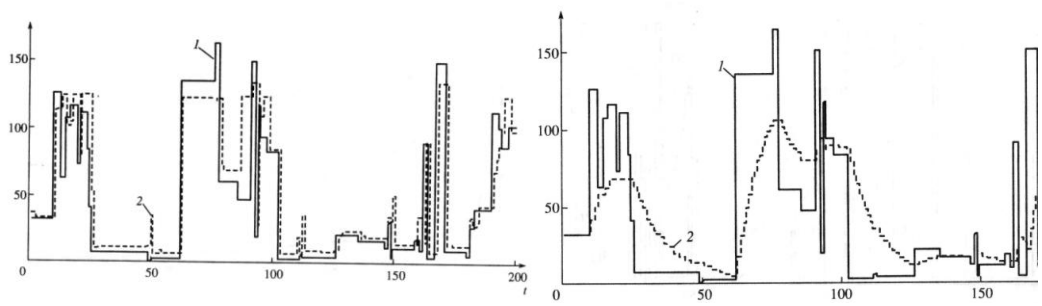
$$\hat{R}_k = \hat{R}_{k-1} + \alpha(M - \hat{R}_{k-1}), \tag{5}$$

где $\hat{R}$ – оценка текущего значения RTT;

α – усилительный коэффициент фильтра (шаговая постоянная, определяющая скорость сходимости к установившемуся состоянию и обеспечивающая устойчивость оценки при $0 < \alpha \le 1$);

M – измерение RTT последнего подтвержденного пакета.

Сравнение результата оценок с использованием оценки по зашумленным наблюдениям и стандартной оценки TCP приведены на рис.2, а (для оценки по зашумленным наблюдениям) и б (для стандартного TCP).



а б

Рис. 2. Изменение RTT и его оценки при зашумленных наблюдениях (а) и стандартным способом (б)

Как следует из анализа, вне зависимости от версии протокола TCP его работа в сети более корректно представляется и поддается описанию и предсказанию с помощью аппарата случайных процессов. В отличие от используемых на сегодняшний день процедур стохастической аппроксимации для случайных величин, случайные процессы требуют более сложных процедур оценки, прежде всего процедур Калмана-Бьюси. Триада уравнений наблюдения, состояния и оценки для случайных процессов в общем виде может быть записана как [4]:

$$y(t) = H(t)x(t) + \upsilon(t), \tag{6}$$

$$\frac{dx(t)}{dt} = A(t)x(t) + C(t)\xi(t), \tag{7}$$

$$\frac{d\hat{x}(t)}{dt} = A(t)\hat{x}(t) + V(t)H^{\mathrm{T}}(t)N_{\upsilon}^{-1}[H(t)\hat{x}(\mathrm{t}) - \mathrm{y(t)}], \tag{8}$$

$$\frac{dV(t)}{dt} = A(t)V(t) + V(t)A^{T}(t) - V(t)H^{T}N_{\upsilon}^{-1}H(t)V(t) + C^{T}(t)N_{\xi}C(t), \tag{9}$$

где N_{ξ} – шум генерации в модели состояния;

N_{υ} шум наблюдения в уравнении наблюдения.

Точность оценки параметра RTT – одного из важнейших показателей производительности сети и главного определяющего параметра при расчете таймеров TCP в случае использования математического аппарата марковских цепей и случайных процессов намного выше, чем в случаях использования стандартных, зачастую эвристических, методов.

Литература:

1. Jacobson V. Congestion Avoidance and Control // Comput. Commun. Rev. 1988. V. 18. №4. P. 314-329.

2 Jacobson V. Modified TCP Congestion Control and Avoidance Alogrithms // Technical Report 30,Apr 1990.

3 Brakmo L.S., Peterson L.L. // TCP Vegas: End to End Congestion Avoidance on a Global Internet // IEEE Journal on Selected Areas in Communication, vol. 13[1995],(1465-1490)

4 Поповский В.В., Олейник В.Ф. Математические основы управления и адаптации в телекоммуникационных системах: учеб./ -Х.: ООО "Компания СМИТ", 2011. - 362с.

Секция № 2

БЕСПРОВОДНЫЕ СЕТИ И ТЕХНОЛОГИИ

НАВЧАЛЬНО – ЛАБОРАТОРНИЙ КОМПЛЕКС ДЛЯ ВИВЧЕННЯ АНАЛОГОВИХ ЕЛЕКТРОНІКИ ТА СХЕМОТЕХНІКИ

Бондаренко М.Ф., Онищенко В.О., Семенець В.В., Тиртишніков О.І., Крук О.Я.
Харківський національний університет радіоелектроніки
61166, Харьків, пр. Леніна, 14
Полтавський національний технічний університет імені Юрія Кондратюка
36601, м. Полтава, Першотравневий проспект, 24, каф. комп'ютерної інженерії,
тел. (0532) 7-18-55

The urgency of development of "intellectual" laboratory stands for studying electronics and the analog circuitry, equipped by flexible multipurpose system of protection against mistakes and "incorrect" actions of the user is shown.

Вступ

Особливе місце в системі підготовки інженерів радіотехнічного профілю займають лабораторні практикуми по дослідженню властивостей компонентів і типових схем – як аналогових, так і цифрових пристроїв і функціональних вузлів. Причому, якщо цифрові пристрої на логічному рівні можуть цілком адекватно моделюватися програмними засобами, то дослідження на фізичному рівні (на рівні струмів і напруг) аналогових схем необхідно проводити з використанням реального вимірювального устаткування й відповідних лабораторних стендів (ЛС).

Проведене авторами оглядове дослідження ринку виявило, зокрема, практично повну відсутність сучасних, доступних і надійних технічних рішень для проведення лабораторних практикумів з аналогових електроніки та схемотехніки, при безсумнівній наявності потреби в таких. Тому фахівцями Харківського національного університету радіоелектроніки та Полтавського національного технічного університету імені Юрія Кондратюка, на підставі угоди про співробітництво між названими університетами, був спільно розроблений комплект ЛС, призначений для вивчення основ електроніки й аналогової схемотехніки. ЛС дозволяють одержати практичні навички дослідження різноманітних напівпровідникових приладів, схем на транзисторах й ОП (підсилювачів, генераторів, активних RC- фільтрів й ін.).

Крім того, виявилася ї недостатність сучасної вітчизняної навчальної літератури з аналогових електроніки та схемотехніки.

Нині навчально-лабораторний комплекс складається з трьох лабораторних стендів та відповідного лабораторного практикуму.

Склад та особливості комплекту лабораторних стендів

Багаторічний досвід проведення авторами лабораторних робіт дозволяє стверджувати, що переважна більшість відмов лабораторного устаткування, у силу специфіки його використання, відбувається саме під впливом експлуатаційних факторів, які є, порівняно з іншими, найменш передбачуваними. Отже, одним з найбільш ефективних способів підвищення надійності й відмовостійкості ЛС є оснащення їх гнучкою й багатофункціональною («інтелектуальною») системою управління і захисту устаткування від помилок й «некоректних» дій користувача, що виконує лабораторну роботу. Саме така система на основі мікроконтролера фірми Atmel реалізована в комплекті лабораторних стендів ЛС-1, 2, 3, що і є головною особливістю стендів [1].

Нині комплекти лабораторних стендів ЛС-1, 2, 3 використовуються в навчальному процесі на кафедрах біомедичних електронних приладів і систем, радіоелектронних пристроїв, основ радіотехніки, мікроелектроніки, проектування та експлуатації електронних апаратів Харківського національного університету радіоелектроніки (28 комплектів) та на кафедрах комп'ютерної інженерії, комп'ютерних інформаційних технологій та систем Полтавського національного технічного університету імені Юрія Кондратюка (14 комплектів).

Комплект ЛС, призначений для вивчення основ електроніки й аналогової схемотехніки, складається з трьох плат: ЛС-1, ЛС-2, ЛС-3. На рис. 1, 2, 3 показано їх зовнішній вигляд.

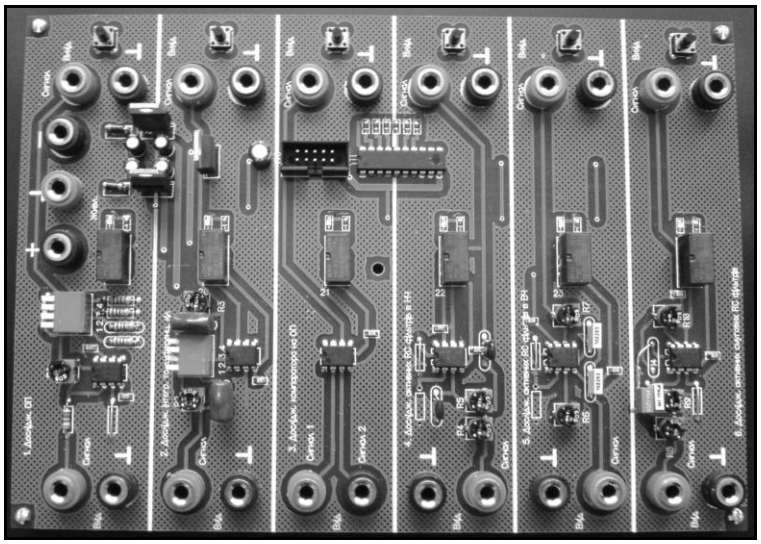


Рис. 1 – Зовнішній вигляд ЛС-1

ЛС-1 орієнтований на вивчення операційних підсилювачів (ОП) та схем, побудованих на його основі. Стенд дозволяє проводити лабораторні роботи по дослідженню підсилювача на ОП з інвертуючим входом, схем інтегратора, диференціатора і компаратора, активних RC фільтрів на ОП.

ЛС-2 забезпечує дослідження властивостей напівпровідникових елементів і схем з їх застосуванням. Він дозволяє проводити лабораторні роботи по дослідженню вольтамперних характеристик різних напівпровідникових приладів: випрямляючого діода, світлодіода, стабілітрона, біполярного та польового транзисторів, а також схем мультивібратора, транзисторного ключа та генератора пилкоподібної напруги.

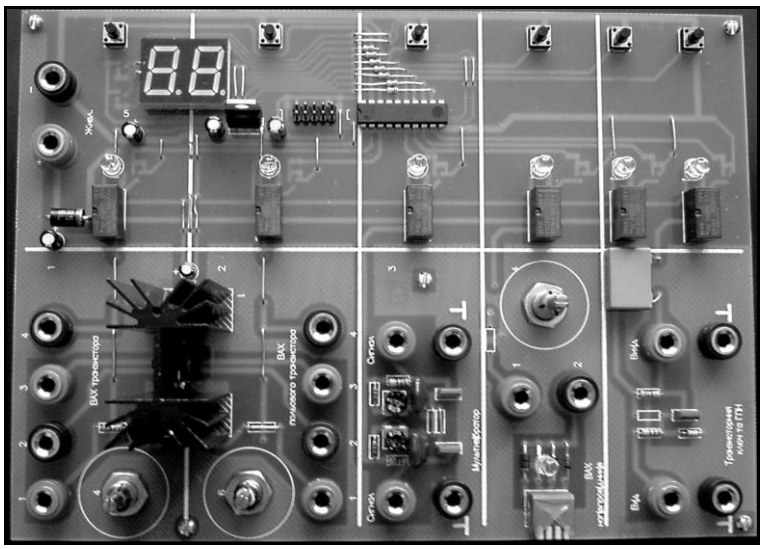


Рис. 2 – Зовнішній вигляд ЛС-2

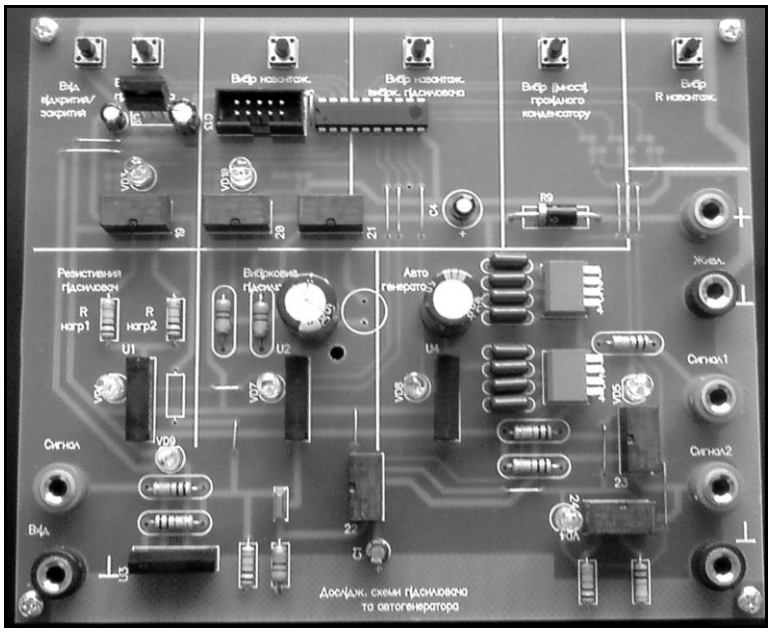


Рис. 3 – Зовнішній вигляд ЛС-3

ЛС-3 орієнтований на дослідження підсилювальних та генераторних схем, побудованих на біполярних транзисторах, а саме: підсилювача напруги, вибіркового підсилювача та генератора – триточки.

Як видно, ЛС є секціонованими, тобто на кожній платі розміщений набір схем, згрупованих за конструктивними та функціональними ознаками. Шина живлення пристроїв є загальною і комутованою. Вибір пристрою для дослідження і подача живлення на нього відбувається за допомогою схеми управління, реалізованої на мікроконтролері і наборі реле, що повністю усуває необхідність будь-яких перекомутацій блоку живлення при зміні досліджуваного пристрою.

Організаційне та методичне забезпечення лабораторного практикуму

Типове лабораторне робоче місце складається з комплекту ЛС, функціонального генератора, лабораторного блока живлення, двоканального осцилографа та мультиметра. Можливий варіант комплектації робочого місця показаний на рис. 4.

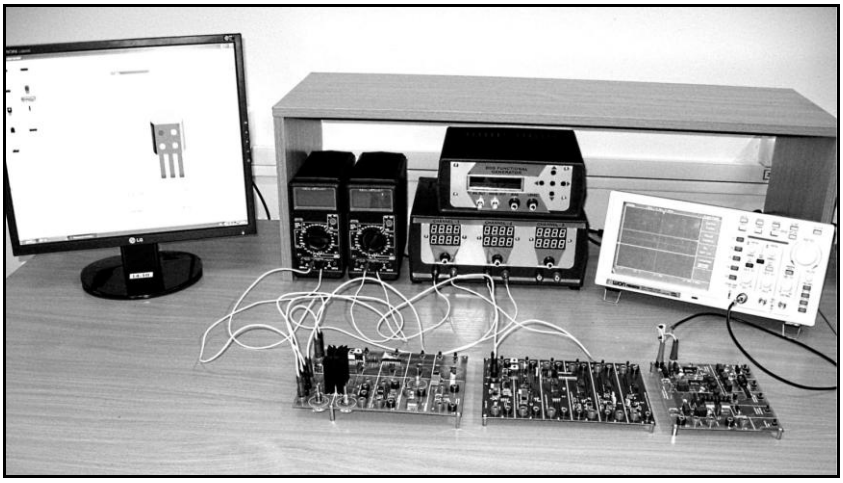


Рис. 4 – Варіант комплектації лабораторного робочого місця

Лабораторний практикум з аналогової електроніки та схемотехніки [2], який містить методичні рекомендації щодо проведення 14 лабораторних робіт, також спільно розроблений фахівцями Харківського національного університету радіоелектроніки і кафедри комп'ютерної інженерії Полтавського національного технічного університету імені Юрія Кондратюка та виданий в обох названих університетах. Він узагальнює досвід практичної експлуатації ЛС при викладанні дисциплін: «Теорія електричних кіл», «Теорія електричних кіл та сигналів», «Аналогова схемотехніка», «Основи схемотехніки», «Основи електротехніки та електроніки» та інших для майбутніх інженерів різних напрямів підготовки.

Висновки

Реалізована в лабораторних стендах система захисту, що використовує як стандартні, так й «інтелектуальні» рішення, дійсно забезпечує надійне й безвідмовне функціонування стендів. Наприклад, за три роки інтенсивного використання в навчальному процесі Полтавського національного технічного університету імені Юрія Кондратюка чотирнадцяти комплектів ЛС не зафіксовано жодної їхньої відмови.

Найближчим часом лабораторний практикум, з врахуванням результатів його практичної апробації, буде допрацьований до начального посібника, який планується для подання на отримання грифу міністерства освіти і науки, молоді та спорту України.

В подальшому планується доповнення комплексу стендом ЛС-4, на якому будуть реалізовані типові схеми вторинних джерел електроживлення електронних пристроїв, а саме: перетворювач постійної напруги у змінну, два блоки живлення – імпульсний та безпосереднього перетворення. Відповідно, лабораторний практикум буде доповнений трьома лабораторними роботами із дослідження відповідних вторинних джерел електроживлення.

Література:

1. Аврунин О.Г., Корж Ю.Н., Крук О.Я., Носова Т.В., Семенец В.В., Тиртишніков О.І. Обеспечение отказоустойчивости лабораторных стендов для изучения аналоговой электроники и схемотехники // Радіоелектронні і комп'ютерні системи. – ХАІ, 2010. – 7(48). – с. 147 – 151.

2. Бондаренко М.Ф., Онищенко В.О., Семенець В.В., Нікулін М.Б., Крук О.Я., Корж Ю.М. Лабораторний практикум з аналогової електроніки та схемотехніки // Харків: ХНУРЕ, Полтава: ПолтНТУ, 2011, 70 с.

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ СЕЛЕКТИВНЫХ УСТРОЙСТВ НА ВОЛНОВОДАХ СЛОЖНОГО СЕЧЕНИЯ ДЛЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Г.Ф. Заргано[1], В.В. Земляков[1], О.С. Лабунько[2]
[1]Южный федеральный университет
344090, Россия, г. Ростов-на-Дону, ул. Зорге 5, физический факультет, тел. (863) 297-51-29
[2]Радиочастотный центр южного федерального округа
344002, Россия, г. Ростов-на-Дону, пр. Буденновский, д.50, тел. (863) 290-33-77
E-mail: zargano@yandex.ru[1], vvzem@yandex.ru[2], kan@rfc-south.ru[3]

The problems of analysis and synthesis of directional couplers with the system of small rectangular and crossline apertures, band-pass filters on transverse junctions and mode transformers on double ridge waveguides are solved. Electromagnetic fields and cutoff wave numbers are calculated by method of partial regions including field singularities at the edge. The synthesis results for each type of devices are given.

Введение. Развитие телекоммуникационных систем связано с постоянным повышением требований к электрическим, эксплуатационным характеристикам, а также массогабаритным показателям элементов и устройств, входящих в приемо-передающие тракты и узлы обработки сигналов, что в свою очередь приводит к возрастанию сложности современных систем и требует поиска решений по созданию аппаратуры нового поколения. Необходимость передавать большие мощности при минимальных потерях даже в миллиметровом диапазоне приводит к необходимости использования волноводных элементов при конструировании основных узлов. Большую актуальность в этой области имеет широкий класс селективных волноводных устройств, к которым относятся канало-селективные устройства (направленные ответвители, ди- и мультиплексоры), частото-селективные устройства (фильтры), а также относительно новый тип – модо-селективные устройства или модовые волноводные трансформаторы.

На сегодняшний момент алгоритмы и методики анализа и синтеза селективных волноводных устройств на волноводах простых сечений (круглых и прямоугольны) достаточно хорошо отработаны и соответствующая элементная база практически не требует доработок. Однако, существенным недостатком волноводов простого сечения является их узкополосность, что в современном мире широкополосных сигналов значительно снижает их возможности и повышает массогабаритные показатели устройств и сложность итоговой аппаратуры в связи с необходимостью одновременного использования нескольких волноводов, настроенных на разные рабочие поддиапазоны.

Проблема узкополосности волноводных трактов может быть решена путем перехода на волноводы сложного сечения (ВСС), например, гребневые волноводы, которые позволяю расширить рабочий диапазон частот до трех и более октав. К сожалению, алгоритмы и методики разработки устройств на волноводах простого сечения не могут быть непосредственно перенесены на волноводы сложного сечения, что объясняется, во многом, отсутствием точного решения задачи о собственных значения ВСС и необходимостью приближенного расчета электромагнитных полей с очень высокой степенью точности.

Наиболее эффективным методом расчета электродинамических характеристик ВСС, поперечное сечение которых может быть разбито на простые прямоугольные непересекающиеся области, является метод частичных областей с учетом особенности электромагнитного поля на ребре, хорошо зарекомендовавший себя, как с точки зрения скорости расчетов, так и по точности получаемых результатов [1].

Несмотря на то, что ВСС известны и применяются уже на протяжении более 30 лет, и результаты расчетов ряда основных базовых элементов, хотя и с малой точностью, представлены в литературе, к настоящему моменту отсутствует отработанная единая методика анализа и синтеза полнофункциональных селективных устройств на волноводах сложного сечения.

Данная работа посвящена построению алгоритмов и разработке методик синтеза направленных ответвителей с малыми отверстиями связи, полосовых фильтров на плоско-поперечных неоднородностях и модовых волноводных трансформаторов на изгибах и плавных вариациях поперечного сечения для ВСС, в частности, для П- и Н-волноводов.

Направленные ответвители с малыми отверстиями связи. Одним из наиболее распространенных типов направленных ответвителей (НО) являются ответвители с системой малых отверстий связи, классической теорией для расчета которых является квазистатическая теория Бете [2]. В этом случае пара волноводов, соединенных отверстием связи, представляется идеальным восьмиполюсником, для которого рассчитываются элементы матрица рассеяния. Для поиска характеристик НО, состоящего из серии последовательно распложенных отверстий связи используется теория каскадного соединения многополюсников.

Анализ характеристик рассеяния одиночных прямоугольных отверстий связи был подробно проведен в работе [2]. В частности было показано, что при построении многоэлементных широкополосных направленных ответвителей наиболее эффективно использовать либо крестообразные элементы связи, либо узкие прямоугольные щели, повернутые вокруг своей оси.

В данной работе с помощью разработанной методики был произведен синтез НО с переходным ослаблением 20 дБ для Н-волновода с размерами h/l=0.465, g/l=0.749, c/l=0.197, путем минимизации среднеквадратичного отклонения переходного ослабления от заданных значений. Область связи в НО образована двумя рядами по 20 одинаковых крестообразных отверстий (рис. 1) и двумя рядами по 20 одинаковых повернутых прямоугольных отверстий.

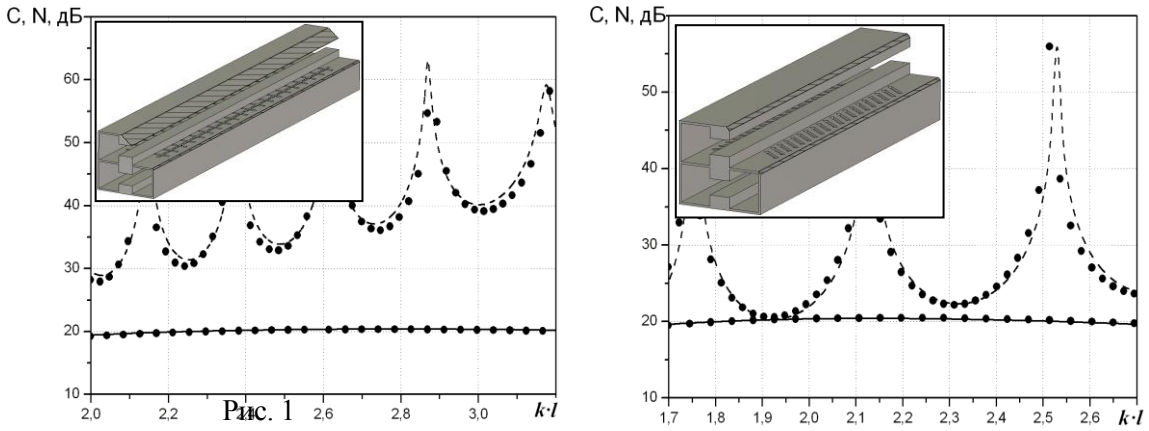


Рис. 1

Размеры и размещение крестообразных отверстий связи: x_0 = 0.4727 – смещение центров отверстий связи относительно боковой стенки волновода, a x b = 0.2673 x 0.0525 – размеры отверстия, Δl = 0.6017 – расстояние между центрами отверстий. На рис. 1 приведены зависимости направленности N (пунктирная линия) и переходного ослабления C (сплошная линия) синтезированного НО. Из графиков на рис. 1 видно, что НО обладают хорошей широкополосностью (~45÷50%) с перепадом переходного ослабления не более ± 0.5 дБ и направленностью не менее 30 дБ. Относительный продольный размер синтезированного НО составил L/l = 11.4 или L/λ = 4.7 – где λ – центральная длина волны рабочего диапазона.

Размеры и размещение прямоугольных отверстий связи: x_0 = 0.4140, a x b = 0.3220x 0.0515, Δl = 0.3442, $\alpha = 41.65^0$ – угол поворота отверстия. На рис. 2 также приведены зависимости направленности и переходного ослабления синтезированного НО. Данный НО также обладают хорошей широкополосностью (~45÷50%) с перепадом переходного ослабления не более ± 0.5 дБ и направленностью не менее 20 дБ, однако его относительный продольный размер составил L/l = 6.6 или L/λ = 2.3.

Для проверки достоверности получаемых результатов было проведено сравнение с результатами численного эксперимента, осуществленного с помощью компьютерного моделирования сеточными численными методами, решающими поставленную задачу в строгой постановке. Результаты компьютерного моделирования представлены на рис. 1 маркерами. Необходимо отметить, что применение сеточных методов, особенно в задачах многопараметрической оптимизации, даже сегодня при наличии мощных ЭВМ является весьма трудоемким и длительным процессом, поэтому их наиболее эффективно использовать лишь на последнем этапе синтеза. Применение прямоугольных отверстий связи, повернутых на некоторый угол вокруг своей оси, позволяет уменьшить продольный размер устройства и упростить его компьютерное моделирование, по отношению к НО с крестообразными отверстиями связи, а также добавить дополнительный свободный параметр в процедуру синтеза НО – угол поворота, что дает возможность улучшить характеристики получаемых устройств. Однако, отсутствие направленности у прямоугольного элемента связи в отличие от крестообразного, приводит к тому, что уровень направленности синтезированного НО в среднем на 10 дБ ниже, чем у НО на рис. 1.

Полосно-пропускающие фильтры на плоско-поперечных неоднородностях. При исследовании селективных свойств сложных микроволновых устройств, содержащих плоско-поперечные неоднородности (стыки, сдвиги и тонкие диафрагмы) в ВСС, необходимо решать задачу нахождения многоволновых обобщенных матриц рассеяния [3].

Коэффициенты отражения и прохождения всех волн находятся из условия равенства электрического поля на апертуре неоднородности с учетом ортогональности собственных векторных функций волноводов. Неизвестное векторное электрическое поле в отверстии неоднородности в виде разложения по собственным векторным функциям, удовлетворяющим граничным условиям на контуре апертуры неоднородности.

Используя формулы для матриц рассеяния каждого из соединяемых многополюсников, получаем матрицу рассеяния в случае каскадного соединения двух многополюсников. При решении задачи синтеза селективного устройства удобно совместно пользоваться методами радиотехнического и прямого синтеза. Первый позволяет выбрать модель фильтра, представляющую собой цепь на сосредоточенных элементах, и провести расчет параметров волноводных неоднородностей и длин регулярных отрезков волновода на основе этой модели. Такой метод не позволяет получить точные значения заданных характеристик проектируемого устройства, однако приближенное решение задачи синтеза на выходе радиотехнического этапа может быть использовано в качестве начальной точки для процедуры многопараметрической оптимизации в процедуре прямого синтеза.

Результаты электродинамического анализа и синтеза частото-селективных устройств на базе тонких диафрагм, плоско-поперечных сдвигов как с четвертьволновыми, так и с непосредственными связями приведены в работах [3].

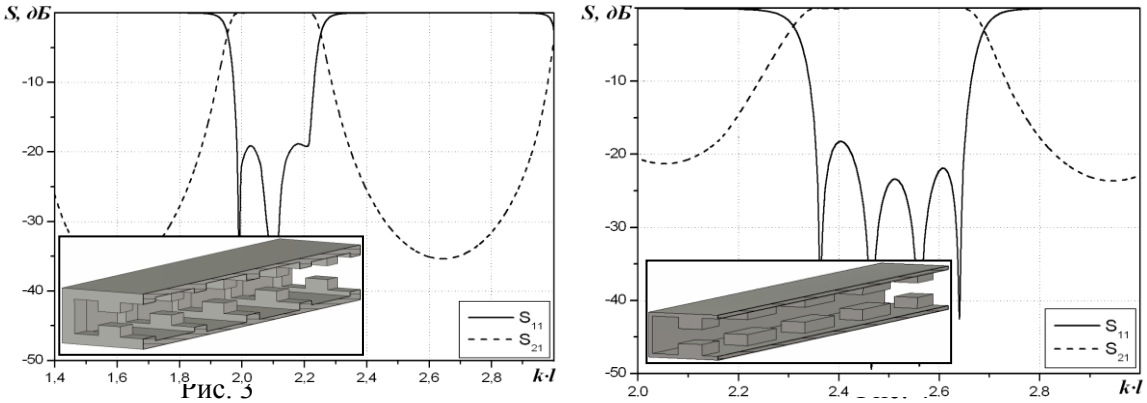


Рис. 3

В данной работе приведем результаты синтеза полосно-пропускающих фильтров на плоско-поперечных стыках Н-волноводов. Используем Н-волновод с размерами $h/l = 0.5$, $c/l = 0.4$, $a/l = 0.314$. Одним из популярных базовых стыков при конструировании таких

фильтров является стык Н-волновода с прямоугольным. На рис. 3 представлен внешний вид синтезированного фильтра. В данной конструкции прямоугольные волноводы играют роль объемных резонаторов, соединенных четвертьволновыми отрезками Н-волновода. Фильтр, представленный на рис. 4, также имеет в своей конфигурации отрезки прямоугольного волновода, однако в данном случае он выполнен в виде единой линейной структуры. С точки зрения производства такая конструкция является технологически более удобной, но ее селективные свойства оказываются несколько хуже, чем в предыдущем случае. На рис. 3 и 4 представлены зависимости S-параметров от нормированного волнового числа для представленных фильтров.

Модовые трансформаторы на волноводах сложного сечения. Технология проектирования МВТ на плавных изгибах волноводов позволяет создавать устройства с достаточно широкой полосой пропускания (до 10%), очень высокой эффективностью преобразования (до 99%), а также позволяют трансформировать пары распространяющихся мод практически в любых комбинациях.

Для расчета изогнутых волноводных элементов и элементов с плавно изменяющимся поперечным сечением наиболее эффективно применение метода поперечных сечений (МПС) [4].

Согласно МПС, электромагнитное поле в каждом поперечном сечении нерегулярного участка волновода представляется суммой волн регулярного волновода того же сечения с неизвестными амплитудными коэффициентами. Относительно этих коэффициентов, являющихся с точностью до некоторого множителя амплитудами волн, распространяющейся соответственно в положительном и отрицательном направлениях, из уравнений Максвелла следует бесконечная система линейных обыкновенных дифференциальных уравнений первого порядка. Связь различных мод волновода, распространяющихся в положительном и отрицательном направлениях определяется с помощью коэффициентов связи, которые являются функциями геометрии деформации, и могут быть получены в явном виде из общих интегральных уравнений [4] через функции, пропорциональные соответственно продольным компонентам электрического и магнитного векторов Герца волновода.

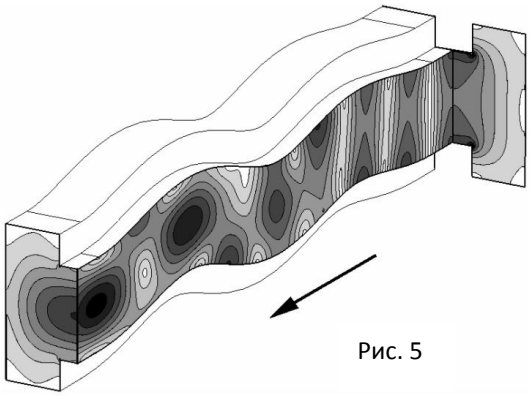


Рис. 5

Таблица 2

Нормированные критические волновые числа Н-волновода

Порядковый номер волны	Волна	$k_c \cdot l$
1	H^1_{eo}	1.239455
2	H^1_{oe}	1.672907
3	H^1_{oo}	1.844090
4	E^1_{oo}	2.827031
5	H^1_{ee}	2.903666
6	H^2_{eo}	3.343241

Рассмотрим пример моделирования МВТ на изгибах Н-волновода. При расчетах и моделировании МВТ использовался квадратный Н-волновод с размером гребней: ширина – 0.25l, высота – 0.2l, где l – поперечный размер волновода. Таблица 2 дает представление о спектре нормированных критических волновых чисел $k_c \cdot l$ исследуемого Н-волновода. Индекс «*e*» в обозначении типа волны соответствует граничному условию типа электрической стенки на осях симметрии волновода, индекс

«*о*» - граничному условию типа магнитной стенки, а верхний индекс соответствует номеру волны при данных граничных условиях.

Рассмотрим трансформатор моды H^1_{eo} в моду E^1_{oo} на изгибах Н-волновода с нормированным волновым числом $k \cdot l$ = 3.18. В этом случае количество распространяющихся мод равно – 5 (таблица 2). Однако, в трансформации данной пары мод при изгибе волновода в плоскости YZ, исходя из правила отбора, будут участвовать только три моды - H^1_{eo}, H^1_{oo}, E^1_{oo}. В качестве критерия оптимизации геометрии трансформатора выберем требование максимального уровня затухания паразитных мод, в том числе и входной, на выходе преобразователя не более -20 дБ. Относительная длина трансформатора составила по оси *z*: *L*/*l* = 8, что соответствует $L/\lambda = 4$. Ширина этой полосы во многом зависит от количества периодов базовой функции и определяется обычно по уровню затухания паразитных мод на выходе трансформатора -10дБ. Для оптимизированных трансформаторов эта величина составила 7.5%.

На рис. 5 приведен результат моделирования модуля электрического поля в плоскости YZ для трансформатора H^1_{eo} - E^1_{oo} на линии *x* = 0. Для повышения наглядности на рисунке показаны также распределения модуля электрического поля на входе и выходе трансформатора в плоскости *XY* для соответствующих мод.

Литература:

1. Заргано Г.Ф., Ляпин В.П., Михайлевский В.С и др. Волноводы сложных сечений. – М.: Радио и связь, 1986. – 124 с.
2. Заргано Г.Ф., Земляков В.В., Пелецкий Р.В., Г.П. Синявский. Исследование параметров связи П-волноводов через малые отверстия различной формы // Электромагнитные волны и электронные системы. – 2009. – № 5. с. 29-37.
3. Г.Ф. Заргано, В.В. Земляков, А.В. Хохлачев. «Моделирование фильтров с непосредственными связями на тонких диафрагмах в желобковых волноводах». // Электромагнитные волны и электронные системы, 2008, № 5, с. 71-76.
4. В.В. Земляков, Г.Ф. Заргано, Г.П. Синявский. «Трансформация мод при изгибах Н-волноводов». // «Радиотехника и электроника», т. 53, № 2, 2008, с. 177-183

ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПРИМЕНЯЕМЫЕ ДЛЯ ОПИСАНИЯ ОСНОВНЫХ СВОЙСТВ СЛОЖНЫХ СИСТЕМ РАДИОКОНТРОЛЯ

Корниенко С.А.
Северо-Кавказский государственный технический университет
355000, Ставрополь, пр.Кулакова,2, каф. Защиты Информации, тел. (88652) 95-65-46,
E-mail:rfc-stv@yandex.ru; факс (88652) 95-6546

This article presents a set of functional characteristics that must be considered in the analysis and synthesis of radio control (RCC) in different conditions. Problems arising in the analysis, require quantitative (numerical) evaluation of the behavior. The article describes the requirements for numerical characteristics. For the analysis of selected characteristics for which more appropriate analysis: efficacy, safety, quality control, noise, estimation of complexity.

Введение

Количественные данные о поведении СРК можно получить: 1) экспериментально; 2) наблюдением; 3) математическим описанием системы. Наиболее достоверной будет оценка СРК с использованием математического описания или с помощью числовых характеристик. Каждая числовая характеристика должна удовлетворять следующим требованиям [1]:

1) величина должна зависеть от процесса функционирования системы, которая вычисляется исходя из математического описания СРК;

2) давать наглядное представление об одном из свойств СРК;

3) допускать приближенную оценку по экспериментальным данным.

Теоретическая часть

Выберем числовые характеристики, которые зависят от процесса функционирования СРК, и описывают ее основные свойства, например: эффективность, надежность, качество управления, помехозащищенность, оценка сложности.

Рассмотрим показатель эффективности. Под показателями эффективности сложной СРК будем понимать такую числовую характеристику системы, которая оценивает степень приспособленности системы к выполнению поставленных перед ней задач.

Основными задачами СРК, является [2]:

1) выявление неразрешенных для использования РЭС и прекращение их работы;

2) выявление источников радиопомех (как непреднамеренных, так и специально организованных);

3) контроль загрузки радиочастотного спектра в широком диапазоне радиочастот;

4) определение местоположения источников несанкционированных радиоизлучений;

5) обеспечение электромагнитной совместимости РЭС.

Сложные системы (СС) функционируют в условиях действия большого числа случайных факторов. Поэтому результаты работы СС будут носить случайный характер. Для того чтобы оценка эффективности системы относилась к некоторому среднему ее поведению и не зависела от случайного сочетания действующих на систему факторов, в качестве показателей эффективности выберем вероятности соответствующих случайных событий или средние значения (математическое ожидание) соответствующих величин. Любой показатель эффективности R зависит от ряда параметров. Среди них основную роль играют параметры системы (технические, информационные, эксплуатационные, экономические, временные, социальные) $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ и параметры, характеризующие воздействия внешней среды $\beta_1, \beta_2, \beta_3, \ldots, \beta_m$. Таким образом показатель эффективности можно записать выражением:

$$R=R(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n ; \beta_1, \beta_2, \beta_3, \ldots, \beta_m) \quad (1)$$

В [3], определены коэффициенты характеризующие показатели качества СРК:

1) диапазон рабочих частот обнаружения и технического анализа - $К_{ДРЧ}$,

2) диапазон пеленгования - $К_{ДП}$,
3) чувствительность приемника - $К_{ЧПРМ}$,
4) динамический диапазон свободный от интермодуляции - $К_{ИНТЕРМ}$,
5) инструментальная погрешность(точность пеленгования) – $К_{ИПОГР}$,
6) время пеленгования - $К_{ВПЕЛ}$,
7) помехоустойчивость - $К_{ПОМЕХ}$,
8) надежность - $К_{НАД}$,
9) скорость сканирования (без пеленгования, с пеленгованием) – $К_{ССБПЕЛ}$ и $К_{ССПЕЛ}$ соответственно,
10) полоса мгновенного обзора - $К_{ПМО}$,
11) коэффициент использования оборудования - $К_{ИО}$,
12) удобство эксплуатации - $К_{УЭКСПЛ}$,
13) стоимостные и временные характеристики – $К_{СТ}$ и $К_{ВР}$,
14) социальная значимость - $К_{СОЦ}$, поэтому вектор отдельных показателей качества системы РК можно представить:
$К=< К_{ДРЧ}, К_{ДП}, К_{ЧПРМ}, К_{ИНТЕРМ}, К_{ИПОГР}, К_{ВПЕЛ}, К_{ПОМЕХ}, К_{НАД}, К_{ССБПЕЛ}, К_{ССПЕЛ}, К_{ПМО}, К_{ИО}, К_{УЭКСПЛ}, К_{СТ}, К_{ВР}, К_{СОЦ}>$, тогда в качестве лучшего значения вектора приймем максимум взвешенной суммы:

$$К_{\Sigma}= \lambda_1 К_{ДРЧ} +\lambda_2 К_{ДП} +\lambda_3 К_{ЧПРМ} +\lambda_4 К_{ИНТЕРМ} +\lambda_5 К_{ИПОГР} +\lambda_6 К_{ВПЕЛ} + \\ +\lambda_7 К_{ПОМЕХ}+ +\lambda_8 К_{НАД} +\lambda_9 К_{ССБПЕЛ} + \lambda_{10} К_{ССПЕЛ} +\lambda_{11} К_{ПМО} + \lambda_{12} К_{ИО+} \\ + \lambda_{13} К_{УЭКСПЛ} + \lambda_{14} К_{СТ} + +\lambda_{15} К_{ВР} +\lambda_{16} К_{СОЦ} \qquad (2)$$

где λ_i - $i=\overline{1,m}$ — коэффициенты, характеризующие важность показателей качества СРК.
Внешними воздействиями на СРК могут быть такие показатели, как: электромагнитная обстановка в районе размещения СРК, загруженность радиочастотного спектра в диапазоне работы СРК, климатические условия в которых эксплуатируется СРК. Но показатель эффективности зависит не только от показателей качества системы и внешней среды, а и от структуры системы, характера связей между подсистемами разных уровней, вида управляющего алгоритма и закономерностей функционирования.
Поэтому при оценке эффективности необходима серьезная проработка алгоритмов как оценки организационной структуры службы РК, так и оценки аппаратурной составляющей элементов подсистем различных уровней, в том числе анализа состояний самих подсистем по отношению к общей СРК.

Далее рассмотрим такой показатель, как качество управления, которому в СС принадлежит исключительная роль. Оценка качества управления является одной из наиболее важных сторон общей оценки эффективности системы.
В СС выделяют специальные элементы — обеспечивающие переработку информации для целей управления. Осуществляемые ими функции условно можно назвать принудительным управлением. Качество управления в СС зависит от многочисленных факторов. Наиболее существенные из них для удобства рассмотрения можно свести в следующие четыре группы:
1) факторы, связанные с качеством критериев управления,
2) факторы, определяющие частоту циклов управления,
3) факторы, характеризующие качество осведомительной информации,
4) факторы, связанные с качеством оператора (алгоритма) управления.
Проблема оценки качества управления еще недостаточно исследована. Поэтому в настоящее время нет возможности предложить универсальные методы ее решения. Имеется некоторый опыт, позволяющий рассматривать задачи, встречающиеся в практике системотехники. Остановимся кратко на этом вопросе.

В первую очередь рассмотрим задачу сравнительной оценки качества управления. Пусть заданна конкретная СС, эффективность которой характеризуется показателем R. Предположим, что применительно к этой системе рассматриваются два варианта комплекса управления: вариант А и вариант В. В общем случае свойства комплекса управления суще-

ственно сказываются на эффективности системы. Поэтому при различных вариантах комплекса управления показатель эффективности R будет принимать различные значения. Пусть в случае варианта А его значение будет равно R_A, в случае варианта В — R_B. Тогда, для сравнительной оценки качества управления сложной СРК удобно использовать показатель: $\Delta R_{УПР} = R_A - R_B$. (3). При помощи величины $\Delta R_{УПР}$ можно произвести обследование некоторого числа вариантов управляющего комплекса СС и выбрать из них наилучший. Сравнительная оценка качества управления позволит выбрать лучший из некоторого числа вариантов управляющий комплекс.

Рассмотрим показатель сложности СРК. При проектировании сложных СРК часто осуществляется выбор одного из некоторого числа возможных вариантов систем РК. Естественно, что критерием для такого выбора в первую очередь служит значение показателя R эффективности (с учетом всех остальных, важных для данного класса систем, свойств: надежности, помехозащищенности). Однако если существуют варианты системы (два или более), эквивалентные с точки зрения их эффективности, преимущество обычно получает менее сложный из них.

Как было указано в [2] , сложность СРК можно оценить величиной:

$$S = (1 + \upsilon \cdot \alpha_{перв.}) \cdot \sum_{j=1}^{k} Y_j \cdot \sum_{l=1}^{n} A_{jl} \cdot (1 + \upsilon \cdot \alpha_{втор.}) \cdot \sum_{i=1}^{s} Y_i \cdot \sum_{d=1}^{m} A_{id} \ , \qquad (4)$$

где υ - коэффициент, учитывающий сложность связей системы в целом по сравнению со сложностью элементов и подсистем в отдельности.

Далее было получено выражение для оценки сложности системы с учетом фактического числа связей, реализованных в первичных и вторичных подсистемах РК:

$$S = \left(1 + \upsilon \cdot \frac{P^*}{n(n-1)}\right) \cdot \sum_{j=1}^{k} Y_j \cdot \sum_{l=1}^{n} A_{jl} \cdot \left(1 + \upsilon \cdot \frac{G^*}{m(m-1)}\right) \cdot \sum_{i=1}^{s} Y_i \cdot \sum_{d=1}^{m} A_{id} \ . \qquad (5)$$

Интуитивное представление о сложности системы связывает это ее свойство с объемом оборудования (число элементов, их вес, габариты и т. д.), разветвленностью связей между элементами и степенью их взаимодействия, квалификацией персонала, осуществляющего изготовление элементов, монтаж, наладку и эксплуатацию системы, стоимостью изготовления системы и удобством ее практического применения.

Однако в современных условиях развития техники одной интуиции недостаточно. Возникла необходимость в формальном понятии СС. Это важно с точки зрения исключения элементов субъективизма и получения по возможности более объективных оценок. Кроме того, без этого невозможен формальный синтез СС, интенсивно развивающийся в последние годы.

Выводы

Выбор числовых характеристик, зависящий от сложности СРК, позволяет описать ее основные свойства и определить показатели качества СРК. Проведенный теоретический анализ по показателям: эффективность, качество управления, оценка сложности, показывает, что качество работы сложной СРК необходимо оценивать при помощи этих показателей. Под показателями эффективности сложной СРК будет пониматься такая числовая характеристика системы, которая оценивает степень приспособленности СРК к выполнению поставленных задач.

Разработка методики оценки сложности СРК S, (4) и (5) представляет большой практический и теоретический интерес. Поэтому необходима проработка алгоритмов как оценки организационной структуры службы радиоконтроля, так и оценки аппаратурной составляющей элементов подсистем различных уровней, в том числе анализа состояний самих подсистем по отношению к общей СРК.

В процессе создания такой методики необходимо провести системный анализ существующих СРК, с учетом их декомпозиции на подсистемы, проанализировать недостатки и оценить накопленный положительный опыт.

Литература:

1. Бусленко Н.П., Калашников В.В., Коваленко И.Н. Лекции по теории сложных систем, Москва «Советское радио», 1973

2. Корниенко С.А. Применение системного анализа при оценке структурной сложности служб радиоконтроля, Научно-технический журнал «Информационные технологии моделирования и управления» №1(35), Воронеж, 2007 год

3. Корниенко С.А. Задача выбора не худшей системы радиоконтроля с использованием основных методов векторной оптимизации, Научно-технический журнал «Информационные технологии моделирования и управления» № Воронеж, 2008

ПОМЕХОУСТОЙЧИВОСТЬ СИСТЕМ ДКМВ СВЯЗИ С MIMO

Нечаев Ю.Б., Дворжакова И.О., Малютин А.А., Радько П.Н.
ОАО «Концерн «Созвездие», 394000, Воронеж, Плехановская, 14
Воронежский госуниверситет, 394000, Воронеж, Университетская пл., 1
E-mail:malyutin@nm.ru

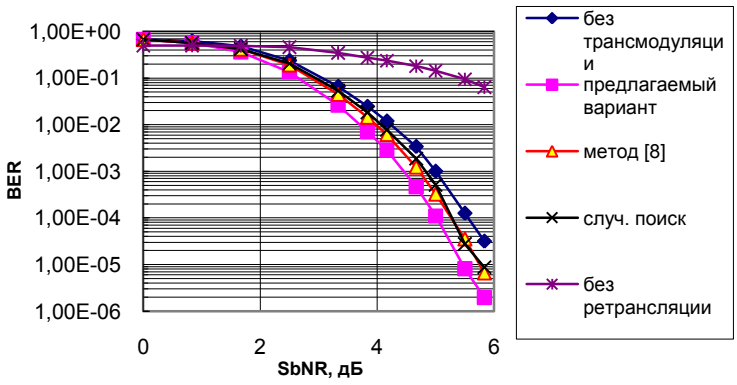
Simulations were made to compare interference immunity characteristics of manipulation codes which were set out in I part of the paper with both formally known codes and codes obtained using a random search algorithm. In this paper was analysed the influence of the characteristics of all three communication channels (source-retransmitter, source- receiver and retransmitter -receiver) on efficiency metrics of the systems using these introduced methods.

В [1], на основе генетического алгоритма двоичного переключения [2], был предложен новый метод построения сигнальных созвездий для систем связи, использующих методы кооперативного MIMO. В данной работе представлены полученные при помощи моделирования характеристики их помехоустойчивости и проанализировано влияние на них свойств всех трёх каналов связи образующих систему: источник – ретранслятор, источник – получатель и ретранслятор – получатель.

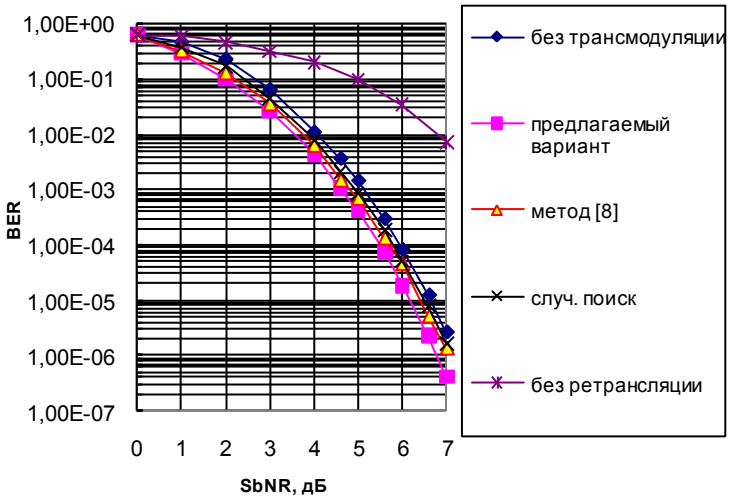
Моделирование работы системы связи, использующей полученные манипуляционные коды, проводилось в квазистационарном канале: параметры канала (отсчёты импульсной характеристики) задавались неизменными для одного OFDM символа (т.е. для одного блока из канальных символов) и изменялись независимым друг от друга случайным образом для следующего символа. Тактовая, цикловая и частотная синхронизация полагались идеальными.

Качество каналов связи источник – получатель и ретранслятор – получатель полагалось одинаковым, т.е. средние мощности сигналов источника и ретранслятора на входе приёмника получателя были равны. (Это равносильно ситуации, когда мощности передатчиков источника и ретранслятора равны, а потери распространения сигнала одинаковы, либо неравенство потерь компенсируется соответствующим неравенством мощностей). Замирания в них – независимы. Моделировалась работа системы связи с 32-мя поднесущими в ТЧ канале (300 – 3400 Гц). Объём статистики испытаний для оценки величины вероятности ошибок выбирался адаптивно исходя из обеспечения малой величины погрешности оценок: не менее 100 ошибок на выборку при оценке одной точки. Полученные результаты изображены на рис. 1. Графики соответствуют случаю безошибочного приёма сигнала ретранслятором.

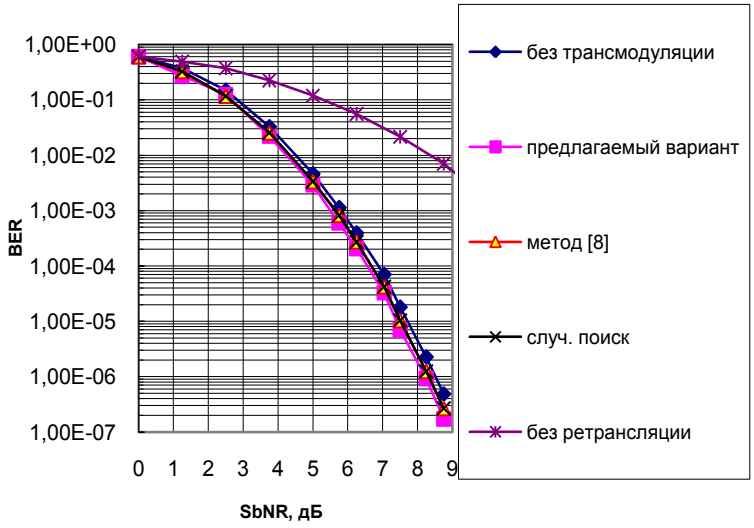
Помимо вышеупомянутого, на тех же реализациях замираний и помех проводилось моделирование работы следующих систем связи: 1) с манипуляционными кодами, полученными при помощи случайного поиска, 2) кодами, полученными по методу [4], 3) систем без трансмодуляции и 4) без ретрансляции. Результаты моделирования всех вышеперечисленных систем также изображены на рис. 1.



а)



б)



в)

Рис. 1. Характеристики помехоустойчивости системы связи, использующей предложенные манипуляционные коды, в сравнении с характеристиками систем с другими известными кодами, без трансмодуляции и без кодирования: а) BER для 64QAM, б) BER для 32QAM, в) BER для 16QAM.

Выводы

1. Результаты моделирования демонстрируют, что величина энергетического выигрыша по сравнению с системами, не использующими трансмодуляцию составляет около 4, 6 и 8 дБ соответственно для 16QAM, 32QAM и 64QAM созвездий, стандартно используемых в КВ модемах.

2. Величина энергетического выигрыша предложенных манипуляционных кодов по сравнению с манипуляционными кодами из [4] составляет около 3, 4, 6 дБ, а по сравне-

нию с манипуляционными кодами, полученными методом случайного поиска более 4, 5 и 6 дБ для 16QAM, 32QAM и 64QAM созвездий, соответственно.

3. Преимущество предложенного метода возрастает при увеличении кратности используемой модуляции.

Литература:

1. *Дворжакова И.О., Малютин А.А., Нечаев Ю.Б., Радько П.Н.* Построение сигнальных созвездий для систем ДКМВ связи с MIMO. Наст. сборник.

2. *Нечаев Ю.Б., Малютин А.А.* Манипуляционные коды для систем с итеративной обработкой принимаемого сигнала // Инфокоммуникационые технологии. – 2009. - № 1. – С. 7 - 17.

3. MIL-STD-188-110B, 27 APRIL 2000. Military Standard. .Interoperability and Performance Standards for Data Modems.

4. *K.J. Rayliy, A.K. Sadek, Weifeng Su, A. Kwasinski.* Cooperative Communications and Networking. Cambridge University Press, 2009, 627 p.

ПОСТРОЕНИЕ СИГНАЛЬНЫХ СОЗВЕЗДИЙ ДЛЯ СИСТЕМ ДКМВ СВЯЗИ С MIMO

Нечаев Ю.Б., Дворжакова И.О., Малютин А.А., Радько П.Н.
ОАО «Концерн «Созвездие», 394000, Воронеж, Плехановская, 14
Воронежский госуниверситет, 394000, Воронеж, Университетская пл., 1
E-mail:malyutin@nm.ru

This paper sets out a method for constructing manipulation codes for HF communication systems with retransmission using the concept of cooperative MIMO. This method is based on genetic algorithms for binary switching. With the help of this method we developed manipulation codes for constellation diagrams 16QAM, 32QAM and 64QAM, whose characteristics are the best or closest fit with strong probability.

В последнее время технологии кооперативного MIMO (Multiple-input multiple-output), получили широкое распространение и являются очень перспективной областью исследований, находя всё новые и новые сферы применения. Как известно, использование современных методов обработки сигнала (модуляции, кодирования и т.д.), рассчитанных на возможность одновременного использования нескольких приёмников и/или передатчиков, позволяет существенно повысить пропускную способность системы связи без увеличения мощности и расширения полосы частот, занимаемой сигналом. Особенно велик выигрыш в нестационарных, подверженных замираниям, каналах связи, каковыми, как правило, являются все КВ каналы. Собственно, разнесённый приём изначально считался одним из самых эффективных методов повышения помехоустойчивости и помехозащищённости систем КВ радиосвязи, в которых он впервые и стал использоваться. Однако в связи с бурным развитием беспроводных, сотовых, спутниковых систем связи технологии MIMO впервые стали применяться именно в последних, получивших массовое распространение системах коммерческой связи. И в настоящее время возможен процесс переноса и заимствования технических решений, первоначально предназначавшихся для использования в данных областях, в область технологий КВ связи. Разумеется, этот перенос не может быть чисто механическим, а должен учитывать специфику КВ диапазона: особенности распространения сигналов и помех в нём.

Непосредственное использование методов MIMO в «чистом» виде в КВ системах связи принципиально возможно, но часто затруднительно и не столь эффективно по причине необходимости больших геометрических размеров антенных систем для разнесённого приёма/передачи. Однако использование ретрансляторов в качестве виртуальных приёмных и передающих антенн открывает широкие перспективы для их применения.

При построении сети КВ связи необходимо учитывать особенности распространения сигнала в данном диапазоне в пределах обслуживаемой территории. Основной отличительной особенностью в данном случае является то, что прохождение сигнала, как правило, принципиально возможно между всеми узлами сети. Причём, географически более близко расположенные точки не обязательно имеют лучший канал связи друг с другом, чем расположенные на большем удалении.

Из этого следует, что на первый план при проектировании сети связи выходит задача разработки протоколов физического уровня, поддерживающих сетевые режимы работы, а не задача построения оптимальных протоколов сетевого уровня (маршрутизации и т.д.), как в сетях связи других частотных диапазонов. Т.е. при построении сети КВ связи должен учитываться тот факт, что все узлы сети способны обмениваться сообщениями между собой, а организация сетевого режима работы должна состоять в разработке протоколов работы аппаратуры физического и канального уровня, увеличивающих надёжность и другие качественные характеристики передачи сообщения за счёт использования совместных ресурсов сети. В частности, за счёт использования распределённого пространственно-временного кодирования, образования «виртуальных» (т.е. распределённых между абонентами сети) многоантенных систем приёма и передачи и т.д. Спецификой

построения сетевых режимов является учёт особенностей обработки сигнала на физическом уровне. Аналогично, выбор средств физического уровня (модуляции, кодирования и т.д.) производится с учётом сетевых возможностей.

Модель системы связи с ретрансляцией, использующей принципы кооперативного MIMO, изображена на рис 1. Её отличительной особенностью является возможность приёма и обработки получателем сообщения как сигнала от источника сообщения, так и сигнала, ретранслированного в промежуточном узле.

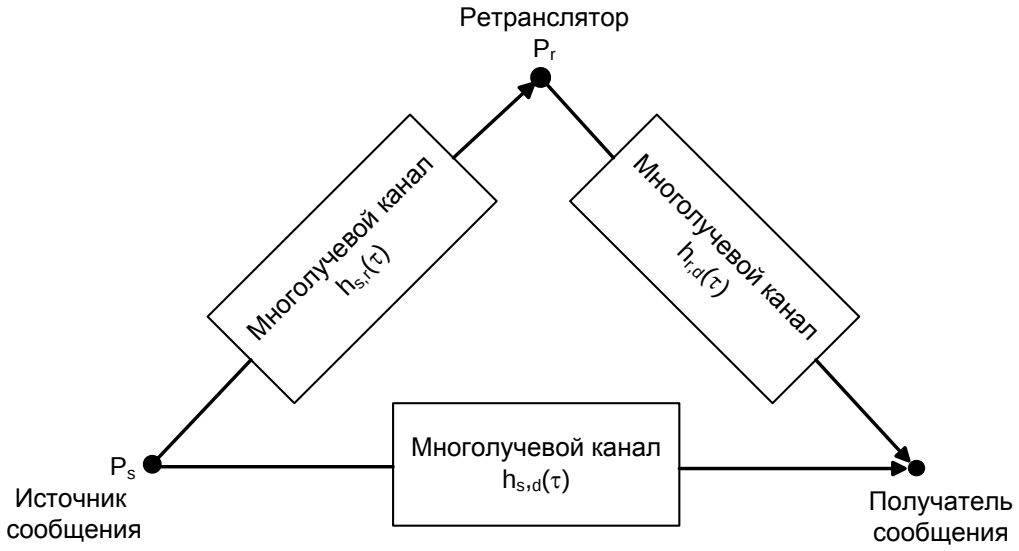


Рис.1. Модель системы связи с ретрансляцией, использующей принципы кооперативного MIMO

Одним из наиболее распространённых протоколов ретрансляции для кооперативного MIMO является протокол прямой ретрансляции (Decode-and-Forward - DF) [1]. Привлекательной особенностью данного протокола ретрансляции является простота реализации и малое время задержки. Что, наряду с достаточно хорошими характеристиками, делает его одним из наиболее вероятных претендентов на практическое применение [2].

Конкретно будем рассматривать адаптивный вариант данного протокола [2], в котором ретрансляция сообщения производится только при условии правильной демодуляции сигнала ретранслятором. Данный протокол может быть улучшен без усложнения процедуры обработки и без увеличения её длительности путём изменения вида манипуляционного кодирования в процессе ретрансляции путём т.н. трансмодуляции (transmodulation) или ремаппинга (remapping).

Этот метод был недавно предложен в [3] и развит в последующих работах. Однако предложенный в [3] метод построения кодов был получен из чисто интуитивных соображений, а разработанные на его основе коды применимы только к прямоугольным сигнальным созвездиям. В [4] предложен критерий построения оптимальных манипуляционных кодов. На его основе могут быть получены коды для созвездий не более чем с 8 точками. В то время как, для высокоскоростных частотно-эффективных систем связи КВ диапазона необходимо использование 16-, 32- и 64-х точечных созвездий сложной непрямоугольной формы.

Вот почему представляет интерес задача построения оптимальных (или близких к ним) манипуляционных кодов для сигнальных созвездий, стандартно используемых в КВ модемах передачи данных. Задача является особенно привлекательной, поскольку изменение вида манипуляционного кодирования, состоящее просто в перенумерации сигналь-

ных точек, позволяя добиться положительного эффекта, никак не усложняет процедуры обработки и не требует дополнительных ресурсов для реализации.

Кроме того, не тождественное манипуляционное кодирование источника сигнала и ретранслятора повышает скрытность системы связи, затрудняя обнаружение факта их совместной работы в составе одной сети.

Суть метода трансмодуляции состоит в увеличении Евклидова расстояния между принимаемыми получателем символами составного алфавита (т.е. символами, образующимися в результате наложения во времени символов источника сообщения и ретранслятора) путём изменения вида манипуляционного кода символов ретранслятором.

Будем рассматривать модемы, использующие для борьбы с многолучевым распространением сигнала в канале метод ортогонального частотного мультиплексирования (OFDM).

Критерием построения оптимального манипуляционного кода может служить минимизация символьной ошибки SER или двоичной ошибки BER.

Для небольших сигнальных созвездий возможен компьютерный перебор всех возможных вариантов перенумерации сигнальных точек с целью поиска наилучшего, минимизирующего соответствующую вероятность ошибки. Но для больших созвездий сложность такого подхода резко возрастает. Данная задача является разновидностью известной квадратической задачи о назначениях и в терминах теории алгоритмов является NP-трудной. Для неё могут быть предложены только эвристические алгоритмы, способные с той или иной вероятностью найти решение, близкое к наилучшему. С этой целью часто предлагаются для использования различные генетические алгоритмы. Вместо поиска точного решения, максимизирующего значение целевой функции они используют подходы, основанные на понятии «приемлемости решения» и строят алгоритмы, позволяющие это решение найти. Данные алгоритмы используют итеративные методы, последовательно отыскивая всё лучшие варианты решения, до достижения им приемлемого уровня качества или до тех пор, пока не будет исчерпан ресурс на объём вычислений. Основная проблема при построении такого рода алгоритмов – ложная сходимость к локальному (а не к глобальному) экстремуму целевой функции.

Для решения поставленной задачи будем использовать алгоритм эволюционно-генетического поиска (BSA). Данный алгоритм применялся в задачах неравномерного квантования и для выбора метода манипуляционного кодирования в [5]. В то же время этот метод является достаточно простым по структуре и экономичным с точки зрения вычислительных ресурсов. Считается, что он хорошо преодолевает проблему скатывания в область локальных экстремумов.

Алгоритм находит локальный минимум функции стоимости. Однако, если он выполняется несколько раз, проинициализированный случайным образом, то с большой вероятностью может быть найден глобальный минимум. Показателем качества решения может служить его относительная частота повторяемости при различных случайных инициализациях. Строгого доказательства оптимальности полученного решения нет.

При помощи разработанного подхода были найдены оптимизированные манипуляционные коды для сигнальных созвездий 16QAM, 32QAM и 64QAM для модемов КВ диапазона. Поиск проводился путём многократных независимых попыток использования процедуры BSA со случайной начальной инициализацией. Окончательно, выбирался результат с лучшими характеристиками.

Помимо алгоритма BSA, выбор наиболее подходящих вариантов проводился при помощи простого случайного поиска: путём выбора варианта с минимальным значением целевой функции при случайном выборе ξ, с ограничением на время выполнения вычислений. Последний путь, позволяя добиться характеристик выше средних, не приводил к столь хорошим результатам как BSA за точно такое же время вычислений. Так же был реализован т.н. «жадный» алгоритм, состоящий в попарной замене соответствия точек так, чтобы в результате значение целевой функции на данном шаге было бы минималь-

ным. Данный алгоритм имел склонность к скатыванию к локальному экстремуму и не давал больших преимуществ по сравнению со случайным поиском.

Выводы

1.На основе использования генетических алгоритмов разработан метод оптимизации вида манипуляционного кодирования для систем связи с кооперативным MIMO и трансмодуляцией. Достоинством метода, по сравнению с другими известными, является возможность построения кодов для многоточечных сигнальных созвездий сложной формы.

2.При помощи разработанного метода получены оптимизированные манипуляционные коды для сигнальных созвездий, стандартно используемых в КВ модемах передачи данных.

3.Анализ статистики повторяемости решений позволяет утверждать, что для 16QAM и 32QAM созвездий разработанные манипуляционные коды с высокой вероятностью обеспечивают наилучшие характеристики помехоустойчивости, а для созвездия 64QAM приводят к заметному их (характеристик) улучшению.

Литература:

1. *J. N. Laneman, D. N. C. Tse, and G. W.Wornell*, Cooperative diversity in wireless networks: Efficient protocols and outage behavior, IEEE Trans. Information Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

2. *J. N. Laneman and G. W. Wornell*, Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks, IEEE Trans. Information Theory, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

3. *K. G. Seddik, A. S. Ibrahim, and K. J. R. Liu*. Trans-modulation in wireless relay networks. IEEE Communications Letters, 121(3):170–172, March 2008

4. *K.J. Rayliy, A.K. Sadek, Weifeng Su, A. Kwasinski*. Cooperative Communications and Networking. Cambridge University Press, 2009, 627 p.

5. *Нечаев Ю.Б., Малютин А.А.* Манипуляционные коды для систем с итеративной обработкой принимаемого сигнала // Инфокоммуникационые технологии. – 2009. - № 1. – С. 7 - 17.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК ВОЗДЕЙСТВИЯ ПОМЕХ НА СИСТЕМЫ СИНХРОНИЗАЦИИ

Шахтарин Б.И., Асланов Т.Г.
Московский государственный технический университет им. Н.Э.Баумана.
107005. Москва, 2-я Бауманская 5. Тел: +7(926)4522222, E-mail: tabasik@gmail.com

Comparative analysis of the descriptions of the interferences on the timing systems

Comparative analysis of the descriptions of the interferences on the timing systems is given in the paper. Some results of probability density function (PDF) modeling of skip of phase lock (PhL) on different mathematical models are given by the author.

Последние десятилетия характерны широким применением систем синхронизации. Наибольшее распространение системы синхронизации нашли в радиотехнике, навигации-ии в следящих системах.

Все эти системы работают в условиях воздействия помех.

Помехи обуславливают случайный характер результатов синхронизации и поэтому, изучение этих процессов производится методами математической статистики.

Помехоустойчивости систем синхронизации посвящено много работ.

В связи с изложенным, представляет интерес сравнительный анализ характеристик воздействия помех на системы синхронизации, выполненный с использованием математических моделей, разработанных разными авторами.

Для удобства изложения, в начале, приведем таблицу соответствия обозначений, принятых у авторов (в Росси и США)

Таблица 1

№ п/п	Обозначение параметра		Наименование, назначение параметра
	Россия	США	
1	ν	β	
2	β	γ	Частотная расстройка
3	r	α	Отношение сигнал/шум (ОСШ) в полосе ФАП
4	ε	$\sqrt{R}$	Отношение помеха/сигнал
5	x_0= arcsin(β)	ψ_1	Состояние равновесия
6	x_1	c_1	Показатель помехи без расстройки
7	ρ	αM_0	Переходной процесс с помехой

По [1] справедливо разложение ПРВ $W(x)$ в ряд Фурье

$$W(x)=\frac{e^{\rho\cos x}}{2\pi R_\Sigma}\left[I_0(\rho)+2\bar{\nu}\sum_{n=1}^{\infty}\frac{(-1)^n}{n^2+\bar{\nu}^2}(\bar{\nu}\cos nx-n\sin nx)I_n(\rho)\right]. \qquad (1)$$

где: $I_0(\rho)$, $I_n(\rho)$ – модифицированные функции Бесселя,

В соответствии с [2] ПРВ в стационарном решении может быть записан как:

$$p(z)=\frac{1}{4\pi^2 e^{-\beta\pi}\left|I_{j\beta}(\alpha M_0)\right|^2}e^{\beta z+\alpha A_1\cos z-\alpha A_2\sin z}\int^{z+2\pi}e^{-[\beta y+\alpha A_1\cos y-\alpha A_2\sin y]}\,dy \qquad (2)$$

где: $I_{j\beta}$ - модифицированная функция Бесселя мнимого порядка

$$A_1=J_0(c_1)+\sqrt{R}J_1(c_1)\sin\psi_1;\quad A_2=\sqrt{R}J_1(c_1)\cos\psi_1;\quad M_0=\sqrt{A_1^2+A_2^2};$$

Особым случаем является отсутствие начальной расстройки.

В этом случае $\beta=\gamma=0$ и (2) преобразуется к виду:

$$p(z) = \frac{1}{4\pi^2 e^{-\beta\pi}\left|I_{j\beta}(\alpha M_0)\right|^2} e^{\alpha A_1 \cos z - \alpha A_2 \sin z} \int^{z+2\pi} e^{-[\alpha A_1 \cos y - \alpha A_2 \sin y]}\, dy \qquad (3)$$

где

$$\int^{z+2\pi} e^{-[\alpha A_1 \cos y - \alpha A_2 \sin y]}\, dy = \int^{z+2\pi} e^{-\alpha M_0 \sin(y+P_0)}\, dy = 2\pi I_0(\alpha M_0) \qquad (4)$$

тогда ПРВ в стационарном режиме имеет вид:

$$p(z) = \frac{1}{2\pi I_0(\alpha M_0)} e^{\alpha A_1 \cos z - \alpha A_2 \sin z} \qquad (5)$$

$$p(z) = \frac{1}{2\pi I_0(\alpha)} e^{\alpha \cos z} \qquad (6)$$

В отсутствии помехи $z(t) = \phi(t)$ получим известный результат:

$$p(\phi) = \frac{1}{2\pi I_0(\alpha)} e^{\alpha \cos \phi} \qquad (7)$$

Для сравнительного анализа ПРВ, рассчитанных по уравнениям (1). (3), (5) и (7) произведено моделирование в MatLabe.

На рис. 1 приведены ПРВ срыва синхронизации ФАП рассчитанные: кривая 1- по выражению (3), кривая 2 - по выражению (1).

Расчет произведен при ОСШ *(r)*, равном 2. Кривая 3 рассчитана по выражению (5), исключением из рассмотрения в выражении (3) начальной расстройки *ε*. Кривая 4 рассчитана по уравнению Тихонова В.И. (7).

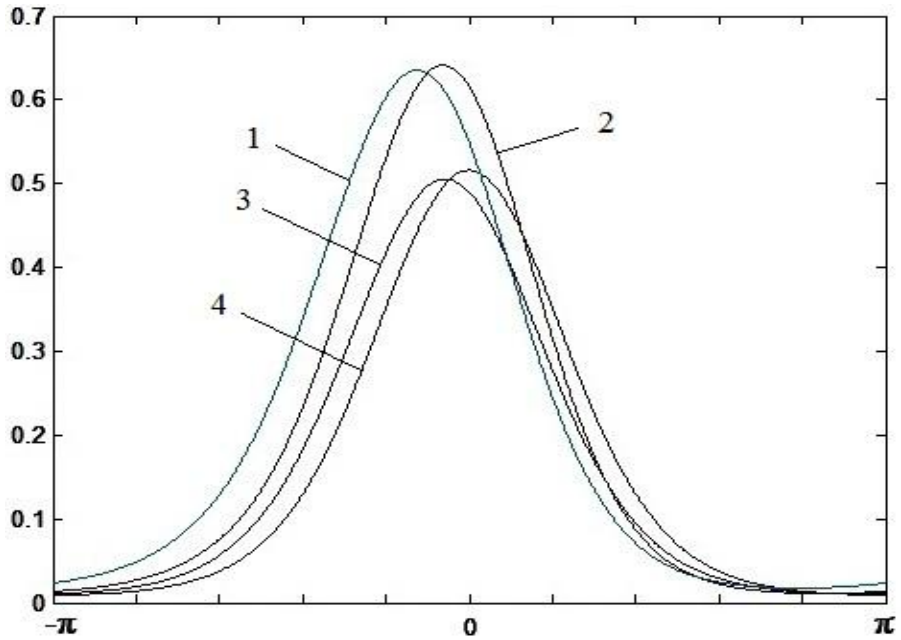


Рис. 1. Расчет ПРВ по выражениям (1), (3), (5) и (7) с учетом начальной расстройки *ε=0.8* и без него. *r = 2*.

Из сравнения кривых видно, что дисперсия и второй центральный момент ПРВ по выражениям (1) и (7) меньше, чем по выражению (3). В то же время, при идентичных условиях фазовая расстройка ПРВ по выражению (3) выше, чем по выражению (1)

На рис. 2 приведена ПРВ срыва синхронизации ФАП при ОСШ *(r)* равном 1.5, *ε=0.8*. Кривая 1 рассчитана по выражению (3) , кривая 2 по - (1)

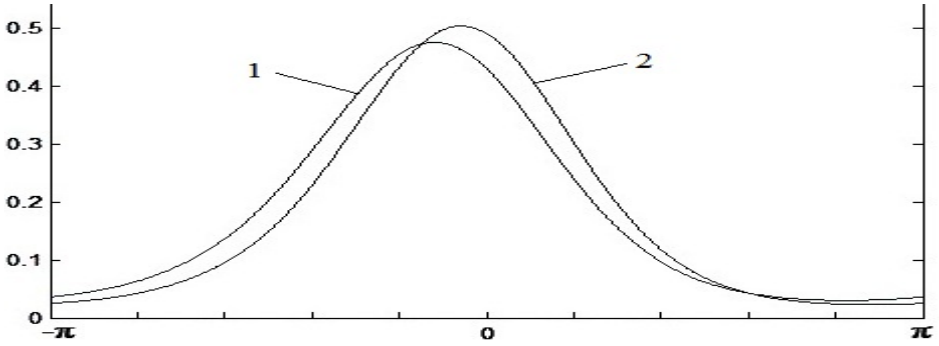


Рис. 2. Расчет ПРВ по (1) и (3) с учетом начальной расстройки $\varepsilon=0.8$. $r = 1.5$.

На рис. 3 приведена ПРВ срыва синхронизации ФАП при ОСШ *(r)* равном 1, $\varepsilon=0.8$. Кривая 1 рассчитана по выражению (3) , кривая 2 по - (1)

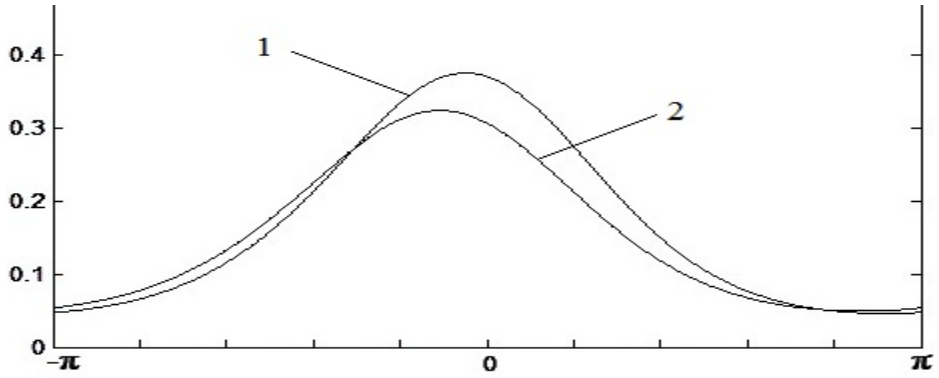


Рис.3. Расчет ПРВ по (1) и (3) с учетом начальной расстройки $\varepsilon=0.8$. $r = 1$.

Выводы, сделанные по рис. 1 справедливы и для рис. 2 и 3.

На рисунках 4, 5, 6, приведены ПРВ соответствующие рис. 1, 2 и .3, при отсутствии начальной расстройки.

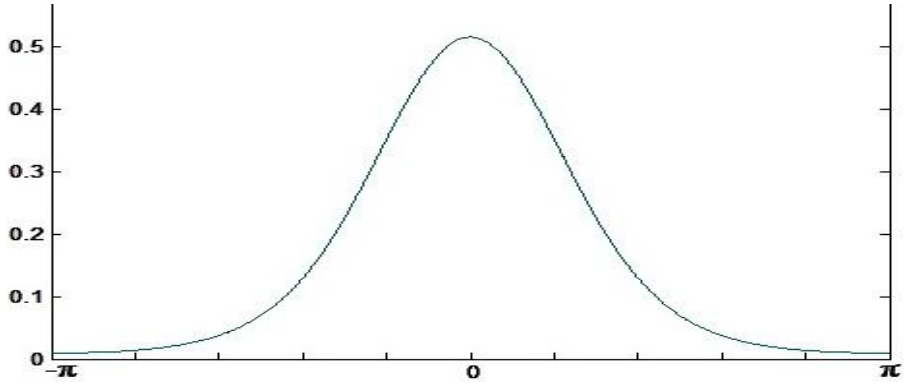


Рис. 4. Расчет ПРВ по (1) и (3) при отсутствии начальной расстройки. $r = 2$.

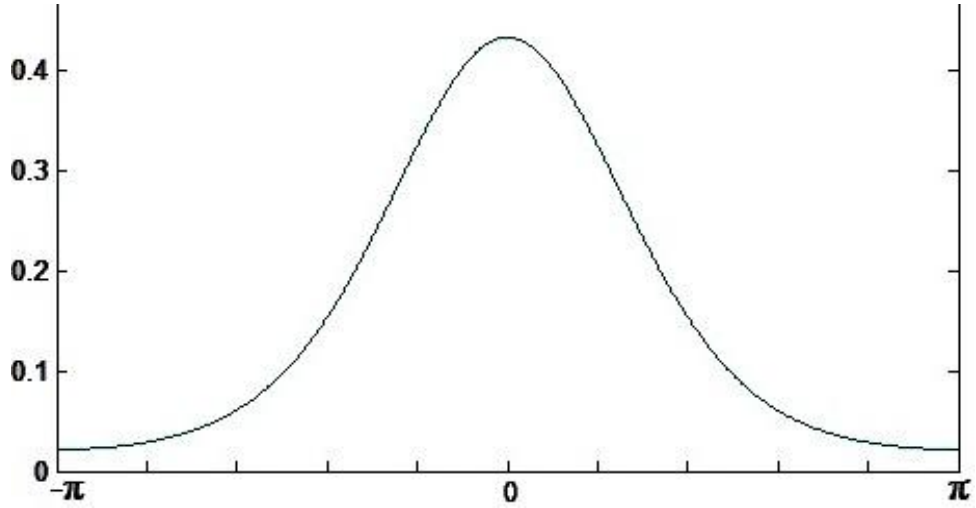


Рис. 5. Расчет ПРВ по (1) и (3) при отсутствии начальной расстройки. *r = 1.5.*

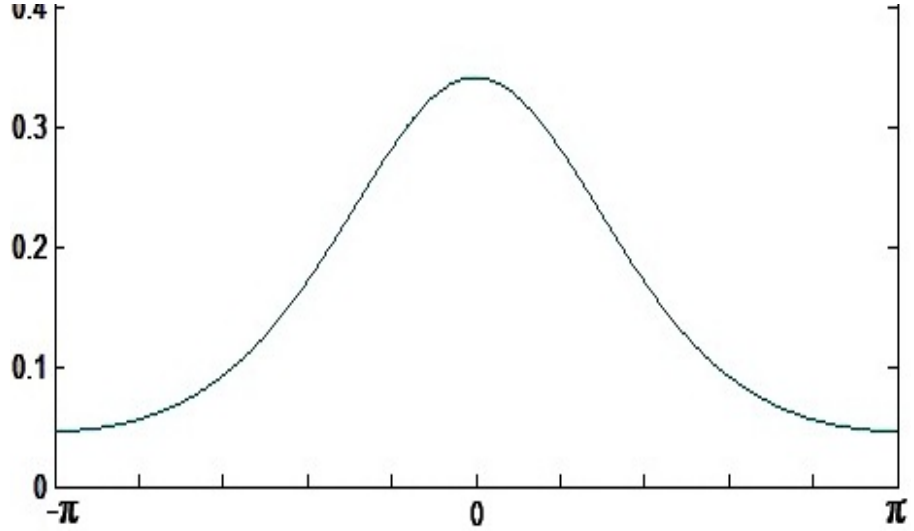


Рис. 6. Расчет ПРВ по (1) и (3) при отсутствии начальной расстройки. *r = 1.*

Анализ рисунков 4, 5, 6 показывает, что при отсутствии начальной расстройки, ПРВ, рассчитанные по выражениям (1), (3), (5) и (7) идеально накладываются друг на друга.

Таким образом, моделированием ПРВ срыва синхронизации ФАП по математическим моделям (1), (3), (5) и (7) показала, что дисперсия и второй центральный момент ПРВ по (1) и (7) меньше, соответственно чем по (3) и (5). В то же время, при идентичных условиях фазовая расстройка ПРВ по (3) и (5) выше, чем по (1) и (7).

Литература:

1. *Шахтарин Б.И.* Статистическая динамика систем синхронизации. М.: Радио и связь, 1998. – 488 с.

2. http://www.tosiacomm.com/Murat F. Karsi IEEE Paper.pdf

МНОГОЛУЧЕВОСТЬ В ЗЕРКАЛЬНЫХ РАДИОТЕЛЕСКОПАХ: ЧУВСТВИТЕЛЬНОСТЬ В ШИРОКОМ ПОЛЕ ОБЗОРА

Юпиков О.А.
Севастопольский национальный технический университет
99053, Севастополь, ул. Университетская 33, каф. радиотехники и телекоммуникаций
E-mail: lichne@gmail.com; тел. (050) 591-60-15

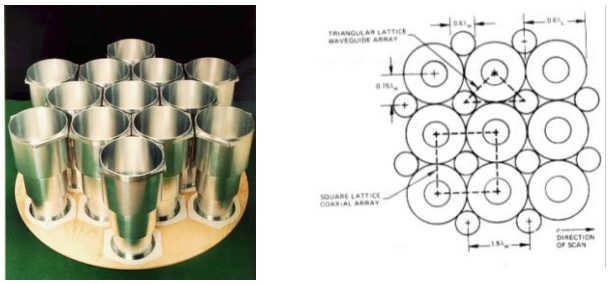
The given work is devoted to the modern developments in the field of radio astronomy instrumentation. In particular, the sensitivity of the multi-beam reflector radio telescope which is fed by phased array (PAF) is considered. Using PAF as reflector feed allows obtaining wide and continuous field of view (FOV) of the telescope. This has several advantages with compare to horn-cluster feeds which are described in this work. The sensitivity inside whole FOV was computed using three different beamforming schemes.

Введение

Традиционно в качестве облучателей зеркал рефлекторных антенн используются рупора, как правило, гофрированные. Однако, основная проблема современных радиотелескопов-интерферометров с рупорами — низкая скорость обзора неба. Чтобы получить максимальную разрешающую способность интерферометра, один цикл измерений длится 12 часов (пока Земля совершит пол оборота вокруг своей оси, т.о. получив самую длинную базу). За этот цикл просматривается только участок неба площадью равной площади поля обзора антенны. Так, например, у Вестерборгского радиотелескопа (*WSRT*, Нидерланды) ширина диаграммы направленности (ДН) на частоте 1,42 ГГц равна примерно 0,5 градуса. Несложно подсчитать, что при такой ширине ДН построение карты полной небесной сферы (площадью 4π кв. радиан) займет около 140 лет. На более высоких частотах это время будет еще больше.

Одним из способов увеличения скорости обзора неба является применение в качестве облучателей групп, или кластеров, рупоров в конфигурации «один рупор – один луч». Это позволяет одновременно проводить наблюдения нескольких участков неба. Были предложены различные варианты. Некоторые из них показаны на рис. 1 [1].

Однако, хотя использование кластеров из рупорных облучателей в конфигурации «один рупор – один луч» дает выигрыш в скорости обзора неба, оно имеет существенные недостатки: узкая рабочая полоса частот (для рупоров в составе кластеров она не превышает 30%) и низкая чувствительность в точках пересечения соседних лучей [1], из-за чего требуется несколько позиционирований зеркала, чтобы покрыть поле обзора.



а) б)

Рис. 1. Рупорные кластеры:
а) облучатель для *Parkes Radio Telescope*, ($\Delta f/f = 0{,}16$); б) концепция двухполосного кластерного облучателя

Покрыть все поле обзора за одно позиционирование зеркала можно с использованием плотных антенных фокальных решеток (АФР), так как она позволяет формировать хорошо перекрываемые лучи (уровень в точках пересечения соседних лучей уменьшается не более чем на 3 дБ). Под понятием «плотная» антенная решетка понимается решетка с расстоянием между ее элементами на верхней частоте рабочего диапазона менее λ для рефлекторов с $F/D>1$ и менее 0,6λ для рефлекторов с $F/D<0{,}5$ [2]. Это необходимо, чтобы полностью семплировать поле в фокальной области.

АФР исследуются уже давно, начиная с 70х годов. Теоретически рассматривались такие вопросы, как оптимальное расстояние между элементами решетки и оптимальное отношение F/D зеркала, КИП, составляющие шумовой температуры системы, общие выражения для максимизации чувствительности системы с АФР, взаимное влияние элементов решетки друг на друга и вклад в шумовую температуру системы за счет этого, влияние искажения поверхности зеркала на параметры системы и другие вопросы. Однако анализа всей *многолучевой* системы в комплексе еще не было выполнено.

В настоящей работе приведенные выше результаты теоретических исследований объединяются в единую модель рефлекторной антенной системы с фокальной решеткой, и с помощью этой модели проводится анализ прототипа многолучевой системы *APERTIF* [3]. В докладе приводятся некоторые полученные результаты.

Основная часть

На рис. 2 показана функциональная схема анализируемой антенной системы. Она состоит из: 1) рефлектора, 2) плотной многоэлементной антенной решетки с устройством питания ее элементов, 3) малошумящих усилителей (МШУ), 4) цифрового формирователя ДН. С выхода каждого элемента решетки выходят как сигнал e_m, так и шум c_m.

В рассмотренной антенной системе формирователем одновременно формируются 37 лучей гексагональном в поле обзора площадью 8 кв. градусов (рис. 3). Окружностями показаны сечения лучей на уровне –3 дБ. Уровень –3 дБ задан в первом приближении, и может меняться в процессе оптимизации непрерывности поля обзора

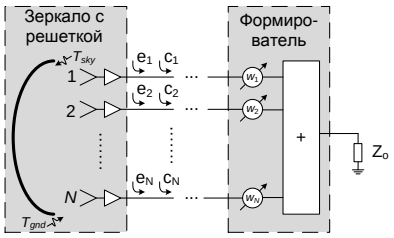


Рис. 2. Функциональная схема антенной системы

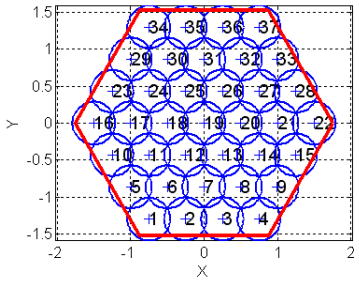


Рис. 3. Конфигурация лучей в поле обзора

Были рассмотрены три схемы формирования лучей: 1) метод согласования по полю [4]; 2) метод максимизации чувствительности [5]; 3) метод максимизации чувствительности с ограничениями по направлениям, известный также как *Linear Constrained Minimum Variance* (*LCMV*) [6].

Метод согласования по полю (*CFM – conjugate field matching*) — самый простой способ вычисления весовых коэффициентов для формирователя, при котором антенная система принимает максимум падающей на нее энергии, то есть ведется согласованный прием. Весовые коэффициенты $\mathbf{w_{opt}}$ в этом методе равны комплексно-сопряженной величине сигнала на выходе соответствующих элементов решетки при приеме сигнала от источника в заданном направлении, то есть

$$\mathbf{w_{opt}} = \mathbf{e}^{*}\left(\theta_0, \varphi_0\right), \tag{1}$$

где $\mathbf{w_{opt}} = \left[w_1,\ w_2,\ \ldots,\ w_M\right]^T$ — весовые коэффициенты для приема падающей волны с заданной поляризацией; $\left(\theta_0, \varphi_0\right)$ — направление требуемого максимума ДН системы; $\mathbf{e}\left(\theta_0, \varphi_0\right)$— сигнальный вектор при приеме падающей волны с направления $\left(\theta_0, \varphi_0\right)$.

Здесь и далее под сигнальным вектором **e** понимается набор значений выходного сигнала с каждого элемента решетки (канала приема), то есть $\mathbf{e} = [e_1, e_2, \ldots, e_M]^{\mathrm{T}}$, где M — количество антенных элементов в решетке, верхний индекс T означает транспонирование.

Метод максимизации чувствительности (*MaxSNR*). Оптимальные по критерию максимальной чувствительности весовые коэффициенты рассчитываются в соответствии со следующим выражением:

$$\mathbf{w_{opt}} = \mathbf{C}^{-1}\mathbf{e}(\theta_0, \varphi_0), \tag{2}$$

где **C** — шумовая корреляционная матрица.

Элементы матрицы **C** являются коэффициентами корреляции между напряжениями на портах соответствующей пары элементов решетки как при приеме шумов окружения, так и учитывая внутренние шумы антенной системы и взаимную связь между элементами решетки. Более подробно о расчете этой матрицы см., например, [7].

Метод максимизации чувствительности с ограничениями по направлениям *(LCMV).* По данному методу формирования лучей весовые коэффициенты для формирователя рассчитываются следующим образом:

$$\left(\mathbf{w_{opt}}\right)^{\mathrm{H}} = \mathbf{g}^{\mathrm{H}}\left[\mathbf{G}^{\mathrm{H}}\mathbf{C}^{-1}\mathbf{G}\right]^{-1}\mathbf{G}^{\mathrm{H}}\mathbf{C}^{-1}, \tag{3}$$

где **G** — матрица размером MxN_{dir}, содержащая сигнальные вектора с N_{dir} направлений ограничений (M — количество элементов в решетке); **g** —вектор размерностью N_{dir}x1, элементы которого устанавливают уровень ДН луча в каждом из N_{dir} направлений. Направления ограничений были выбраны в точках пересечения лучей.

Моделирование антенной системы.

На рис. 4 и 5 показаны фото и электродинамическая модель АФР.

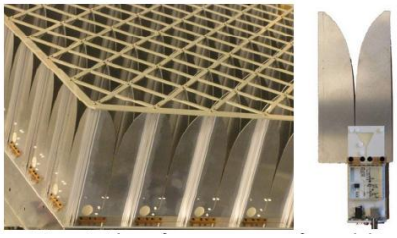


Рис. 4. Фото антенной решетки, установленной в фокусе *WSRT*, и один ее элемент

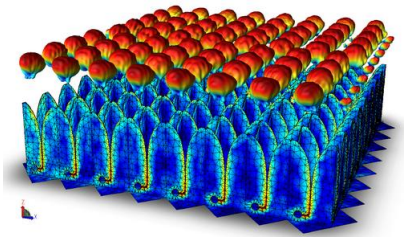


Рис. 5. Распределение токов в антенной решетке и ДН ее отдельных элементов

Используя созданную модель, были рассчитаны такие параметры радиотелескопа, как: а) весовые коэффициенты для элементов решетки; б) первичные и вторичные ДН для некоторых лучей; в) коэффициенты эффективности системы (КИП, коэффициент перехвата, коэффициенты амплитудного и фазового распределений в апертуре зеркала); г) шумовая температура и ее составляющие; д) КНД системы; е) чувствительность системы для нескольких лучей в поле обзора. Чувствительность в многолучевом поле обзора для трех рассмотренных схем формирования лучей, а также зависимость ее неравномерности от частоты показаны на рис. 6 и 7 соответственно.

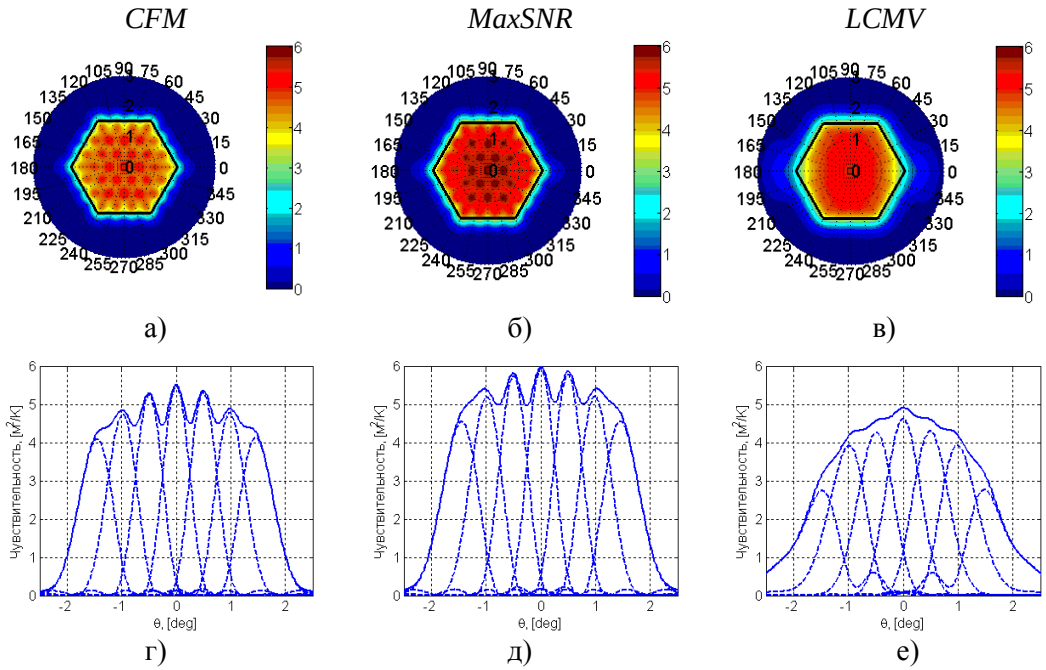


Рис. 6. Чувствительность в поле обзора антенной системы для трех схем формирования лучей

Выводы

Анализируя результаты, показанные на рис. 6 и 7, можно сделать следующие выводы.

1) схема *CFM* не дает максимальной чувствительности системы, хотя КНД при ней максимален, и обладает существенной неравномерностью в поле обзора, поэтому целесообразно применять другие схемы формирования лучей;

2) схема *LCMV* позволяет достичь компромисса между чувствительностью системы и ее неравномерностью внутри поля обзора;

3) при использовании схемы *LCMV* чувствительность быстро падает при увеличении угла сканирования из-за искажения формы луча.

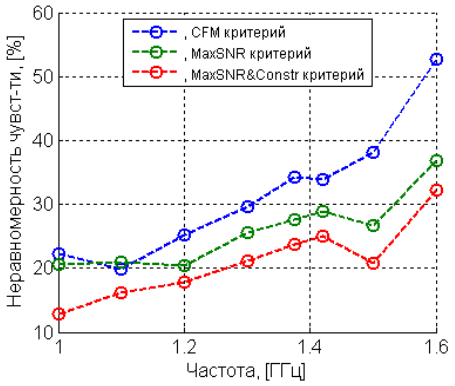


Рис. 7. Зависимость неравномерности чувствительности от частоты для трех схем формирования лучей

Литература:

1. Veidt B. SKA memo 71: Focal-Plane Array Architectures: Horn Clusters vs. Phased-Array Techniques [электронный ресурс] / Режим доступа: http://www.skatelescope.org/uploaded/29162_71_Veidt.pdf

2. Ivashina M. V. Optimal number of elements and element spacing of wide-band focal plane arrays for a new generation radio telescope / M. V. Ivashina, M. Ng Mou Kehn and P.-S. Kildal // *Proc. of EuCAP2007.* — November 2007. — P. 1—6.

3. W. van Cappellen APERTIF: Phased Array Feeds for the Westerbork Synthesis Radio Telescope / W. van Cappellen, L. Bakker // Proc. of IEEE Int. Symp. on Phased Array Systems and Technology. — 12-15 October, 2010. — P. 1—5

4. Lo Y.T. Optimization of directivity and signal-to-noise ratio of an arbitrary antenna array / Y.T. Lo, S.W. Lee // IEEE Trans. — Aug., 1966. — Vol.54, No.8. — P. 1033— 1045.

5. Wood P. J. Reflector antenna analysis and design / P.J.Wood. — IEE, Peter Peregrinus LTD, New York, 1980.

6. Van Trees Harry L. Detection, Estimation and Modulation Theory, Part IV, Optimum Array Processing / Harry L. Van Trees. — Wiley-Interscience, 2002. — 1456 p.

7. Maaskant R. Analysis of large antenna systems: Ph.D. dissertation: 07.06.2010 / Maaskant Rob. — Eindhoven Univ. of Technology, The Netherlands, June 2010. — 274 p. (http://alexandria.tue.nl/extra2/201010409.pdf)

МЕТОДЫ АНАЛИЗА OFDM СИГНАЛОВ В СИСТЕМАХ АВТОМАТИЧЕСКОГО РАДИОМОНИТОРИНГА

Белокуров А.А., Вотяков О.И., Кузниченко В.С., Петров В.Л., Писаренок Г.Г.
Центральное казенное конструкторское бюро „Протон”
61001, Харьков, пл. Восстания, 7/8, тел. (057) 732-15-48

Offered the aproximate method estimations to accuracy of the determination temporary parameter OFDM signal, founded on their correlation analysis with provision for characteristic cyclic prefix structure. The Aproximation of the spectrum OFDM signal in frequency area limited on frequency by white noise has allowed to find root-mean-square mistake of the estimation of the temporary interval to orthogonality. The Way to linearizations to dependencies of the interval to orthogonality and values of the carrying frequencies is received expression for root-mean-square mistake of the estimation of the value of the carrying frequencies.

Постановка проблемы. Построение эффективных систем передачи информации в настоящее время неразрывно связано с проблемой интенсификации использования временного и частотно-энергетического ресурса физических каналов связи. Одним из направлений решения этой проблемы является применение сложных сигналов с комбинированными видами модуляции в сочетании с методами сужения спектра и помехоустойчивым кодированием [1,2]. В последнее время интенсивно используются сигналы OFDM (Orthogonal Frequency Division Multiplexing). Сложность структуры таких сигналов является причиной существенных затруднений при решении задач радиомониторинга. Поэтому совершенствование методов автоматического цифрового анализа многочастотных многофазных сигналов является весьма актуальной задачей.

Традиционным методом первичного выявления параметров контролируемых сигналов в настоящее время является их анализ на основе алгоритмов быстрого преобразования Фурье (БПФ). Использование алгоритмов БПФ для обработки OFDM сигнала предполагает наличие точной информации на приемной стороне о ряде параметров сигнала: количестве уровней квантования, частоте дискретизации, величине тактового интервала и длительности префикса. При решении задач радиомониторинга эти данные, как правило, неизвестны. В связи с этим, развитие программно-аппаратных средств цифровой обработки сигналов, ориентированных только на использование алгоритмов БПФ не всегда является оправданным.

Целью исследования является определение путей цифрового анализа первичных параметров OFDM сигналов в системах автоматического радиомониторинга, определение этапов обработки.

Основная часть. В математической модели основными структурными временными параметрами OFDM сигналов, открывающими доступ к дальнейшему анализу всех идентифицирующих признаков, являются значения продолжительности интервала модуляции T_p и интервала ортогональности T.

Точное определение временных параметров через характеристики спектра в условиях множества несущих, многократно модулированных по фазе, даже при очень большой частоте дискретизации обречено на неудачу.

Для анализа OFDM сигналов могут быть предложены два подхода. К первому отнесем методы оценивания сигналов неизвестной структуры [3]. Под структурными параметрами модели будем понимать ее размерность - целочисленный параметр числа поднесущих частот n, значения продолжительности интервала модуляции T_p и интервала ортогональности T.

Существенной особенностью рассматриваемой модели является необходимость оценивания целочисленного параметра числа поднесущих частот, по которому нельзя дифференцировать функцию плотности вероятности и поэтому, традиционные методы оценивания неприменимы.

В этой ситуации могут быть использованы модификации метода максимального правдоподобия для случая неизвестной размерности модели. Одной из таких модификаций является информационный критерий Акаике (ИКА) [3]. Таким образом, задача идентификации сводится к заданию множества допустимых моделей и множества допустимых времен начала регистрации интервалов модуляции и оцениванию параметров каждой модели методом максимального правдоподобия с последующим выбором модели, обладающей минимальным значением ИКА.

Информационный критерий Акаике представляет собой аддитивную поправку к условной функции правдоподобия, зависящую от размерности модели. Для предложенной модели она имеет вид

$$\text{ИКА}[n,A(n)]=-\ln f(Q/n,A(n))+n, \quad (1)$$

где f(Q/n,A(n))- функция правдоподобия для реализации Q при фиксированной структуре модели (n),

$A(n)=[T,\ T_p, \Delta f, \vec{F}\,]$ - искомая совокупность оцениваемых вторичных параметров для фиксированного набора первичных параметров (n),

$\vec{F}=\{f_1,\ldots,f_n\}$ - вектор номиналов поднесущих частот.

Процедура минимизации ИКА заключается в нахождении оценок максимального правдоподобия для каждого набора первичных параметров (n) с последующим выбором набора (n), обеспечивающего минимальное значение ИКА в заданном интервале. Алгоритм работает следующим образом: для каждого значения размерности модели n и для заданных временных интервалов "запускается" алгоритм оценивания параметров модели методом максимального правдоподобия, при этом не только оценивается набор параметров A(n) для данной размерности n, но и фиксируется достигнутое значение логарифмической функции правдоподобия ln f(Q/n,A(n)).

Рассмотренный подход требует чрезвычайно больших вычислительных ресурсов, возрастающих в геометрической прогрессии с возрастанием числа и возможных значений переменных. Поэтому его реализация в реальном масштабе времени в системах автоматического радиомониторинга является весьма проблематичной.

Ко второму подходу отнесем методы поэтапной обработки, когда на каждом из этапов определяется часть параметров, а не вся их совокупность.

Учитывая тот факт, что OFDM сигналы содержат префикс, на первом этапе целесообразно использовать корреляционный метод определения структурных временных параметров T_p и T, в основу которого положен принцип «скользящего» временного окна.

Для проведения корреляционного анализа формируются два временных окна наблюдения сигнала и содержащие по K неперекрывающихся элементов массива $Q:\overrightarrow{Y0}=\{q_j,q_{j+1},\ldots q_{j+K-1}\}$, $\overrightarrow{Y1}=\{q_{j+i+K},q_{j+i+K+1},\ldots q_{j+i+2K-1}\}$, отстоящих на величину L.

Определение структурных временных параметров осуществляется на основе расчета нормализованной функции взаимной корреляции сигнала в окнах:

$$M(d,L)=\frac{\sum_{m=d}^{d+K-1} q(m)\cdot q(m+L)}{\sum_{m=d}^{d+K-1}\left|q(m)^2\right|\cdot\sum_{m=d}^{d+K-1}\left|q(m+L)^2\right|}. \quad (2)$$

Оценка величин *d* и *L* осуществляется по формуле:

$$\hat{d},\hat{L}=\arg\max_{d,L} M(d,L). \quad (3)$$

Решение задачи дает возможность определить с ошибкой, не превышающей величину интервала дискретизации параметры OFDM сигнала: величину интервала ортого-

нальности, длительность интервала модуляции и значение Δf разноса частот между каналами.

Найденные частотно-временные параметры сигнала являются основой для решения следующих задач: тактовой (временной синхронизации); частотной синхронизации; определения количества и значений частот информационных (допплеровских, синхронизации) каналов; демодуляции сигнала (расчет фазы и амплитуды сигнала на тактовых интервалах); определения количества позиций фаз информационных каналов; расчета значения отношения сигнал/шум.

Временная синхронизация заключается в корректном определении позиций элементов из массива Q, соответствующих началу каждого тактового интервала (интервала модуляции). Начало тактового интервала правильнее всего положить связанным с началом серии максимальных откликов коррелятора (2,3).

С учетом этого может быть определено максимальное число колебаний в полосе $F_{эф}$ может быть разложено по двум квадратурным компонентам [4,5,6,7]. Учитывая, что поднесущие частоты могут принимать значения, начиная от $f_н$ с шагом Δf, нахождение амплитуд квадратур проще и надежнее всего организовать при помощи решения системы линейных алгебраических уравнений (СЛАУ). Преимущество использования метода линейной алгебры по сравнению с традиционными спектральными методами состоит в том, что вычислительная сложность решения СЛАУ (например, методом Гаусса) не превышает вычислительной сложности быстрого преобразования Фурье. Для нахождения вектора номиналов работающих частот $\vec{F} = \left\{ f_1, \ldots, f_{n_p} \right\}$ можно использовать различные способы составления и решения СЛАУ.

На следующем этапе применение аппарата СЛАУ позволит осуществить демодуляцию сигнала в каждом из предполагаемых частотных каналов. Оценка уровня сигнала в каждом канале и расчет «фазового созвездия» будут основой для принятия решения о количестве информационных каналов (допплеровских, синхронизации), определения значений частот этих каналов.

Таким образом, полученные параметры на основе обработки цифровых выборок дают возможность полностью идентифицировать структуру OFDM сигнала.

На рис.1 представлены результаты расчета зависимости среднеквадратической ошибки оценки временного интервала ортогональности Т $\sigma_{\Delta t} / t_д$ от отношения E_b / N_0 (энергии одного бита к плотности мощности шума) при частоте дискретизации $f_д$=8000Гц ($t_д = 1.25 \times 10^{-4}$ с), для трех OFDM сигналов (n=12, Δf=200Гц; n=60, Δf=44.44Гц; n=45, Δf=62,5Гц). Анализ показывает, что среднеквадратическая ошибка определения временных параметров OFDM сигналов (длительность интервала ортогональности) при отношении сигнал/шум 0…10 дБ имеет порядок половины величины интервала дискретизации. Это говорит о том, что корреляционный метод обеспечивает довольно высокую точность определения временных параметров даже в зашумленных выборках.

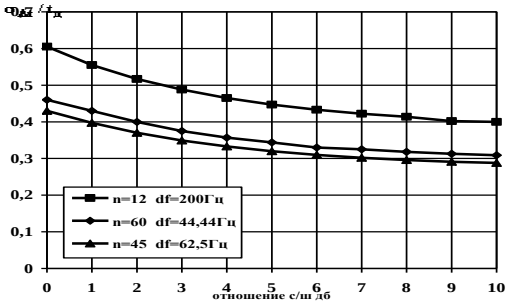


Рис.1. Зависимость $\sigma_{\Delta t} / t_д$ от отношения E_b / N_0 в дБ

На рис.2 представлены результаты расчета зависимости среднеквадратической ошибки оценки разноса частот между поднесущими $\sigma_{\Delta f}$ (Гц) от отношения E_b / N_0 при частоте дискретизации $f_д$=8000Гц ($t_д = 1.25\times10^{-4}$ с), для трех OFDM сигналов (n=12, Δf=200Гц; n=60, Δf=44.44Гц; n=45, Δf=62,5Гц).

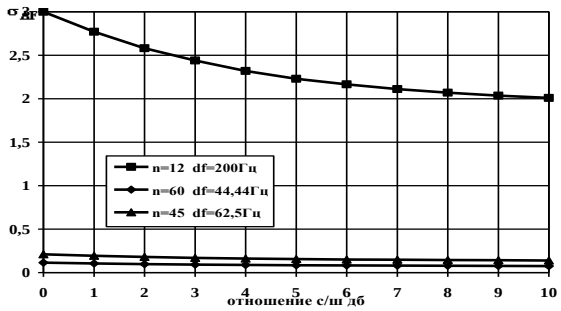


Рис.2. Зависимость $\sigma_{\Delta F}$ (Гц) от отношения E_b / N_0 в дБ

Анализ показывает, что среднеквадратическая ошибка определения величины разноса частот $\sigma_{\Delta F}$ при отношении сигнал/шум 0…10дБ для OFDM сигналов с n=12 не превосходит 3Гц, а для сигналов с n=45 и n=60 не больше 0.25Гц. При отношении сигнал/шум 5дБ и больше результаты проведенного статистического моделирования с точностью до 5% совпадают с теоретическими.

Выводы. Основной результат исследований заключается в получении универсального метода комплексного анализа структурных параметров OFDM сигналов. В отличие от известных спектральных методов предложено использование корреляционных свойств префиксной структуры многочастотных сигналов и помехоустойчивых решений переопределенных систем уравнений. Этот подход позволил добиться полной структурной идентификации сигнала в условиях обширной неопределенности и цифровой выборки минимального объема и весьма невысокого качества. Фактически, становится возможной помехоустойчивая демодуляция сигналов в цифровой форме при предельно низкой частоте дискретизации и малом разрешении квантователей.

Литература:

1. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра: Пер. с англ. / Под рад. В. И. Журавлева. − М.: Радио и связь, 2000. − 520 с.

2. Тихонов В. И. Оптимальный прием сигналов.− М.: Радио и связь, 1983.− 320 с.

3. Воробьёв С.А. Моделирование и структурный анализ сигналов с повторяющимися признаками формы в медико-биологическом эксперименте. Автореферат дис. докт.техн.наук .- http://vorobei.narod.ru

4. Белокуров А.А., Кузниченко В.С., Рассомахин С.Г. Принципы и подходы к анализу параметров OFDM сигналов в системах автоматического радиомониторинга // Системи обробки інформації. – Х.: ХУПС, 2010. – Вип. 6 (87). – С. 55-59.

5. Кузниченко В.С. Цифровой корреляционный метод анализа OFDM сигналов в системах автоматического радиомониторинга.//Системи управління, навігації та зв'язку. – К.:ЦНДІ НіУ, 2010, вип.4(16).- С.256-260.

6. Кузниченко В.С. Определение списка робочих частот OFDM сигналов в системах автоматического радиомониторинга в условиячх априорной неопределенности.//Системи управління, навігації та зв'язку. – К.:ЦНДІ НіУ, 2011, вип.1(17).- С.275-278.

7. Кузниченко В.С. Оценка точности корреляционного определения временных параметров OFDM сигналов в системах радиомониторинга.//Радиоелектронные и компьютерные системы. – Х.:НТС ХАИ, 2011, вип. 5(2).- С.18-21.

ФОРМИРОВАНИЕ ЭФФЕКТА ПРОВОДИМОСТИ В МНОГОКОМПОНЕНТНЫХ ПОЛУПРОВОДНИКОВЫХ ПЛЕНОЧНЫХ СЕНСОРНЫХ СТРУКТУРАХ В ГАЗОВЫХ СРЕДАХ

Прусский А.В.[1], Калугин В.Д.[2], Кальной С.Е.[3], Тютюник В.В.[2]
[1]Институт государственного управления в сфере гражданской защиты Национального университета гражданской защиты Украины
[2]Национальный университет гражданской защиты Украины
[3]Харьковский университет Воздушных Сил имени Ивана Кожедуба

Fragments of model of carrying over of a charge in a sensitive material of a semiconductor sensor are considered. It is established that high sensitivity and promptitude of the gage is reached at the expense of fractality effect structures of a sensitive element. It is shown that processes of a desorption of molecules of gas from sensitive mass at 800-1000К proceed with a high speed (1,6·10-3 ÷ 3,1·10-1 s) and consequently don't bring errors in the subsequent measurements of an analytical signal.

Введение. Проблема раннего обнаружения возгорания горючих материалов (ГМ) заключается в том, чтобы по сверхмалым количествам газообразных продуктов первичной стадии горения ГМ можно было бы выявить факт развития пожара в самый начальный момент его зарождения. Поэтому разработка сверхчувствительных систем раннего обнаружения очага возгорания ГМ с газовыми пожарными извещателями (ГПИ) является актуальной задачей обеспечения пожарной безопасности зданий и сооружений.

Цель работы – разработать математическую модель для расчёта условий стабильного функционирования полупроводникового чувствительного элемента спиралевидного типа (ППЧЭ СТ) с сохранением высокой чувствительности, быстродействия и стабильности аналитического сигнала.

Методика экспериментов. Сопоставительный анализ чувствительности различных типов газовых сенсоров (термокаталитические, термокондуктометрические, электрохимические, оптические, полупроводниковые и другие) на газообразные продукты пиролиза ГМ, пожаровзрывоопасные и токсичные газы, показал, что лишь полупроводниковые (ПП) сенсоры могут одновременно использоваться для выявления продуктов пиролиза и контроля изменения концентраций пожаровзрывоопасных и токсичных газов [1]. Поэтому в работе предлагается использовать в качестве чувствительного элемента (ЧЭ) для ГПИ – датчик с ППЧЭ СТ, созданный на базе доступных и дешевых материалов (SnO_2, In_2O_3, Al_2O_3, TiO_2) и без использования благородных металлов (Pt, Ru, Au и др.) в качестве катализаторов адсорбции молекул газов.

Результаты исследований. Физическая модель основана на предположении, что в пористой шероховатой структуре ЧМ формируется хаотичный электрический потенциал. Отдельным кластерам чувствительной массы соответствуют минимумы потенциала V_{min}, в которых локализуются электроны проводимости. Таким образом, кластеры чувствительной массы малых размеров являются «ловушками» для электронов и поэтому проводимость имеет малые значения [2]. При адсорбции молекул газа на кластере меняется электрический потенциал как данного, так и соседних кластеров. В результате этого возникает «прогиб» усреднённого потенциала $V_{уср}$, охватывающий большую группу кластеров. В образовавшейся потенциальной яме для электронов образуется единый уровень энергии, находясь на котором электроны двигаются в пределах этого широкого минимума усреднённого потенциала. Фактически электроны делокализуются и в пределах минимума могут свободно переходить с одного кластера на другой. Таким образом, возле каждой адсорбированной молекулы возникает макроскопическая проводящая область m [2]. По мере увеличения концентрации адсорбированных молекул макроскопические области проводимости начинают объединяться и создают сплошные цепочки, в результате чего формируются дополнительные пути продвижения электронов. Проводимость при этом резко возрастает. Согласно «теории протекания» скачок проводимости начинается, когда концентрация областей проводимости достигает ~ 17 %

[2].

По достижении количества таких областей до $n_{опт}$, проводимость ЧМ достигает максимума.

С точки зрения фрактальных свойств чувствительной массы, происходящие в ней явления можно описать с использованием элементов теории фракталов. «Налипание» молекул газа на кластеры чувствительной массы приводит к изменению фрактальной размерности структуры, которая связана с изменением проводимости [2].

Теоретическая модель проводимости подобных газочувствительных датчиков включает представление о том, что они (сенсоры), обладающие высокой пористостью, рассматриваются как неупорядоченная система оксидных кластеров нанометрического масштаба. Каждый такой кластер представляет собой потенциальную яму, в которой локализуются электроны. Неупорядоченность (хаотичность) потенциала приводит к тому, что в таких структурах отсутствуют понятия зоны проводимости и валентной зоны [2,3], что очень близко к модели «прыжковой» проводимости, (электрон движется от кластера к кластеру «прыжками» путём туннелирования под потенциальными барьерами, которые их разделяют). Отсюда получена оценка для проводимости [2,3]:

$$\sigma^{ЧЭ} = \sigma_0 \cdot e^{-\frac{4}{3}\left(\frac{4\alpha r_{S_0}}{a}\right)^{3/4}\left(\frac{W_0}{kT}\right)^{1/4}} \qquad (1)$$

Влияние адсорбции молекул газа на прыжковую проводимость чувствительной массы может быть учтено с помощью коэффициента «сжатия» $K_{сж}$ фрактального рельефа чувствительного элемента в параметрах r_s и W [3]. Фрактальная длина $l_L^{ЧЭ}$ может быть выражена через фрактальную размерность D [2,3] $l_L^{ЧЭ} \sim \frac{1}{\delta^{D-2}}$, где δ – фрактальный масштаб поверхности (размер кластера) [2,3].

После взаимодействия с газом возрастает фрактальная размерность $D \to D + \Delta D$, и тогда новая фрактальная длина равна $l_L^{ЧЭ+Г} \sim \frac{1}{\delta^{D-2+\Delta D}}$ [2,3]. В результате для коэффициента сжатия имеем простое выражение: $K_{сж} = 1/\delta^{\Delta D}$. (2)

Из (1) и (2) для проводимости ППЧЭ СТ после взаимодействия с газом получаем:

$$\sigma^{ЧЭ+Г} = \sigma_0 \cdot e^{-\frac{4}{3}\left(\frac{4\alpha r_{S_0}}{a}\right)^{3/4}\left(\frac{W_0}{kT}\right)^{1/4}\cdot\delta^{\Delta D}}. \qquad (3)$$

Из (1) и (3) находим относительное увеличение проводимости ЧМ ППЧЭ СТ при адсорбции молекул газа:

$$\frac{\sigma^{ЧЭ+Г}}{\sigma^{ЧЭ}} = \left(\frac{\sigma^{ЧЭ}}{\sigma_0}\right)^{\delta^{\Delta D}-1}. \qquad (4)$$

Поскольку $\frac{\sigma^{ЧЭ}}{\sigma_0} < 1$ и $\delta \ll 1$, то из (4) следует, что проводимость ЧМ резко (как двойная показательная функция) возрастает с увеличением фрактальной размерности ЧЭ [3].

Для численной оценки δ исходим из того, что при «прыжковом» движении элек-

тронов характерным размером является размер нанокластеров ЧМ $\sim 10^{-9} м$, который задаёт масштаб рельефа электрического потенциала $\sim 10^{-9} \div 10^{-10} м$. Учитывая, что геометрические размеры чувствительной массы $\sim 10^{-3} м$, получаем оценку для фрактального масштаба $\delta \sim 10^{-6} \div 10^{-7}$ [3]. Характер зависимости относительного увеличения проводимости ППЧЭ СТ (4) от изменения её фрактальной размерности ΔD (для $\delta = 10^{-6}$, $\delta = 10^{-7}$ и $\frac{\sigma^{ЧЭ}}{\sigma_0} = 10^{-1}$) хорошо согласуется с результатами эксперимента. Сделан вывод о том, что уменьшение фрактального масштаба (размеров кластеров) δ позволяет повысить чувствительность ППЧЭ СТ по концентрации газа и по времени реакции адсорбции [3].

В связи с высокой чувствительностью используемой конструкции ППЧЭ СТ для ГПИ на газы первичной стадии горения ГМ, возникает технически важная задача регенерации, то есть приведения поверхности сенсора к исходному состоянию для проведения последующих циклов измерений. Длительность полного рабочего цикла измерения складывается из времени регистрации адсорбированных молекул газа в воздушной среде (быстродействия) и времени регенерации сенсора.

Установлено, что регенерация очень эфффективно происходит при температурах ~ 1100 К, которая близка к температуре разрушения ЧМ. Дополнительные исследования режимов работы датчика с ППЧЭ для ГПИ на СО и его последующей регенерации показали, что оптимальный режим десорбции, при котором датчик ГПИ наиболее полно повторяет свои технические характеристики и имеет максимальные показатели эксплуатационного ресурса, устанавливается при токе нагревательного элемента 45 мА, что соответствует температуре на ЧЭ 723–773 К [4].

При построении математической модели учитываем, что изменение числа молекул газа (n) на поверхности ЧЭ ГПИ при регенерации определяется кинетическим уравнением [2,4]:

$$\frac{dn}{dt} = v_+ + v_-, \tag{5}$$

где v_+ – частота адсорбции; v_- – частота десорбции молекул газа.

Решение уравнения (4) при условии $v_+ > v_-$ дает уравнение [2,4]:

$$n(t) = \left[n_i^f \cdot e^{-f \cdot w \cdot t} + n_{0_r}^f \cdot \left(1 - e^{-f \cdot w \cdot t}\right) \right]^{1/f}, \tag{6}$$

где n_i – начальное количество молекул газа на поверхности ЧЭ ГПИ, n_{0r} – равновесное количество молекул на поверхности ЧЭ ГПИ при температуре регенерации $T_г$, $w = \beta \cdot v_d \cdot e^{-E/кT_г}$ – вероятность десорбции молекулы газа в единицу времени (комбинация фрактальных размерностей $f = (D^г - D^{чэ} + 1)/D^г$).

Регенерация в потоке чистого воздуха (C = 0), описывается условием $n_{0r} = 0$. В этом случае регенерация ЧЭ происходит быстрее и описывается соотношением [2,4]: $n(t) = n_i \cdot e^{-w \cdot t}$. (7)

Из (6) и (7) видно, что вероятность отрыва молекулы (w) определяет характерное время регенерации $\tau = 1/w$. Для $v_d = 10^{13}$ Гц, E = 2 еВ и $T_г = 1100$ К получаем оценку $\tau = 1{,}6 \cdot 10^{-4}$ с.

В действительности время регенерации (t_r) зависит от начального количества молекул газа на поверхности ЧЭ ГПИ (n_i) и конечного количества молекул $n_i < n_c$, до которого требуется очистить поверхность. Из уравнения (6) получаем [2,4]:

$$t_r = \frac{1}{f \cdot w} \cdot \ln\left(\frac{n_i^f - n_{0_r}^f}{n^f - n_{0_r}^f} \right). \tag{8}$$

В случае, когда регенерация начинается с момента достижения порога перколяции, т.е. сразу после срабатывания сенсора, $n_i = n_c$. Очистка поверхности проводится до уровня $n = 10^{-2} \cdot n_c$.

Однако возможны ситуации, когда при наличии молекул газа в воздухе время регенерации ЧЭ ГПИ будет очень большим. В подобных случаях предпочтителен режим регенерации в потоке чистого воздуха, когда C = 0. В этом случае, согласно (7):

$$t_r = \frac{1}{w} \cdot \ln\left(\frac{n_i}{n}\right). \qquad (9)$$

Считая, что процесс регенерации начинается из состояния с максимальным заполнением поверхности ЧЭ молекулами газа, величину n_i определяем:

$$n_i = n_{\max} = \left(\frac{L}{r_0}\right)^{D^{ЧЭ}}. \qquad (10)$$

Выводы. Показано, что подбором фрактальной структуры сенсора, а также температуры ($T_г$), можно получить времена регенерации меньшие, чем время срабатывания сенсора. В этих условиях процесс регенерации не будет лимитирующим фактором в работе сенсора в режиме аналитического определения реальной концентрации газообразных продуктов горения (CO). Согласно расчетов, выполненных в рамках представленной модели для процесса десорбции молекул CO с ЧМ ГПИ при высоких температурах (800 – 1000 K), регенерационные процессы протекает с очень большой скоростью ($1{,}6\cdot10^{-3} \div 3{,}1\cdot10^{-1}$ с) и поэтому не вносят больших погрешностей при переходе в режим адсорбции и измерения аналитического сигнала ГПИ.

Литература:

1. Пруський А.В. Електрохімічні та термодинамічні основи формування наноплівкових напівпровідникових сенсорів для газових пожежних сповіщувачів / Пруський А.В., Калугін В.Д., Тарахно О.В. // Науковий вісник Чернівецького університету. Хімія. – Чернівці, 2008. – Вип. 401.: – С. 126–128.
2. Фрактальный анализ процессов, структур и сигналов / [Буданов П.Ф., Кальной С.Е., Доля Г.Н. и др.]; под ред. Р.Э. Пащенко. – Харьков: ХООО «НЭО «ЭкоПерспектива», 2006. – 348 с.
3. Пруський А.В. Модель напівпровідникового фрактального чутливого елемента датчика газосигналізатора пожежовибухонебезпечних газів та парів токсичних органічних речовин / Пруський А.В., Кальний С.Е., Калугін В.Д. // Проблемы пожарной безопасности. – Харьков: Фолио, 2005. – Вып. 18. – С. 128 – 132.
4. А.В. Прусский. Математическая модель процесса регенерации чувствительной массы полупроводникового датчика спиралевидного типа газового пожарного извещателя / А.В. Прусский, С.Е. Кальной, В.Д. Калугин // Зб. наук. праць: Вісник НТУ «ХПІ». Тем. вип. «Хімія, хімічна технологія та екологія». – Х.: НТУ «ХПІ», 2008. – №32. – С. 128 – 132.

МЕТОД ЗБЕРЕЖЕННЯ ЕНЕРГОРЕСУРСУ НЕОДНОРІДНИХ СЕНСОРНИХ РАДІОМЕРЕЖ З НАДЛИШКОВОЮ КІЛЬКІСТЮ ВУЗЛІВ ПРИ ЗАБЕЗПЕЧЕННІ ЗАДАНОЇ ЯКОСТІ ПОКРИТТЯ РАЙОНУ МОНІТОРИНГУ

Коваленко І.Г, Романюк В.А
Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України "Київський політехнічний інститут"
01010, Київ, вул. Московська 45/1, тел. (044)353-92-81
E-mail: kig777@ukr.net, моб: (067)501-09-13

A new method of energy savings in wireless sensor networks with an excess of nodes, which divides the network by the required number of subsets of nodes that operate in different time periods, and organize their functioning to ensure the conservation of energy resources of nodes, the maximization "lifetime" of the network and guarantee overlapping monitoring and connectivity nodes.

Вступ. В даний час для моніторингу географічних районів, охорони об'єктів та контролю переміщень особового складу та техніки пропонується використовувати сенсорні радіомережі (СР), які складаються з сенсорних вузлів з функціями моніторингу навколишнього середовища, обробки і передачі даних [1]. Основними елементами сенсорних вузлів є: датчики контролю зовнішнього середовища, мікрокомп'ютер, батарея живлення, прийомопередавач. Вузли СР мають автономне джерело електроживлення обмеженої ємності, тому характерними вимогами до них є мінімізація витрат енергетичних ресурсів вузлів та максимізація часу функціонування мережі. Складність знаходження балансу між ефективністю енергозберігання та продуктивністю передачі інформаційних потоків вимагає розробки ряду методів енергозбереження вузлів СР [2].

Однією з проблем розгортання сенсорних мереж є забезпечення покриття зон моніторингу. Для сенсорних радіомереж крім покриття визначеної зони моніторингу та основних мережевих характеристик можуть висуватись також вимоги з оперативності розгортання, надійності та живучості. Для оперативного розгортання СР використовується розсіювання вузлів СР з літака, ракети або інші засоби випадкового розміщення. При цьому забезпечити необхідну зону покриття при виконанні вимог до СР та випадковому розташуванні сенсорів можливо тільки за допомогою внесення значної надлишковості кількості вузлів. Надлишковість вузлів дозволить підвищити якість покриття зони моніторингу (за охватом і перекриттям зон моніторингу та зв'язності вузлів для забезпечення надійності та живучості СР), але призведе до зайвих енерговитрат та завад в СР. Крім того, в районі моніторингу для організації СР можуть бути задіяні неоднорідні сенсорні вузли з різними радіусами зон моніторингу та передачі даних. Тому постає актуальною задача розробки методів збереження енергоресурсу сенсорної радіомережі з надлишковою кількістю неоднорідних вузлів, які забезпечують задане перекриття зон моніторингу та задану зв'язність окремих вузлів.

Був проаналізований існуючий досвід при розробці методів енергозбереження в сенсорних радіомережах з надлишковою кількістю вузлів [3-4]. Були виявлені переваги та недоліки окремих методів і з їх врахуванням розроблений новий метод збереження енергоресурсу сенсорної радіомережі з надлишковою кількістю різнотипних вузлів при забезпеченні заданого перекриття зон моніторингу та заданої зв'язності окремих вузлів.

Суть методу полягає в тому, що загальна чисельність вузлів СР розділяється на необхідну кількість підмножин вузлів, що працюють в різні періоди часу, після чого організується їх функціонування для забезпечення зберігання енергетичних ресурсів вузлів та максимізації «часу життя» сенсорної радіомережі при забезпеченні заданих показників перекриття зон моніторингу та зв'язності вузлів. Для вирішення цих задач було отримано наступні результати:

*1 Модель СР***.** Для вирішення поставленої задачі були введені наступні обмеження. Нехай N сенсорних вузлів випадковим чином рівномірно розміщені в районі моніторингу

Ω кругової форми з радіусом R. Будемо вважати, що площа району $S_\Omega \to \infty$ та $N \to \infty$, але $N/S_\Omega = const$. Будемо рахувати, що вузли розподілені по площині району Ω за Пуасоновським розподілом з інтенсивністю N/S_Ω. Шлюз розташований випадково в районі Ω. Існує M типів сенсорних вузлів. Кількість сенсорних вузлів i-го типу дорівнює $\rho_i N\,(0 \le \rho_i \le 1,\ 1 \le i \le M,\ \sum_{i=1}^{M} \rho_i = 1)$. Радіус моніторингу сенсорного вузла типу i дорівнює $r_{мi}$, максимальний радіус передачі вузла типу i дорівнює $r_{пi}$. Будемо рахувати, що $\forall i, j \in M, r_{мi} < r_{мj}$, якщо $i < j$. СР представимо в вигляді зв'язного графу $G = (V,E)$, де V – множина сенсорних вузлів, $|V| = N$; E – множина зв'язків між вузлами

2 Визначена залежність відсотка покриття району моніторингу k_{mS_Ω} від кількості вузлів СР при забезпеченні m-кратного перекриття зон моніторингу та відсотка вузлів k_{nE}, що мають n-кратну зв'язність в напрямку передачі даних шлюзу при заданих типах і характеристиках вузлів та району моніторингу

Значення k_{mS_Ω} та k_{nE} – вихідні дані, які залежать від завдань, що покладаються на СР (використовувались значення: $k_{mS_\Omega} = k_{nE} = 0{,}99$) .

Для розробленої моделі були отримані залежності розрахункових значень $k^*_{mS_\Omega}$ та k^*_{nE} від кількості вузлів:

$$k^*_{mS_\Omega} = 1 - \sum_{x=0}^{m-1} \sum_{n_1+\cdots+n_M=x} \frac{1}{\prod_{i=1}^{M} n_i!} \times \left(\prod_{i=1}^{M} \left(\frac{\rho_i N r_{мi}^2}{R^2} \right)^{n_i} e^{\left(-\frac{\rho_i N r_{мi}^2}{R^2} \right)} \right), \qquad (1)$$

$$k^*_{nE} \ge \left(1 - e^{-\frac{N\left(r_п^{\min}\right)^2}{R^2}} \sum_{x=0}^{n-1} \frac{\left(\frac{N\left(r_п^{\min}\right)^2}{R^2} \right)^x}{x!} \right)^N . \qquad (2)$$

Якщо $k^*_{mS_\Omega} \ge k_{mS_\Omega}$, можна казати, що N вузлів відповідних типів забезпечують m-кратне перекриття району моніторингу Ω з радіусом R.

Якщо $k^*_{nE} \ge k_{nE}$, можна казати, що N вузлів забезпечують n-кратну зв'язність СР відповідно вихідним даним $r_п^{\min}, R$.

3 Розроблений алгоритм визначення необхідної кількості множин вузлів СР та часових періодів їх функціонування з використанням залежностей (1) та (2).

Особливістю нового методу є підвищення енергозбереження СР при надлишковості вузлів $\xi_{нв} \in [1{,}5..2), [2{,}5..3),\ \xi_{нв} = N/N_{mn}$ (N_{mn} – необхідна вузлів для виконання умов з забезпечення m-кратного перекриття зон моніторингу та n-кратної зв'язності). Для цього пропонується збільшити кількість підмножини вузлів та періодів їх функціонування.

4 Розроблений алгоритм оптимального розбиття вузлів на визначену кількість підмножин та періодів функціонування.

В розробленому методі енергозберігання, на відміну від аналогічних, пропонується алгоритм рівномірного розподілу вузлів на визначену кількість підмножин та періодів функціонування.

5 Розроблений алгоритм маршрутизації з урахуванням: періодів функціонування та використання енергетичних ресурсів вузлів; вимог зменшення та рівномірності навантаження на вузли, наближених до шлюзу; вимог з відновлення зв'язності мережі при виході з ладу окремих вузлів.

На відміну від існуючих методів енергозбереження в СР з надлишковою кількістю вузлів новий метод на мережевому рівні при маршрутизації повідомлень використовує маршрути з меншим енергетичним навантаженням, забезпечує рівномірне навантаження

наближених до шлюзу вузлів, забезпечує відновлення зв'язності мережі при виході з ладу окремих вузлів. Крім того при застосуванні методу використовуються мінімальні радіуси передач вузлів.

6 Імітаційна моделі СР, реалізація розробленого методу на основі моделі. Оцінка ефективності розробленого методу.

Для імітаційного моделювання пропонується використовувати програмний комплекс The Network Simulator [5]. . В якості показників ефективності пропонується застосувати час життя мережі [2] та реальний відсоток *m*-кратного покриття. При застосуванні спрощеної моделі СР (стандартних протоколів канального та фізичного рівня (IEEE 802.11 DCF), $m = n = 2$, надлишковості $\xi_{\text{нв}} > 2$) отримано результати, які дозволяють зробити висновок, що розроблений метод дозволяє підвищити час життя мережі до 15% при покращенні покриття зони моніторингу до 10% площі відносно існуючих методів даного класу. Крім того, розроблений метод, на відміну від існуючих, збільшує час життя мережі при надлишковості вузлів $\xi_{\text{нв}} \in [1{,}5..2)$ до 25%.

Висновки. Розроблений метод зберігання енергоресурсу сенсорної радіомережі з надлишковою кількістю різнорідних вузлів при забезпеченні заданого перекриття зон моніторингу та заданої зв'язності окремих вузлів дозволяє підвищити час функціонування СР до 25% при покращенні якості покриття району моніторингу до 10%.

Напрямки подальших досліджень. При розробці методу було виявлено, що при збільшенні обсягів СР, частоти та обсягу збору інформації вузлами СР збільшується трафік через вузли, що наближені до шлюзу. При цьому збільшується частота колізій при випадковому доступі до радіоресурсу, що призводить до зниження пропускної спроможності, підвищеного енергоспоживання вузлами та зменшення часу функціонування СР. Тому постає актуальною задача розробки методів збереження енергоресурсу сенсорних радіомереж на канальному рівні.

Література:

1. *Міночкін А.І, Романюк В.А.*, Жук О.В. Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць № 4. – К.: ВІТІ НТУУ "КПІ". – 2007. – С. 112 – 119.
2. *Коваленко І.Г., Романюк В.А., Діянчук І.М.,* Аналіз методів енергозбереження в сенсорних радіомережах// Збірник наукових праць № 1. – К.:ВІТІ НТУУ «КПІ». – 2011. – С. 76 – 84.
3. Jin Y., Wang L., Jo J., Kim Y., Yang M., Jiang Y., "EECCR: An Energy-Efficient m-Coverage and n-Connectivity Routing Algorithm Under Border Effects in Heterogeneous Sensor Networks", IEEE Transactions on Vehicular Technology, 2009, vol. 58, no. 3.
4. Dong Y., Chang H., An Energy Conserving Routing Algorithm for Wireless Sensor Networks// International Journal of Future Generation Communication and Networking, Vol. 4, No. 1, 2011, pp. 39 – 53.
5. VINT Project, The Network Simulator-ns, http://www.isi.edu/nsnam/ns.

МОДЕЛИРОВАНИЕ МАРШРУТИЗАЦИИ В СВЕРХБОЛЬШОЙ СЕНСОРНОЙ СЕТИ С ОЦЕНКОЙ ЭНЕРГОПОТРЕБЛЕНИЯ

Нечаев Ю.Б.[1], Баев А.Д.[2], Стромов А.В.[3]
[1]ОАО «Концерн «Созвездие»
394018, Воронеж, ул. Плехановская, 14, тел. (473)2521996.
[2]Воронежский государственный университет
394036, Воронеж, Университетская площадь, 1, математический факультет,
тел. (473)2208533. E-mail: astromov@yandex.ru

The report represents mathematical model of massively dense sensor network with potential field lines based routing. The suggestion is made about how to take into account adaptive information rate and simple smart antennas for nodes while modeling a network.

Введение

Современный уровень развития телекоммуникационных и информационных технологий, растущие потребности по обеспечению мониторинга естественных и искусственных сред и процессов, миниатюризация и низкая стоимость сложных электронных компонентов актуализируют задачи построения беспроводных сенсорных сетей с большим количеством узлов. Предсказания фантастов о появлении «умной пыли» – распределенной сенсорной сети, состоящей из миллионов микроскопических узлов, сейчас уже близки к воплощению в реальность. Такие сети называют сверхбольшими сенсорными сетями (СБСС). Беспроводная сенсорная сеть, предназначенная для мониторинга состояния некоторых параметров в рамках определенной области, состоит из идентичных узлов, каждый из которых состоит из датчика-сенсора, приемопередающего радиомодуля, управляющего процессора и элемента питания. Информация, получаемая сенсорами, собирается на определенных узлах, называемых базовыми станциями, передаваясь по сети множественными ретрансляциями.

Задача передачи информации в СБСС имеет следующие особенности: с одной стороны, в отличие от сетей связи, информационные потоки стабильны и практически не зависят от времени ни по объёму передаваемой информации, ни по маршруту её передачи; с другой стороны, наличие большого количества узлов не позволяет применять классические методы построения маршрутов проактивными или реактивными алгоритмами, так как задержки и расходы сетевого трафика на построение маршрутов или периодический опрос состояния сети могут стать недопустимо большими. Кроме того, при использовании распространенных способов маршрутизации в беспроводных сетях обычно строится только один маршрут от источника информации к получателю (если же было построено несколько, в один и тот же момент времени может использоваться только один из них, так как остальные, как правило, пересекаются с ним в определенном количестве общих узлов). Таким образом, задача резервирования маршрута, а тем более создания дополнительных маршрутов для передачи информации (в случае недостаточной пропускной способности основного) не решается.

Ещё одной особенность СБСС является задача экономного расходования энергетического ресурса узлов (заряда батареи). При наличии единственного маршрута энергетический ресурс составляющих его узлов быстро истощается, и сеть прекращает свою работу. Желательна организация нескольких непересекающихся путей доставки информации с распределением по ним информационного потока. При этом важно сочетать равномерность расходования энергии в узлах сети с приемлемыми временными задержками на доставку информации. Решить поставленные проблемы возможно с помощью алгоритма маршрутизации, основанного на геометрии силовых линий потенциального поля. Области появления информации рассматриваются как истоки, а потребители информации – стоки. Силовые линии поля – маршруты передачи информации. Распределение интенсивности информационных потоков следует осуществлять по принципу «длина маршрута обратно пропорциональна интенсивности потока по нему». Это обеспечивает использование минимально необходимого количества узлов при низкой пропускной способности

[1], или распределение нагрузки с целью продления времени жизни сети с ограниченным энергетическим ресурсом узлов [2].

Математическая модель СБСС

Для математического описания приведённой выше СБСС удобнее использовать не имитационные методы моделирования основанные на подробном воспроизведении работы конкретной сети на основе «микроскопических» параметров, таки как конкретное количество узлов, их расположение, характеристики, состояние узла в каждый момент времени, а перейти к аналитической математической модели, основанной на «макроскопических» характеристиках сети [1, 2, 3]:

– функция плотности информационного потока **W** ($бит/(м \cdot с)$) – непрерывная векторная функция, направление которой совпадает с направлением движения информации в данной точке, а её скалярная величина равна скорости, с которой информационный поток пересекает бесконечно малый отрезок, расположенный в указанной точке перпендикулярно к направлению функции **W**;

– потенциал поля информационного потока U ($Вт$), с физической точки зрения – суммарная мощность, которая будет затрачена всеми ретрансляторами для доставки информации до базовой станции, где функция U обращается в 0, информационный поток **W** направлен против роста потенциала;

– функция плотности производства / потребления информации ρ ($бит/м^2$) принимающая положительные или отрицательные значения в зависимости от того, производится или потребляется пользовательская информация в данной точке области, занимаемой сетью;

– коэффициент информопроводности K ($(бит/с)/Вт$ или $бит/Дж$) –, определяющий свойства сети как среды распространения сигнала [3] и численно равный объему информации, пересекающему отрезок единичной длины, перпендикулярный направлению потока информации **W** за единицу времени, если градиент потенциала равен 1. Маршруты информационных потоков в СБСС описываются уравнением

$$\nabla \cdot (-K \nabla U) = \rho. \qquad (1)$$

Зная функцию потенциала U можно получить явный вид функции **W**, который определяет множество непересекающихся маршрутов передачи информации. Также, интегрируя функцию U по области, занимаемой сетью можно получить оценку суммарных энергетических затрат на передачу информации.

Коэффициент информопроводности

Особое значение имеет выбор коэффициента информопроводности. Задав K как функцию от координат области расположения сети можно учесть различные свойства рассматриваемой СБСС, таки как плотность расположения узлов, влияния на сеть помехи и т. п. Рассмотрим в качестве примера СБСС, узлы которой поддерживают адаптивный алгоритм изменения скорости передачи в зависимости от отношения энергий сигнала / шума (E_S/N_0) в канале [4]. Пусть они также оборудованы антенной системой с адаптируемой диаграммой направленности, способной ослаблять воздействие помехи на скорость передачи информации. Примером простейшего варианта такой системы является антенна из двух вертикальных вибраторов с расстоянием между ними $\lambda/4$, где λ — длина волны используемой несущей. Тогда, при соответствующем выборе разности фаз на вибраторах, можно получить диаграмму направленности антенны от практически круговой в горизонтальной плоскости, при подаче синфазного сигнала на оба вибратора, до кардиоидоподобной, в случае разности фаз равной $\pi/2$. Также узлы, при воздействии помехи, способны независимо ориентировать свои антенны «вырезом» кардиоидоподобной диаграммы в направлении помехи, а также регулировать глубину «выреза», в зависимости от мощности помехи (соответственно, и от расстояния от узла до источника по-

мехи). Рассмотрим случай, когда внутри СБСС с указанными выше особенностями находится источник помехи с изотропной, круговой диаграммой направленности антенны. Тогда в круге некоторого радиуса R_1 вокруг источника помехи, работа узлов СБСС будет невозможна, а в кольце, ограниченном окружностями R_2 и R_1, где $R_2 > R_1$ скорость передачи будет плавно уменьшаться, по мере приближения к внутренней окружности R_1 и на ней обратится в 0. Однако при наличии узлов с адаптивно изменяемой диаграммой направленности антенн, обнуление произойдет только в радиальном направлении к источнику помехи, а в тангенциальном сохраниться возможность передачи информации. Это означает анизотропию коэффициента *K*. Функционирование такой СБСС можно описать следующим уравнением в полярных координатах

$$\frac{\partial}{\partial r}\left(K_1(r,\varphi)\frac{\partial U}{\partial r}\right)+\frac{\partial}{\partial \varphi}\left(K_2(r,\varphi)\frac{\partial U}{\partial \varphi}\right)=\rho, \qquad (2)$$

где $K_1(r,\varphi)\big|_{r=R_1}=0$, а $K_2(r,\varphi)\big|_{r=R_1}>0$. Функции K_1 и K_2 будут фактически получаться одна из другой сдвигом вдоль оси *r*.

Значения R_1, R_2 и вид K_1 и K_2 зависит от конкретных характеристик СБСС и источника помехи. При аппроксимации значений K_1 и K_2 по известным данным о скоростях передачи информации между узлами при различных отношениях сигнал / шум, видно, что справедливо следующее выражение: $\left.\frac{\partial K_1(r,\varphi)}{r}\right|_{r=R_1}=0$. Таким образом, модель СБСС описывается граничной задачей с сильным вырождением на границе, что потребовало дополнительного математического исследования задачи. Были установлены коэрцитивные оценки решений уравнения типа (2), а также доказано существование и единственность его решения в специальных весовых пространствах, типа пространств С. Л. Соболева. При доказательства применялся метод, аналогичный использованному в [5].

Заключение

Предложенная модель адекватно описывает СБСС с перспективным методом определения маршрутов для передачи информации. На её основе могут быть получены оценки характеристик, в том числе энергопотребления, моделируемой СБСС. Также возможна разработка алгоритма маршрутизации, способного адаптивно изменять конфигурацию сети при появлении источника помех.

Литература:

1. S. Toumpis and L. Tassiulas, “Optimal deployment of large wireless sensor networks,” IEEE Trans. Inform. Theory, Jul. 2006.

2. M. Kalantari and M. Shayman, “Energy efficient routing in wireless sensor networks,” in Proc. Conf. Inf. Sci. Syst., NJ, Mar. 2004.

3. Нечаев Ю.Б., Баев А.Д., Стромов А.В. Энергетическая трактовка функции потенциала в математической модели сверхбольшой беспроводной сенсорной сети // Информатика: проблемы, методология, технологии: материалы XI Международной научно-методической конференции, Воронеж, 10–11 февраля 2011 г.: в 3 т. – Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2011. – Т.2. – с. 120-123

4. Cognitive radio technology. Ed. B. Fette, Academic Press, 2009, P. 693.

5. Баев А.Д., Нечаев Ю.Б., Стромов А.В. Об одном методе математического моделирования адаптивных сверхбольших сенсорных сетей. // Современные методы теории функций и смежные проблемы: материалы воронежской зимней математической школы. – Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2011. – с. 33-34.

ВИМІРЮВАЛЬНИЙ СТЕНД ДЛЯ ДОСЛІДЖЕНЬ АКУСТОЕЛЕКТРОННИХ ДАТЧИКІВ КУТА ПОВОРОТУ

Лепіх Я. І., Карпенко А. О., Снігур П. О.
Одеський національний університет імені І. І. Мечникова
65082, Одеса, вул. Дворянська, 2, НДЛ-3 МННФТЦ, тел./ф. +38048 723-34-61.
e-mail: ndl_lepikh@onu.edu.ua

The measuring stand for acoustoelectronic angle turn gauges researches and certification with the minimal discreteness of measurements 0,013 ° in any angle sector is described.

Як відомо, датчики кута повороту є необхідним елементом різноманітних автоматичних систем керування та знаходять застосування у багатьох галузях науки і техніки. Останнім часом інтенсивно розвивається принципово новий клас датчиків кута повороту, що працюють на фізичних принципах, які полягають у використанні акустоелектричних явищ у твердому тілі, зокрема при поширенні в ньому поверхневих акустичних хвиль (ПАХ) [1]. Частотний вид вихідного сигналу окрім високих метрологічних параметрів надає цьому класу датчиків ряд додаткових переваг перед аналогами, зокрема, при вирішенні проблеми інтелектуалізації датчика, а саме спряження його з ЕОМ, можливості створення бездротових датчиків для дистанційних вимірів тощо. Однак вимірювання основних характеристик датчика кута повороту і його атестації існуючими стандартними методами і засобами є громіздким, недостатньо точним і не задовольняє реалізацію високих потенційних можливостей датчиків цього класу.

В даній роботі описано розроблений спеціальний вимірювальний стенд позбавлений цих недоліків і демонструється його використання при експериментальних дослідженнях зразка датчика кута повороту на ПАХ.

В основі роботи датчика лежить явище кутової залежності фазової швидкості поширення ПАХ в анізотропних п’єзоелектриках [2], що відображається у залежності частоти вихідного сигналу від кута повороту. Чутливий елемент датчика на ПАХ включений у позитивний зворотний зв'язок підсилювача високої частоти.

До основних технічних характеристик датчика кута повороту відноситься точність, або основна похибка, з якою можливо виміряти кут повороту. Виходячи з того, що вихідний сигнал датчика має частотний вид, необхідно вимірювати залежність частоти змінного струму з виходу датчика на ПАХ від кута повороту вісі датчика. На основі отриманих результатів можуть бути розраховані параметри датчика і побудовано графік залежності частоти вихідного сигналу від кута повороту.

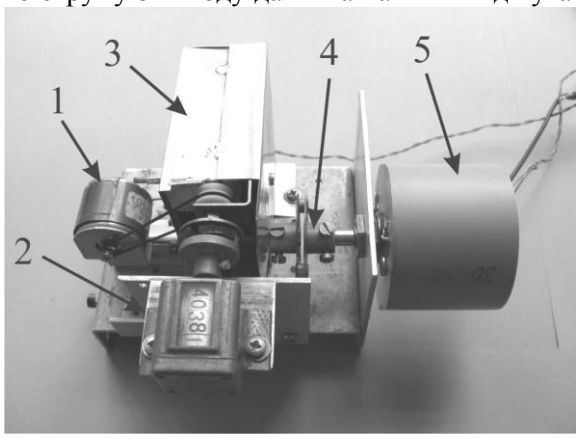


Рис. 1, Вимірювальний стенд з датчиком кута повороту. 1 – реверсний електродвигун; 2 – лічильник обертів; 3 – редуктор годинникового механізму; 4 – вузол механічного зщеплення великої вісі редуктора з віссю датчика кута повороту; 5 – датчик кута повороту.

Висока чутливість і точність переміщення механічних частин вимірювального стенда досягається використанням основного вузла стенда – годинникового механізму, який являє собою елемент точної механіки, що має механічний редуктор з великим передаточним числом (рис. 1).

Взаємодія окремих вузлів стенда реалізується в такій послідовності. На малій осі годиникового механізму - 3 розташований механічний лічильник числа обертів – 2, через пасову передачу мала вісь пов'язана з електродвигуном постійного струму – 1, велика вісь - 4 безпосередньо з'єднана з валом досліджуваного датчика кута повороту – 5, при включеному електродвигуні лічильник - 2 підраховує кількість

обертів малої осі годиникового механізму - 3.

Кількість обертів лічильника редуктора вимірювального стенду на один кутовий градус ω розраховується по формулі

$$\omega = \frac{\Delta n}{\Delta \beta} \left[\text{об}/1^{\circ} \right], \quad (1)$$

де n – кількість обертів лічильника;

Δn – різниця показників лічильника між актами вимірів;

$\Delta \beta$ – різниця величини кута повороту між актами вимірів;.

Калібровка датчика кута повороту здійснювалась шістьма актами вимірів (при повороті вала датчика по годинниковій і проти годинникової стрілки) на базових кутах β = 0°, 180°, 360°. Далі по формулі (1) розраховувалась ω для всіх шести випадків.

Кількість обертів лічильника редуктора вимірювального стенду на один кутовий градус $\omega_{ср}$ визначалася як середнє арифметичне по формулі

$$\omega_{ср} = \frac{1}{6} \sum_{n=1}^{6} \omega_n , \quad (2)$$

де ω_n – кількість обертів лічильника редуктора вимірювального стенду на один кутовий градус *n-го* вимірювання.

Розрахунки по формулах (1), (2) показали, що абсолютна похибка вимірювального стенду становить 1,37´´.

Послідовність дій при вимірюванні наступна.

Датчик установлюється при вимірюваннях на більшу вісь редуктора -2 (рис. 1) і підключається до частотоміра. За допомогою електродвигуна і механічно пов'язаного з ним лічильника обертів виробляється поворот вала датчика до мінімального значення частоти змінного струму з його виходу. Це нижня межа робочого сектора вимірюваних кутів. Далі фіксуються показання частотоміра і лічильника обертів вала електродвигуна, умовно прийняті за кут повороту вала датчика, рівний 0º. Через кожні 79 обертів вала електродвигуна (що відповідає повороту вала датчика на 1º фіксуються значення частоти. Така таріровка виробляється до моменту зриву генерації датчика. Аналогічна процедура виконується у зворотному напрямку - від максимуму частоти до мінімуму.

Таким чином, розроблений вимірювальний стенд забезпечує високу точність визначення кута повороту і може бути корисним як при розробці датчиків кута повороту на основі елементів функціональної мікроелектроніки так і для їх атестації.

Література:

1. Лепіх Я.І., Гордієнко Ю.О., Дзядевич С.В., та ін. Створення мікроелектронних датчиків нового покоління для інтелектуальних систем.; Монографія за ред. Лепіха Я.І.– Одеса: Астропринт, 2010.–296 с.

2. Лепіх Я.І., Метод перелагоджування частоти пристрою на поверхневих акустических хвилях // Патент України №95526. Опубл. 10.08.2011, Бюл. №15.

РАДИОЛОКАЦИОННЫЙ И СВЯЗНОЙ РЕЖИМЫ МОБИЛЬНЫХ СТАНЦИЙ СВЯЗИ И РАДИОЛОКАЦИИ С ЦИФРОВЫМИ АНТЕННЫМИ РЕШЕТКАМИ

Зинченко А.А.[1], Слюсар В.И.[2]
[1]Национальный университет обороны Украины,
03040, г. Киев, Воздухофлотский проспект, 28
[2]Центральный научно-исследовательский институт вооружения и военной техники Вооруженных Сил Украины
03040, г. Киев, Воздухофлотский проспект, 28
e-mail: swadim@inbox.ru

The given work is devoted to the research of signal's model of digital antenna array for radar and communiction applications.

При создании интегрированных систем связи и радиолокационной разведки (ИССРР) на основе технологии цифровых антенных решеток (ЦАР) перспективным направлением является совместное использование принципов MIMO-локации и MIMO-связи в многопользовательском варианте реализации. Оптимальным решением в этом случае представляется применение конформных по конструкции антенных систем, состоящих из нескольких секций-решеток, расположенных по граням усеченной пирамиды. Такие конструкции, как известно, позволяют отказаться от механического сканирования луча и осуществлять мгновенный обзор пространства по секторам ответственности, выполняя когерентное накопление сигналов для улучшения энергетических показателей при работе по малоразмерным целям.

При анализе потенциальных возможностей ИССРР на начальном этапе развития соответствующей теории целесообразно рассматривать независимо радиолокационный и связной режимы функционирования мобильных станций связи и радиолокации (МССР). Такой методический прием позволит исключить из анализа наиболее сложные ситуации, когда связные сигналы приходят одновременно с отраженным от целей радиолокационным излучением, если применяются разные сигналы для связи и локации.

Применительно к радиолокационному режиму работы модель отклика многосекционной ЦАР в случае отдельно взятой МССР, входящей в многопозиционную группировку аналогичных станций, можно представить в матричном виде следующей записью:

$$\mathrm{U} = \mathrm{P} \cdot \mathrm{A} + \mathrm{n},$$

где U – блочный вектор комплексных напряжений сигналов по выходам частотных фильтров пространственных каналов многосекционной ЦАР, P - сигнальная матрица, A – блочный вектор амплитуд сигналов, n – блочный вектор напряжений шумов.

В представленном выражении ключевым элементом является сигнальная матрица P, структура которой определяет компоновку элементов векторов напряжений, амплитуд и шумов. В этой связи рассмотрим формат матрицы P подробнее.

Будем полагать, что E передатчиков активной ЦАР излучает одночастотные непрерывные сигналы на разных длинах электромагнитных волн, а в гранях пирамидальной антенной системы используются плоские решетки с различным количеством элементов по горизонтали (R) и вертикали (D). В указанном варианте излучения от каждой цели будет отражаться многочастотный пакет из E сигналов, с учетом чего структура сигнальной матрицы P для режима радиолокации будет иметь вид:

$$P = \left(Q\,[\blacksquare]\,V\right)[\otimes]F, \qquad (1)$$

где [■] - символ блочного матричного произведения Хатри- Рао [1],

[⊗] - символ блочного кронекеровского произведения,

блочные матрицы характеристик направленности антенных элементов в азимутальной $Q_{rt}(x_m)$ и угломестной $V_{dt}(y_m)$ плоскостях в направлениях на m-й источник сигналов с угловыми координатами (x_m, y_m) представлены в виде:

$$Q=\left[\begin{array}{c|c|c} Q_{11}(x_1) & \cdots & Q_{11}(x_M) \\ \vdots & \ddots & \vdots \\ Q_{R1}(x_1) & \cdots & Q_{R1}(x_M) \\ \hline \vdots & \vdots & \vdots \\ \hline Q_{1T}(x_1) & \cdots & Q_{1T}(x_M) \\ \vdots & \ddots & \vdots \\ Q_{RT}(x_1) & \cdots & Q_{RT}(x_M) \end{array}\right],\quad V=\left[\begin{array}{c|c|c} V_{11}(y_1) & \cdots & V_{11}(y_M) \\ \vdots & \ddots & \vdots \\ V_{D1}(y_1) & \cdots & V_{D1}(y_M) \\ \hline \vdots & \vdots & \vdots \\ \hline V_{1T}(y_1) & \cdots & V_{1T}(y_M) \\ \vdots & \ddots & \vdots \\ V_{DT}(y_1) & \cdots & V_{DT}(y_M) \end{array}\right],$$ где r=1, …, R – порядковый номер антенного элемента в строке антенной решетки в пределах секции; d=1, …, D – порядковый номер антенного элемента в столбце антенной решетки в пределах секции; t=1, …, T – порядковый номер секции многосекционной ЦАР;

$$F=\left[\begin{array}{ccc|c|ccc} F_{11}(\omega_{11}) & \cdots & F_{11}(\omega_{1E}) & \cdots & F_{11}(\omega_{M1}) & \cdots & F_{11}(\omega_{ME}) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{R1}(\omega_{11}) & \cdots & F_{R1}(\omega_{1E}) & \cdots & F_{R1}(\omega_{M1}) & \cdots & F_{R1}(\omega_{ME}) \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline F_{1T}(\omega_{11}) & \cdots & F_{1T}(\omega_{1E}) & \cdots & F_{11}(\omega_{M1}) & \cdots & F_{1T}(\omega_{ME}) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{RT}(\omega_{11}) & \cdots & F_{RT}(\omega_{1E}) & \cdots & F_{RT}(\omega_{M1}) & \cdots & F_{RT}(\omega_{ME}) \end{array}\right]$$ - блочная матрица АЧХ частотных фильтров, синтезированных с помощью дискретного преобразования Фурье на E частотах отраженных от M целей E сигналов.

Предполагается, что задача измерения дальности решается в многопозиционном режиме по полученным от отдельных МССР значениям угловых координат и радиальных скоростей целей. В простейшем случае это может быть триангуляционный метод.

Аналогичную запись следует взять за основу и для составления матричной модели отклика приемной ЦАР в связном режиме работы. Отличие от рассмотренного выше режима радиолокации заключается в необходимости учета матриц передаточных характеристик канала MIMO в азимутальной и угломестной плоскостях, а также трактовке матрицы АЧХ частотных фильтров F в соответствии с типом применяемых сигналов. В случае использования сигналов OFDM выражение (1) модифицируется к виду:

$$P=\left(\left(Q\circ\tilde{H}_Q\right)[\blacksquare]\left(V\circ\tilde{H}_V\right)\right)[\otimes]F\ ,$$

где

$$\tilde{H}_Q=\left[\begin{array}{c|c|c} \tilde{h}_{Q111} & \cdots & \tilde{h}_{Q11M} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QR11} & \cdots & \tilde{h}_{QR1M} \\ \hline \vdots & \vdots & \vdots \\ \hline \tilde{h}_{Q1T1} & \cdots & \tilde{h}_{Q1TM} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QRT1} & \cdots & \tilde{h}_{QRTM} \end{array}\right],\quad \tilde{H}_V=\left[\begin{array}{c|c|c} \tilde{h}_{V111} & \cdots & \tilde{h}_{V11M} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VD11} & \cdots & \tilde{h}_{VD1M} \\ \hline \vdots & \vdots & \vdots \\ \hline \tilde{h}_{V1T1} & \cdots & \tilde{h}_{V1TM} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VDT1} & \cdots & \tilde{h}_{VDTM} \end{array}\right]$$ - блочные матрицы передаточных характеристик канала MIMO в азимутальной $\tilde{h}_{Qrtm}$ и угломестной $\tilde{h}_{Vrtm}$ плоскостях в направлениях на m-й источник сигналов с угловыми координатами (x_m, y_m), где r=1, …, R – порядковый номер антенного элемента в строке антенной решетки в пределах секции; d=1, …, D – порядковый номер антенного элемента в столбце антенной решетки в пределах секции; t=1, …, T – порядковый номер секции многосекционной ЦАР.

В режиме связи демодуляция сигналов может быть осуществлена путем оптимального оценивания вектора комплексных амплитуд сигналов согласно методу максимального правдоподобия по известному выражению $\tilde{A}=\left(P^T P\right)^{-1}P^T U$ с учетом пространственно-временного либо иного типа кодирования MIMO-сигналов. В радиолокационном режиме оцениванию должны подлежать параметрические элементы сигнальной матрицы P,

а именно: неизвестные угловые координаты источников излучения и их допплеровские частоты. Опираясь на представленные матричные записи откликов ЦАР, можно получить нижние границы Крамера-Рао для дисперсий оценок параметров сигналов, используя, например, методику, изложенную в [2]. В связном режиме задача формирования информационной матрицы Фишера упрощается благодаря возможности использования допущения об известных угловых координатах источников сигналов и частотах всех OFDM-поднесущих. Для радиолокационного варианта функционирования МССР при этом необходимо выполнить дифференцирование сигнальной матрицы P по неизвестным угловым координатам целей и допплеровским частотам отраженных сигналов. Анализ соответствующих оценок точности, а также проверка их достоверности путем математического моделирования является целью дальнейших исследований.

Литература:

1. Слюсар В.И. Обобщенные торцевые произведения матриц в моделях цифровых антенных решеток с неидентичными каналами.//Известия вузов. Сер. Радиоэлектроника.- 2003. - Том 46, № 10. - С. 9 - 17.

2. Слюсар В.И. Информационная матрица Фишера для моделей систем, базирующихся на торцевых произведениях матриц// Кибернетика и системный анализ.- 1999.- № 4.- С. 141 – 149.

МАТРИЧНА МОДЕЛЬ ВІДГУКУ БАГАТОСЕКЦІЙНОЇ ЦАР У СКЛАДІ ПІРАМІДАЛЬНОЇ НАНОСХЕМИ

Слюсар Д.В.[1], Слюсар В.І.[2]
[1]Національний технічний університет України «КПІ»,
м. Київ, вул. Політехнічна, 14,
[2]Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України,
м. Київ, Повітрофлотський проспект, 28
e-mail: swadim@inbox.ru

The given work is devoted to matrix model of multi-section digital antenna array in the pyramidal nanochip of wireless network on chip.

При використанні у складі бездротових мереж на кристалі пірамідальних конструкцій наносхем згідно з [1] можуть створюватись багатосекційні наноантенні комплекси на основі цифрових антенних решіток (ЦАР), де в якості секцій слід розглядати решітки, розташовані в окремо взятому рівні піраміди, та сукупність решіток, що відповідають тій чи іншій грані піраміди. Таким чином, необхідно ввести ієрархічну градацію секцій багатосекційної ЦАР одного нанонoду (нанорозмірної базової станції передачі даних) за схемою «грань – рівень». Зазначена специфічна побудова антенних систем вносить певні особливості в обробку сигналів багатокористувальницької системи MIMO на кристалі. Тому розгляд специфіки аналітичної моделі відгуку багатосекційної ЦАР у складі пірамідальної наносхеми є метою даної доповіді.

Якщо подати сукупність напруг сигналів по виходах приймальних каналів багатосекційної ЦАР одного нанонoду у традиційному вигляді [2]:

$$\mathrm{U} = \mathrm{P} \cdot \mathrm{A} + \mathrm{n},$$

де U - блоковий вектор комплексних напруг сигналів по виходах частотних фільтрів просторових каналів сукупності секцій багатосекційної ЦАР, P - сигнальна матриця, A – блоковий вектор амплітуд сигналів, n – блоковий вектор шумових напруг,

то структура сигнальної матриці P та блокових векторів U і A у випадку лінійно-решітчатих секцій ЦАР буде наступною:

$$P = \left(\left(Q \circ \tilde{H}_Q\right)[\blacksquare]\left(V \circ \tilde{H}_V\right)\right)[\blacksquare]F,$$

де $Q = \begin{bmatrix} Q_{111}(x_{1_{11}}) & \cdots & Q_{111}(x_{M_{11}}) \\ \vdots & \ddots & \vdots \\ Q_{R_{TG}11}(x_{1_{11}}) & \cdots & Q_{R_{TG}11}(x_{M_{11}}) \\ \hdashline Q_{1TG}(x_{1_{TG}}) & \cdots & Q_{1TG}(x_{M_{TG}}) \\ \vdots & \ddots & \vdots \\ Q_{R_{TG}TG}(x_{1_{TG}}) & \cdots & Q_{R_{TG}TG}(x_{M_{TG}}) \end{bmatrix}$, $V = \begin{bmatrix} V_{111}(y_{1_{11}}) & \cdots & V_{111}(y_{M_{11}}) \\ \vdots & \ddots & \vdots \\ V_{R_{TG}11}(y_{1_{11}}) & \cdots & V_{R_{TG}11}(y_{M_{11}}) \\ \hdashline V_{1TG}(y_{1_{TG}}) & \cdots & V_{1TG}(y_{M_{TG}}) \\ \vdots & \ddots & \vdots \\ V_{R_{TG}TG}(y_{1_{TG}}) & \cdots & V_{R_{TG}TG}(y_{M_{TG}}) \end{bmatrix}$ - блокові

матриці характеристик спрямованості антенних елементів в азимутальній $Q_{r_{tg}tg}(x_{mg})$ та кутомісній $V_{r_{tg}tg}(y_{mg})$ площинах у напрямках на m-е джерело сигналів з кутовими координатами (x_{mg}, y_{mg}), де r=1, …, R_{tg} – порядковий номер антенного елемента у антенній решітці в межах tg-ї секції,

t=1, …, T – порядковий номер рівня піраміди,

g=1,…., G - порядковий номер грані піраміди,

$$\tilde{H}_Q = \begin{bmatrix} \tilde{h}_{Q1111_{11}} & \cdots & \tilde{h}_{Q111M_{11}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QR_{TG}111_{11}} & \cdots & \tilde{h}_{QR_{TG}11M_{11}} \\ \hdashline \tilde{h}_{Q1TG1_{TG}} & \cdots & \tilde{h}_{Q1TGM_{TG}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QR_{TG}TG1_{TG}} & \cdots & \tilde{h}_{QR_{TG}TGM_{TG}} \end{bmatrix}, \quad \tilde{H}_V = \begin{bmatrix} \tilde{h}_{V1111_{11}} & \cdots & \tilde{h}_{V111M_{11}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VR_{TG}111_{11}} & \cdots & \tilde{h}_{VR_{TG}11M_{11}} \\ \hdashline \tilde{h}_{V1TG1_{TG}} & \cdots & \tilde{h}_{V1TGM_{TG}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VR_{TG}TG1_{TG}} & \cdots & \tilde{h}_{VR_{TG}TGM_{TG}} \end{bmatrix}$$ - блокові матриці передаточних характеристик каналу MIMO в азимутальній $\tilde{h}_{QR_{TG}TGM_{TG}}$ та кутомісній $\tilde{h}_{VR_{TG}TGM_{TG}}$ площинах у напрямках на m-е джерело сигналів з кутовими координатами $\left(x_{m_{tg}}, y_{m_{tg}}\right)$, де r=1, …, R_{tg} – порядковий номер антенного елемента у антенній решітці в межах tg-ї секції,

$$F = \begin{bmatrix} F_{111}(\omega_{1_{11}}) & \cdots & F_{111}(\omega_{M_{11}}) \\ \vdots & \ddots & \vdots \\ F_{S_{TG}1}(\omega_{1_{11}}) & \cdots & F_{S_{TG}11}(\omega_{M_{11}}) \\ \hdashline F_{1TG}(\omega_{1_{TG}}) & \cdots & F_{1TG}(\omega_{M_{TG}}) \\ \vdots & \ddots & \vdots \\ F_{S_{TG}TG}(\omega_{1_{TG}}) & \cdots & F_{S_{TG}TG}(\omega_{M_{TG}}) \end{bmatrix}$$ - блокова матриця амплітудно-частотних характеристик (АЧХ) частотних фільтрів на частотах піднесучих OFDM сигналу,

[■] - символ транспонованого блокового торцевого добутку матриць [2] (блокового добутку Хатрі-Рао).

Кожна грань та рівень піраміди можуть взаємодіяти з різною кількістю джерел випромінювання, що мають неоднакове кутове положення відносно нормалі до секційної ЦАР. Тому у матрицях характеристик спрямованості антенних елементів введені індекси tg при порядковому номері кутової координати джерела сигналу, наприклад, $x_{M_{tg}}$, $y_{M_{tg}}$. Оскільки у загальному випадку у різних рівнях пірамідальних наносхем та різних їхніх гранях можуть розташовуватися неоднакові за кількістю антенних елементів нанорешітки, то в кожному блоці блокових матриць буде своя кількість елементів по вертикалі. Це враховано подвійним індексом кількості просторових каналів R_{GT}.

Якщо решітки мають однакову кількість елементів у вертикальній та горизонтальній площинах, то відповідний параметр R_{GT} для них буде однаковим, як що ж ні, то доцільно при величині R_{GT} ввести додатковий індекс x або y, що характеризував би відповідно горизонтальну та вертикальну площину, тобто отримаємо R_{xGT} та R_{yGT}.

У випадку застосування в кожній секції ЦАР не лінійних, а плоских решіток з різною кількістю елементів у вертикальній та горизонтальній площинах наведені вирази мають бути модифіковані шляхом заміни блокових матриць Q, V та $\tilde{H}_Q$, $\tilde{H}_V$ наступними:

де $Q = \begin{bmatrix} Q_{111}\left(x_{1_{11}}\right) & \cdots & Q_{111}\left(x_{M_{11}}\right) \\ \vdots & \ddots & \vdots \\ Q_{R_{xTG}11}\left(x_{1_{11}}\right) & \cdots & Q_{R_{xTG}11}\left(x_{M_{11}}\right) \\ \hdashline Q_{1TG}\left(x_{1_{TG}}\right) & \cdots & Q_{1TG}\left(x_{M_{TG}}\right) \\ \vdots & \ddots & \vdots \\ Q_{R_{xTG}TG}\left(x_{1_{TG}}\right) & \cdots & Q_{R_{xTG}TG}\left(x_{M_{TG}}\right) \end{bmatrix}$, $V = \begin{bmatrix} V_{111}\left(y_{1_{11}}\right) & \cdots & V_{111}\left(y_{M_{11}}\right) \\ \vdots & \ddots & \vdots \\ V_{R_{yTG}11}\left(y_{1_{11}}\right) & \cdots & V_{R_{yTG}11}\left(y_{M_{11}}\right) \\ \hdashline V_{1TG}\left(y_{1_{TG}}\right) & \cdots & V_{1TG}\left(y_{M_{TG}}\right) \\ \vdots & \ddots & \vdots \\ V_{R_{yTG}TG}\left(y_{1_{TG}}\right) & \cdots & V_{R_{yTG}TG}\left(y_{M_{TG}}\right) \end{bmatrix}$,

$$\tilde{\tilde{H}}_Q = \begin{bmatrix} \tilde{h}_{Q1111_{11}} & \cdots & \tilde{h}_{Q111M_{11}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QR_{xTG}111_{11}} & \cdots & \tilde{h}_{QR_{xTG}11M_{11}} \\ \hdashline \tilde{h}_{Q1TG1_{TG}} & \cdots & \tilde{h}_{Q1TGM_{TG}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{QR_{xTG}TG1_{TG}} & \cdots & \tilde{h}_{QR_{xTG}TGM_{TG}} \end{bmatrix}, \quad \tilde{\tilde{H}}_V = \begin{bmatrix} \tilde{h}_{V1111_{11}} & \cdots & \tilde{h}_{V111M_{11}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VR_{yTG}111_{11}} & \cdots & \tilde{h}_{VR_{yTG}11M_{11}} \\ \hdashline \tilde{h}_{V1TG1_{TG}} & \cdots & \tilde{h}_{V1TGM_{TG}} \\ \vdots & \ddots & \vdots \\ \tilde{h}_{VR_{yTG}TG1_{TG}} & \cdots & \tilde{h}_{VR_{yTG}TGM_{TG}} \end{bmatrix}.$$

Спираючись на отримані математичні моделі відгуків ЦАР у складі наносхеми, демодуляція OFDM сигналів з квадратурно-амплітудною модуляцією та відомими частотами піднесучих і кутовими координатами джерел випромінювання може бути здійснена за виразом $\tilde{\tilde{A}} = \left(P^T P\right)^{-1} P^T U$ з урахуванням просторово-часового чи іншого з різновидів кодування MIMO-сигналів.

Література:

1. Патент України на корисну модель № 60938. МПК H01Q 1/38 (2006.01). Спосіб виготовлення наносхем бездротової мережі на кристалі. / Слюсар Д.В., Слюсар В.І. - Заявка на видачу патенту України на корисну модель № u201103249 від 21.03.2011. - Патент опубліковано 25.06.2011, бюл. № 12.

2. Слюсар В.И. Торцевые произведения матриц в радиолокационных приложениях// Известия вузов. Сер. Радиоэлектроника.- 1998. - Том 41, № 3.- С. 50 - 53.

МЕТОД КОРРЕКЦИИ КВАДРАТУРНОГО РОЗБАЛАНСА

Цыбулев Р.А., Слюсар В.И.
Центральный научно-исследовательский институт вооружения и военной техники Вооруженных Сил Украины
03040, г. Киев, Воздухофлотский проспект, 28
e-mail: swadim@inbox.ru

The given work is devoted to the new method of correction of I/Q unbalance of receivers. This new method use a I/Q demodulators for each quadrature channels. The results of computational modeling are given.

Рассмотренный в [1] метод совместной коррекции квадратурных и межканальных неидентичностей характеристик приемных каналов цифровой антенной решетки (ЦАР) предполагает предварительный расчет корректирующих коэффициентов по контрольному гармоническому сигналу в соответствии с выражением:

$$p1_r = z_r - p_r \cdot t_r, \quad q1_r = q_r \cdot t_r, \quad p2_r = q_r \cdot z_r, \quad q2_r = p_r \cdot z_r + t_r, \quad (1)$$

где q_r, p_r - коэффициенты коррекции квадратурного розбаланса [2], z_r, t_r - коэффициенты коррекции межканальных неидентичностей приемных модулей ЦАР [3].

Собственно процедура коррекции заключается в весовом взвешивании отсчетов АЦП по выходам квадратурных каналов с помощью коэффициентов (1). При этом результат совместной коррекции указанных неидентичностей имеет вид:

$$C_r = \left(\mathrm{A1_r} \cdot p1_r + B2_r \cdot p2_r\right) - \left(B1_r \cdot q1_r - A2_r \cdot q2_r\right),$$
$$S_r = \left(B1_r \cdot p2_r - \mathrm{A2_r} \cdot p1_r\right) + \left(\mathrm{A1_r} \cdot q2_r + B2_r \cdot q1_r\right), \quad (2)$$

где $A1_r$, $B1_r$, $A2_r$, $B2_r$ – напряжения двух соседних во времени отсчетов (с четными и нечетными номерами следования) по выходам АЦП квадратурных аналоговых каналов r-го приемника ЦАР; C_r, S_r – квадратурные составляющие откорректированных напряжений сигналов.

Недостатком метода является использование при формировании откорректированных квадратурных напряжений сигналов C_r, S_r в (2) соседних во времени отсчетов (с четными и нечетными номерами следования) в качестве квадратурных составляющих напряжений сигнальных отсчетов отдельно взятого квадратурного подканала (см. $A1_r$, $B1_r$, $A2_r$, $B2_r$). Такое допущение справедливо только для частоты сигнала f_0, удовлетворяющей условию:

$$f_0 = \frac{4}{(2k-1)} f_d, \quad (3)$$

f_d - частота дискретизации АЦП, k=1; 2;…

В случае допплеровских сдвигов частоты, использования широкополосных сигналов, а также воздействия активных шумовых помех условие (3) невыполнимо, вследствие чего коррекция квадратурного розбаланса выполняется с погрешностью.

Для расширения полосы частот, в которой коррекция квадратурного розбаланса выполнялась бы с допустимой погрешностью, в докладе предлагается новый метод, основанный на выполнении процедуры I/Q-демодуляции сигнальных отсчетов в режиме «скользящего окна» в каждом квадратурном подканале. Структурная схема устройства, реализующего предложенный метод коррекции, представлена на рис.1. Указанная последовательность операций над сигналами может быть выполнена на основе программируемой логической интегральной схемы (ПЛИС), например, типа FPGA фирмы Xilinx. Такой вариант обработки позволяет формировать квадратурные составляющие сигналов $A1_r$, $B1_r$ и $A2_r$, $B2_r$ в широкой полосе частот, ограниченной лишь размерностью демодулятора. В качестве алгоритма I/Q-демодуляции рекомендуется использовать его вариант, изложенный в [4] для 8-отсчетного «скользящего окна», либо обобщение [4] на случай демодуляторов большой размерности, представленное в [5].

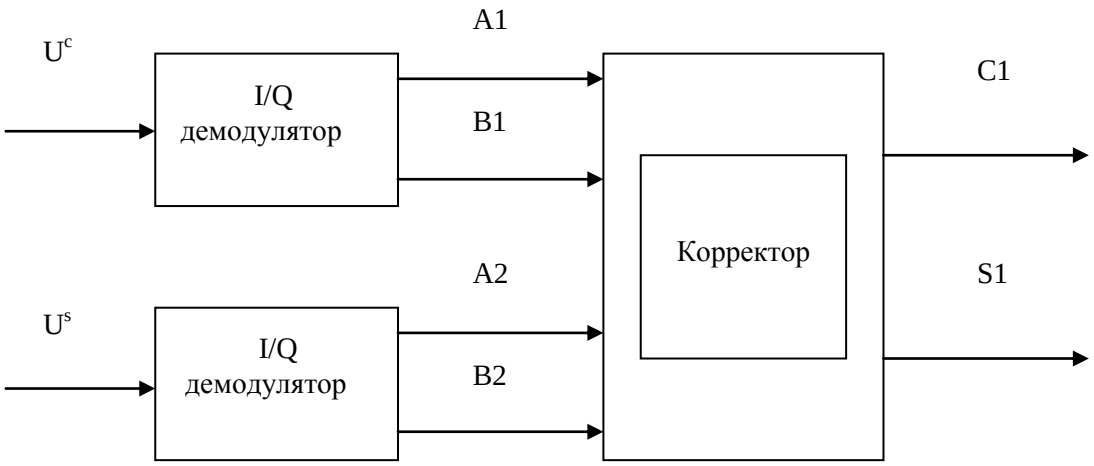


Рис. 1. Квадратурная коррекция отсчетов АЦП

Литература:

1. Слюсар В.И., Цыбулев Р.А. Метод интегрированной коррекции межканальных и квадратурных неидентичностей приемных каналов антенной решетки MIMO.// VII міжнародна науково-технічна конференція студентства і молоді „Світ інформації та телекомунікацій – 2010” (15- 16 квітня 2010 р.). – Київ: ДУІКТ. - С. 52 – 53. – www.slyusar.kiev.ua/DUIKT_kniga_buklet3.pdf.

2. Патент України на корисну модель № 33257. МПК7 G 01 S7/36, H 03 D13/00. Спосіб корекції квадратурного розбалансу з використанням додаткового стробування відліків аналого-цифрового перетворювача. // Слюсар В.І., Масесов М.О., Солощев О.М. - Заявка на видачу патенту України на корисну модель № u200802467 від 26.02.2008. - Патент опубліковано 10.06.2008, бюл. № 11.

3. Слюсар В.И., Покровский В.И., Сахно В.Ф. Патент РФ № 2103768, H01Q3/36, G01R29/10. Способ коррекции амплитудно-фазовых характеристик первичных каналов плоской цифровой антенной решетки. - 1992. - Опубл. 27.01.98, бюл. № 3.

4. Jan-Erik Eklund and Ragnar Arvidsson. A Multiple Sampling, Single A/D Conversion Technique for Demodulation in CMOS.// IEEE Journal of Solid-State Circuits, Vol. 31, No. 12, December 1996. - Pp. 1987 - 1994. - http://iroi.seu.edu.cn/jssc9697/data/31_12_08.PDF.

5. Слюсар В.И., Малярчук М.В., Бондаренко М.В. Методика синтеза I/Q-демодуляторов произвольной размерности.// III-й Міжнародний науково-технічний симпозіум "Нові технології в телекомунікаціях"- (ДУІКТ- КАРПАТИ '2010, с. Вишків). – Київ: Державний університет інформаційно-комунікаційних технологій. - 2 - 5 лютого 2010. - С. 53 - 55. - www.slyusar.kiev.ua/VYSHKIV_2010_2.pdf.

СИНХРОНИЗАЦИЯ СИГНАЛОВ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ НА ОСНОВЕ СИГНАЛЬНОГО ПРОЦЕССОРА

Алексейцев К.Ф., Валковой В.С., Вдовичено Е.И., Дудник Л.А., Жартовский Д.Н., Кузниченко В.С., Нестеров Л.А.
Центральное казённое конструкторское бюро «Протон»
61001, Харьков, ул. Площадь Восстания,7/8, НИО-2, 8(057)732-15-48,
e-mail: proton @ online.kharkov.ua

The radio station meant for the automated backbone radio communication in the short-waves range between combined radio centers, radio posts, and also between radio stations of stationary and mobile basis widely is being used for solving of tactical tasks by all types military units to provide communication to distance 5000 km. Transceiver meant for the noise-protected formalized messages transmitting in the decametric radio waves band during pocketing exchange using automated repeat request (ARQ) in radio routes and with transmitting of voice data in the radio network supplemented by PQRF signals communication is presented in this paper.

Радиотехнические системы связи малой и средней мощности (рис.1,2), предназначенные для организации автоматизированной магистральной радиосвязи в КВ диапазоне между приемо-передающими радиоцентрами, радиопунктами, а также радиостанциями стационарного и мобильного базирования, наряду с зарубежными аналогами, широко используются для решения тактических задач всеми типами военных подразделений требующие обеспечение связи на расстояниях до 5000 км. Условия применимости и характеристики систем дальней телекоммуникационной связи обусловлены их принципом действия. В настоящее время в средствах радиосвязи всё большую популярность приобретает тип передачи сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ). Основной отличительной особенностью этого типа радиосигнала является то, что несущая частота периодически меняется в псевдослучайной последовательности, которая определяется исходным ключом на станциях передачи и приёма. Основная сложность задачи обнаружения сигналов с ППРЧ в КВ диапазоне заключается в выделении узких временных отрезков сигнала (порядка 0.05 сек) малой шириной спектра (порядка 2.4 кГц) в широком диапазоне спектра (порядка 100 кГц). Данная задача усложняется тем, что из-за передачи в широкой полосе частот возможна неоднородность шума в этой полосе и наличие посторонних, постоянно работающих источников радиоизлучения [1]. В зависимости от типа выбранной рабочей полосы, имеется возможность совместной работы с КВ системами связи, использующими относительную фазовую модуляцию. Система синхронизации сигналов ППРЧ состоит в следующем [2]. На приёмной и передающей стороне генератор случайных чисел формирует псевдослучайную последовательность вид которой, определяется задаваемым эталонным временем работы. Расхождение во времени между приемной и передающей станциями может составлять не более 2 мин. Система эталонного времени действует в составе такой системы с 2005 по 2100 года. После запуска генератора псевдослучайной последовательности, алгоритм на основе текущего вре-

Рис. 1- Малогабаритная помехозащищённая КВ-радиостанция

Рис. 2 – Помехозащищённая КВ радиостанция средней мощности

мени и исходного ключа выдает синхропоследовательность (СП) длиной 63 бита. На установленной центральной частоте передатчик на протяжении 1250 мсек посылает данную СП на 10 заданных частотах. Приемник принимает СП только лишь на одной из этих частот за время 125 мсек. Так передатчик работает на 10 частотах до тех пор, пока приемник не выработает прием СП на 8 из этих 10 частот. При этом, вероятность приёма данной СП на одной из принимаемых частот в 8 раз. Затем передатчик совместно с приемником работают одновременно на полученных псевдослучайных 10 частотах, при котором передатчик выдает приемнику рассчитанную скорость и глубину перемежения пакетов для передачи данных. После получения приемником этих двух величин обе системы засинхронизированы. Далее обе системы переходят в рабочий режим передачи пакетных данных по алгоритму защищенной передачи данных.

Общее время входа в синхронизм двух систем составляет не более 15 сек. Данный алгоритм связи с использованием сигналов ППРЧ реализован на сигнальном процессоре ADSP 2191 и модуляции сигналов на основе квадратурного цифрового повышающего конвертора. Прием данных осуществляется с помощью АЦП AD7677 с дальнейшей обработкой сигналов в ADSP 2191. На рис.3 и рис.4 представлены структурные схемы передающей и приёмной части системы, использующей сигналы ППРЧ.

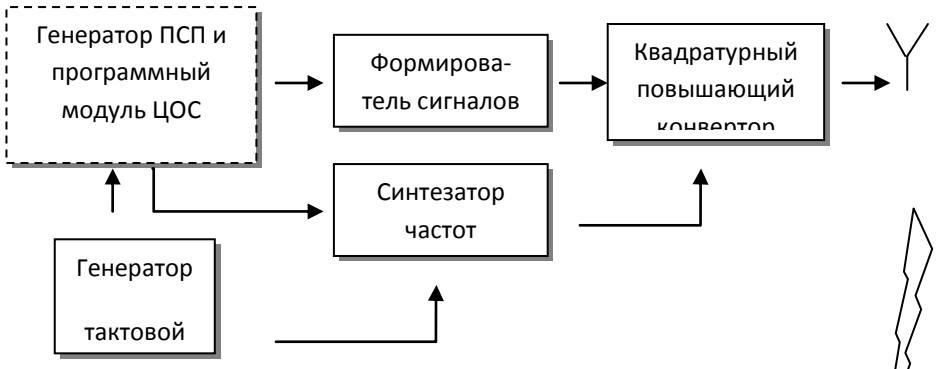


Рис. 3 – Передающая часть системы ППРЧ

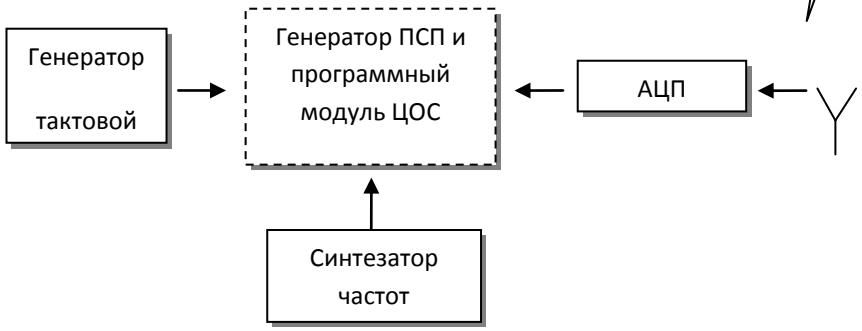


Рис. 4 – Приёмная часть системы ППРЧ

Перечень ссылок:

1. Устюжанин К.В., Ланских В.Г., Крашенинников К.Н. ОБНАРУЖЕНИЕ СИГНАЛОВ ППРЧ В КВ ДИАПАЗОНЕ // III Международная научная конференция «Современные проблемы информатизации в системах моделирования, программирования и телекоммуникациях», с.62

2. Ерохин Виктор Фёдорович

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ВХОДНОГО СИГНАЛА РЕТРАНСЛЯЦИОННОГО ИЗМЕРИТЕЛЯ ЦИФРОВЫМИ МЕТОДАМИ

Величко Д.А., Вдовичено Е.И.
Центральное казённое конструкторское бюро «Протон»
61001, Харьков, ул. Площадь Восстания,7/8, НИО-2, 8(057)732-15-48,
e-mail: proton @ online.kharkov.ua

Один из способов совершенствования ретрансляционного измерителя и повышения его качества состоит в повышении подавления паразитных компонент спектра преобразованного сигнала. Однако реализация такого способа затруднена тем, что частотный разнос между компонентами спектра входного сигнала ретрансляционного измерителя весьма мал. Решить такую задачу можно на основе цифровой обработки входного сигнала, преобразованного к промежуточной частоте. Поэтому в данной работе исследуются методы преобразования входного сигнала ретрансляционного измерителя, формирование цифровых массивов его параметров, выделение информации из этих массивов и некоторые результаты статистической обработки. Исследования проводились методами имитационного моделирования.

При исследованиях, как и в работе [1], использовались непрерывные, немодулированные сигналы и радиоволны миллиметрового диапазона. Переход к широкополосному сигналу может быть реализован так, как это было сделано в [1] – методом переключения частоты непрерывного немодулированного колебания. В этом случае из ансамбля параметров, извлекаемых при работе на разных частотах, составляется информационная картина о контролируемом объекте.

Формирование излучаемого колебания и колебания гетеродина, преобразование волн на трассе распространения и при отражении от контролируемого объекта выполнялось с помощью математического аппарата, использованного в [2]. На рис.1 представлена функциональная схема ретрансляционной системы. На ней обозначено: 1,5 – задающие генераторы излучаемого колебания и гетеродина; 2,6 – умножители излучаемого колебания и гетеродина; 3,7 – полосовые усилители излучаемого сигнала и гетеродина; 4,8 – направленные ответвители; 9,12 – смесители радиолокационного датчика и контрольного сигнала; 10,13 – полосовые усилители

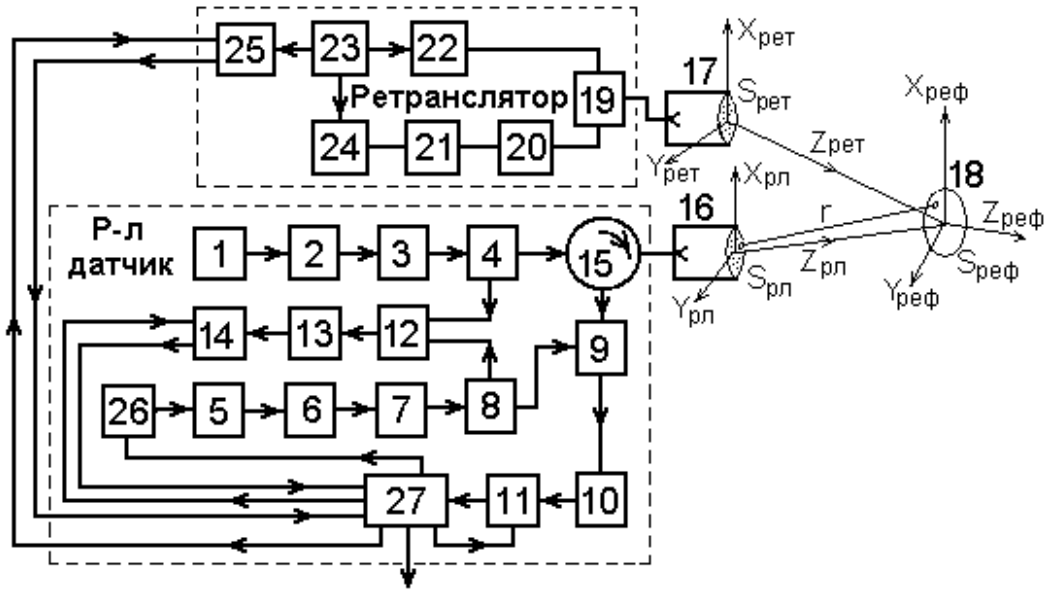


Рис.1 – Функциональная схема ретрансляционной системы

промежуточной частоты; 11,14,25 – АЦП сигналов; 15 – циркулятор; 16,17 – антенны радиолокационного датчика и ретранслятора; 18 – контролируемый объект; 19 – разветвитель – сумматор; 20 – СВЧ фазосдвигатель $\Delta\varphi_{mw} = \pi/4$; 21,22 – рефлекторы СВЧ сигнала; 23 – генератор сдвига; 24 – НЧ фазосдвигатель на $\Delta\varphi_{Rf} = \pi/2$; 26 – блок управления колебаниями гетеродина; 27 – устройство обработки и управления.

При моделировании считалось, что в ретрансляторе сигнал сдвигается по частоте фазокомпенсационным способом, как и в [1]. Отражатели 21 и 22 (рис.1) модулируются гармоническими колебаниями, имеющими круговую частоту Ω_{sh} и начальные фазы φ_{sh} и $\varphi_{sh}+\Delta\varphi_{Rf}$. Коэффициенты амплитудной модуляции отражателей различны. Модулированные в отражателях сигналы поступают в разветвитель–сумматор 19 и ретранслируются в направлении на контролируемый объект 18 (рис.1).

Входной сигнал на выходе антенны радиолокационного датчика содержит все спектральные компоненты ретранслируемого сигнала. Информационный параметр содержится в каждой гармонике спектра принятого сигнала и его можно извлечь из любой гармоники. Полоса частот, занимаемая одной гармоникой, зависит от продолжительности зарегистрированного массива входной информации.

Реальный аналоговый входной сигнал миллиметрового диапазона не удается преобразовать в цифровой код. Поэтому вначале его нужно преобразовать к промежуточной частоте и усилить до уровня, при котором микросхемы могут эффективно выполнять аналого-цифровое преобразование. В соответствии с функциональной схемой преобразование выполняется колебанием гетеродина. Преобразованный аналоговый сигнал имеет вид

$$e_{пр}(t)=U_{пр}(t)\cdot\cos\left[\omega_{пр}(t)\cdot t+\varphi_{рл}^{(\text{вх})}(t)-\varphi_{гет}\right], \quad (1)$$

где $U_{пр}(t)$ – амплитуда колебания на выходе полосового усилителя промежуточной частоты, $\omega_{пр}(t)=\omega_{рл}^{(вх)}(t)-\omega_{гет}$ – круговая промежуточная частота.

Сигнал промежуточной частоты на всем измерительном интервале $T_{изм}$ подвергается дискретизации с помощью АЦП, в этом виде он может быть записан [3]

$$s_{дискр}(t)=\sum_{k=0}^{k=N} s(k\cdot\tau)\cdot\delta(t-k\cdot\tau), \quad (2)$$

где τ – интервал между соседними дискретными точками измерений мгновенных значений напряжения; $N=T_{изм}/\tau$ – количество точек измерения на измерительном интервале; $\delta(t-k\cdot\tau)$ – дельта функция. Значения $s_{дискр}(t)$ записываются в динамический массив для дальнейшей цифровой обработки.

Обработка состоит в определении спектральной составляющей, которая содержит информацию о преобразованиях радиоволны на трассе распространения и в ретрансляторе. При числе отсчетов $N+1$ коэффициенты Фурье $a_{дискр(\omega)}$ и $b_{дискр(\omega)}$ спектральной составляющей с частотой ω дискретизированного сигнала можно выразить

$$a_{дискр(\omega)}=\frac{2}{N+1}\cdot\sum_{k=0}^{N} s_{дискр}(k\tau)\cdot\cos\omega t\ ,\quad b_{дискр(\omega)}=\frac{2}{N+1}\cdot\sum_{k=0}^{N} s_{дискр}(k\tau)\cdot\sin\omega t\ . \quad (3)$$

При этом спектральная составляющая с частотой ω имеет вид

$$e_{filtr}(t)=U_{filtr}\cos\left(\omega\cdot t+\psi_{filtr}\right), \quad (4)$$

где $U_{filtr}=\sqrt{a^2_{дискр(\omega)}+b^2_{дискр(\omega)}}$, $\psi_{filtr}=arctg\left(b_{дискр(\omega)}/a_{дискр(\omega)}\right)$.

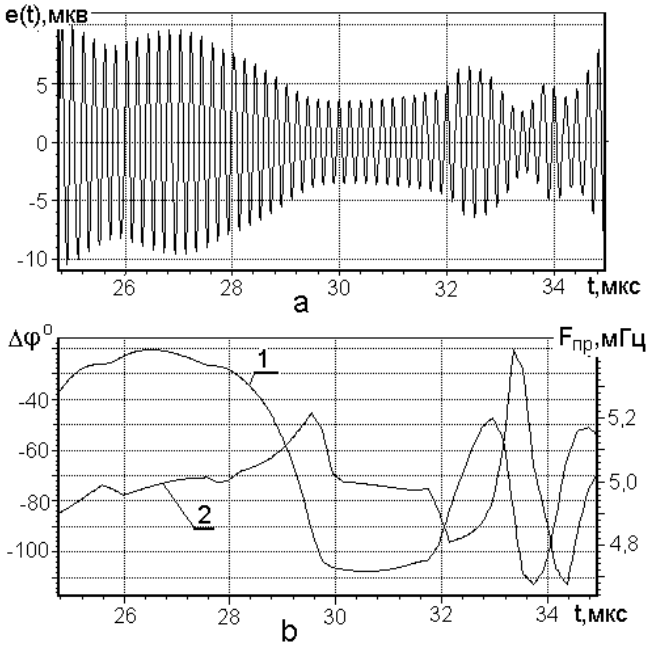
При воздействии шума на входе радиолокационного датчика входной сигнал имеет вид

$$e_{рл\Sigma+N}^{(\text{вх})}(t)=U_{рл}^{(\text{вх})}(t)\cdot\cos\left[\omega_{рл}^{(вх)}(t)\cdot t+\varphi_{рл}^{(\text{вх})}(t)\right]+U_{n}^{(вх)}(t)\cdot\cos\left[\Phi_{n}^{(вх)}(t)\right], \quad (5)$$

где первое слагаемое – детерминированный входной сигнал, $U_{n}^{(вх)}(t)$, $\Phi_{n}^{(вх)}(t)=\omega_n(t)\cdot t+\varphi_n(t)$ – случайные независимые функции амплитуды и полной фазы

шумового колебания соответственно [4], $\omega_n(t)$, $\varphi_n(t)$ – случайные функции круговой частоты и фазы шумового колебания.

Случайная реализация временной зависимости мгновенных значений сигнала и шума на промежуточной частоте, где присутствуют все спектральные компоненты принятого сигнала, имеет вид, представленный на рис.2a. На рис.2b показаны случайные реализации временной зависимости отклонения фазы от линейного закона (кривая 1), вычисленные с учетом всего зарегистрированного интервала [5], и реализация временной зависимости мгновенной частоты от времени (кривая 2). На рис.2a и 2b представлен небольшой участок общего интервала смоделированного входного сигнала от 25мкс до 35мкс. Его полная длительность составляет $T_{изм} = 10000 мксек$. Центральное значение частоты преобразованного сигнала $F_{пр} = 5 МГц$



a – мгновенные значения напряжения
b – отклонения фазы и частоты

Рис.2 – Участок зависимости суммы входного сигнала и шума от времени.

Существующая элементная база фирм Analog Devises, Altera, Texas Instruments и возможности обработки с помощью цифровых процессоров обработки сигналов позволяют увеличить промежуточную частоту до значений свыше сотни мегагерц. Однако время обработки при этом будет увеличиваться, так как будет увеличиваться количество точек в динамических массивах, содержащих параметры колебания.

Спектральная плотность входных шумов при моделировании была принята равной $4 \cdot 10^{-20}\ Вт/Гц$, что соответствует коэффициенту шума 10дБ. Ширина шумовой полосы пропускания усилителя промежуточной полосы оказывалась около 0,5МГц.

В сумме сигнала и шума детерминированная часть входного сигнала не изменялась. Однако в каждом опыте изменялись реализации шумовых колебаний. Спектральная плотность шума оставалась постоянной. При этих условиях были получены распределения амплитуды и фазы отфильтрованной гармоники. На рис.3 показаны распределения амплитуды входного сигнала, на рис.4 – фазы. Кривой 1 на этих рисунках обозначены экспериментальные плотности вероятностей, кривыми 2 – плотность нормального закона распределения. В соответствии с методом моментов [4] параметры нормального распределения были приравнены значениям, полученным в ходе имитационного эксперимента. Экспериментальные распределения были получены по 5000 массивов сигнала и шума, 0,001 часть одного из которых показана на рис.2. Амплитуда сигналов на рис.3 приведена к входу радиолокационного датчика. В результате обработки по каждому массиву было получено колебание, отфильтрованное программно с помощью цифровых процедур.

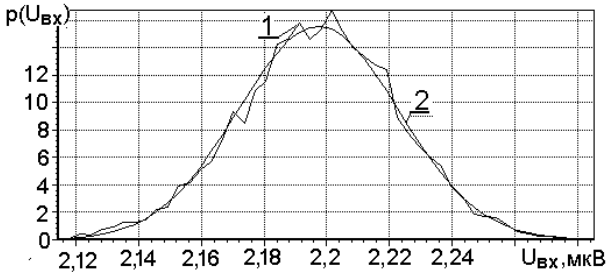


Рис.3 – Распределение амплитуды входного сигнала

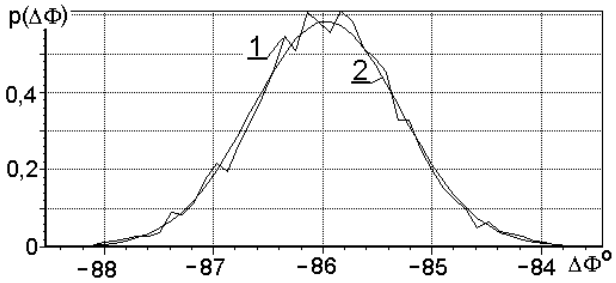


Рис.4 – Распределение фазы входного сигнала

Как видно из приведенных графиков, экспериментальные распределения хорошо совпадают с нормальным законом, как в интенсивной части, так и на «хвостах».

На основании полученных результатов с помощью общеизвестных формул для ошибок измерения амплитуды суммы сигнала и шума с нормальным распределением можно определить соотношение сигнал/шум на выходе цифровой системы обработки принятого сигнала; оно составляет около 40 дБ. Оценка шумовой компоненты колебания, выполненная на основе принятой при имитационном моделировании плотности шума, эквивалентной полосы пропускания и входном сопротивлении, практически совпадает с полученным в опытах значением. Сравнение результатов определения фазового набега представленным методом с результатами работы [1] показывает, что при цифровой обработке преобразованного входного сигнала ретрансляционного измерителя достигнуто существенное, в несколько раз снижение погрешностей.

Таким образом, использование цифровой обработки преобразованного входного сигнала ретрансляционного измерителя и переход к селекции полезной компоненты спектра цифровыми методами позволяет существенно повысить точность измерения ретрансляционной системы, близкий к потенциально достижимому значению.

Литература:

1. Величко А.Ф., Величко Д.А., Курбатов И.В. Фазовые соотношения и способ снижения погрешностей измерения многочастотных ретрансляционных систем // К.: Известия вузов «Радиоэлектроника». 2005. №5. С.57–67.
2. Величко А.Ф., Величко Д.А., Вдовиченко Е.И Определение усредненной разности фаз и разности частот в ретрансляционных измерителях // Радиотехника. – 2011. – Вып. 164. – С. 21 – 29
3. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах. – М., «Сов. радио», 1975, 208 с.
4. Свешников А.А. Прикладные методы теории случайных функций // изд.2-е // М., Изд. «Наука», Главная ред. Физ.-мат. литературы, 1968, 463 с.
5. Величко А.Ф., Величко Д.А., Вдовиченко Е.И. Определение усредненной разности фаз и разности частот в ретрансляционных измерителях // Радиотехника. – 2011. – Вып. 164. – С. 21 – 29.

ТЕСТИРОВАНИЕ XPD – CPA МОДЕЛЕЙ

Ельченко С.В.
ООО “ЭкостарУкраина”
61145, г. Харьков, ул. Новгородская 11а,
E-mail: elchenko@ukr.net тел.: 050-212-09-85

The present work considers testing results of models describing the correlation between cross-polarization discrimination and co-polar attenuation due to rain.

В процессе анализа результатов измерений обнаружена корреляционная связь между кросс-поляризационной избирательности и затуханием, вследствие воздействия на канал связи гидрометров в виде дождя. В следствии чего, выведены несколько математических выражений связывающих XPD и CPA ("Cross-Polarization Discrimination" и "Co-Polar Attenuation"). Выражения XPD и CPA корреляции выведены при использовании теории рассеивания в дождевой капле и моделей распределения размеров и формы дождевой капли. На сегодняшний день существует несколько моделей, описывающих корреляционную связь между XPD и CPA, наиболее широкое применение нашли следующие модели:

1) ITU-R Model [ITU-R, 1997].
2) Dissanayake, Haworth, Watson analytical model (DHW) [Dissanayake et al., 1980]
3) Chu Model [Chu, 1982]
4) Stutzman and Runyon model (SR) [Stuzman and Runyon, 1984]
5) Nowland, Sharofsky and Olsen (NOS) model [Nowland et al., 1977]
6) Van de Kamp Model [Van de Kamp, 1999]
7) Fukuchi Model [Fukuchi, 1990].

Тестирование моделей UTI-R, Fukuchi и DHW, было проведено при использовании параметров спутников Olympus и Hot Bird 8. Измерения со спутника Olympus были выполнены в Эйндховене, Нидерланды, и в Лувен-ля-Нёве, Бельгия. Измерения со спутника Hot Bird 8 были выполнены в Харькове, Украина.

В таблице 1 представлены параметры приемных станций, спутников Olympus и Hot Bird 8, которые необходимы для тестирования моделей UTI-R, Fukuchi и DHW.

Таблица 1. Параметры, используемые для тестирования моделей UTI-R, Fukuchi и DHW.

Дислокация приемной станции	Частота, GHz	Угол возвышения	Вид поляризации	Угол наклона	Период измерений
Эйндховен	12.5	26.7	линейная	71.6	01/01/1991–31/07/1992
Лувен-ля-Нёв	12.5	27.8	линейная	71.1	01/01/1992–31/12/1992
Харьков	12.015	28.6	линейная	108.28 (-71.72)	01/03/2010–01/05/2011

Погрешность моделей относительно измерений, $\varepsilon(p) = XPD(модель) - XPD(измерения)[dB]$, рассчитана как функция годового процентного отношения. Средняя погрешность $\langle \varepsilon(p) \rangle$, среднеквадратическое значение $\sqrt{\langle \varepsilon^2(p) \rangle}$ и среднеквадратическое отклонение σ представлено в таблице 2.

Таблица 2. Погрешность моделей UTI-R, Fukuchi и DHW относительно измерений.

Дислокация приемной станции	Модель	$\langle \varepsilon(p) \rangle$, dB	$\sqrt{\langle \varepsilon^2(p) \rangle}$, dB	σ, dB
Эйндховен	ITU-R	2.125	2.498	1.314
	DHW	4.169	4.658	2.077
	FUK	-4.0880	4.614	2.139
Лувен-ля-Нёв	ITU-R	1.39	2.297	1.827
	DHW	3.5	4.414	2.163
	FUK	-4.071	4.200	1.03.
Харьков	ITU-R	4	4.26	2.19
	DHW	6.2	6.88	5.21
	FUK	-2.6	2.73	2.06

На рис.1 представленна взаимосвязь между кросс-поляризационной избирательностью и затуханием вследствие дождя, для моделей UTI-R, DHW, FUK и измерений в Харькове, Эйдховене. Из графического отображения наглядно видно, что функции $XPD = f(CPA)$ имеют отличия обусловленые погрешностью моделей и измерительного оборудования.

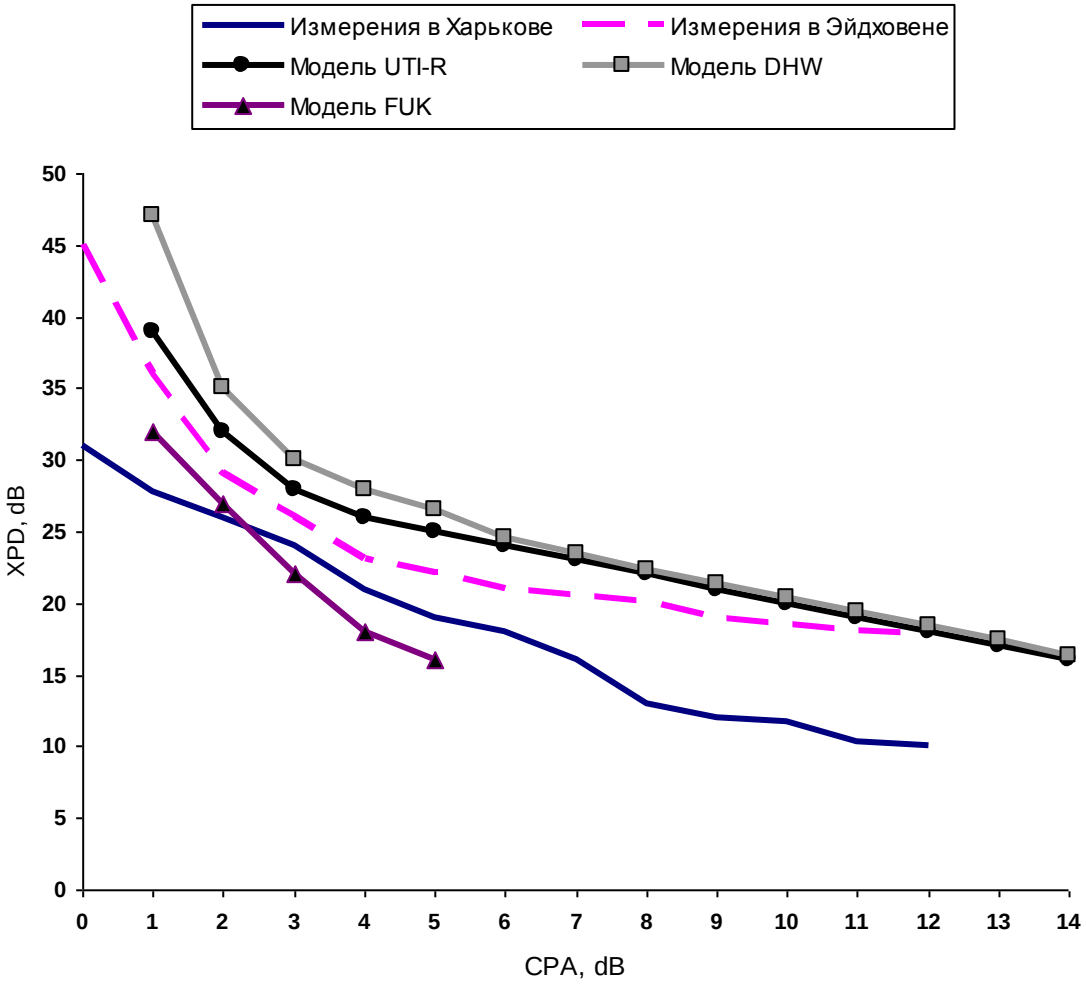


Рис.1. Графическое изображение измерений в Харькове, Эйдховене и моделей UTI-R, DHW, FUK корреляционной связи между XPD и CPA вследствие влияния гидрометеоров в виде дождя.

Рассмотренные модели отображают корреляционную связь между XPD и CPA вследствие воздействия на канал спутниковой связи гидрометеоров в виде дождя. Графическое изображение моделей, на рис.1, наглядно показывает сходство с практическими измерениями, с учетом погрешности. Погрешности указаны в таблице 2, в результате тестирования моделей и сравнения с практическими измерениями. Наиболее близка модель ITU-R к измерениям произведенным в Эйндховене и Лувен-ля-Нёве, среднеквадратическое значение погрешности составляет 2.498 dB и 2.297 dB соответственно. Данная погрешность вызвана неточностью модели и погрешностью измерительного оборудования.

Следует отметить, что модель FUK, основанная на сравнении равновероятного отношения между кросс-поляризационной развязкой и затуханием при использовании статистических данных, наиболее близка к измерениям произведенным в Харькове и значение среднеквадратической погрешности составляет 2.498 dB. Данная модель проверена измерениями, выполненными в Японии в рамках ETS-II и SSE экспериментов, с хорошей точностью на 11.5 GHz (линейная и круговая поляризация) и с постоянным занижением в 6 dB на частоте 34 GHz. Представляется целесообразным дальнейшее использование модели Fukuchi в дальнейших иследованиях.

Литература:

1. Поповский, В.В. Электромагнитная доступность источников радиоизлучения / В.В. Поповский – ВАС,1987 – 262 с.

2. Chu, T. S. A semi-empirical formula for microwave depolarisation versus rain attenuation on earth-space paths/ T. S. Chu // IEEE Trans. Commun. — 1982. — Vol. 30, №12, pp 2550-2554.

3. Fukuchi, H. Prediction of depolarisation distribution on earth-space paths / H. Fukuchi // IEE Proceedings. –1990. – Vol.137, №6.

4. Van de Kamp, M. Depolarisation due to rain: the XPD-CPA relation / M. Van de Kamp // Int. J. Sat. Com. – 2001. – Vol. 9, № 3, pp. 285-301.

5. Dissanayake, A. W., Haworth, D. P., Watson, P. A. Analytical models for cross-polarisation on earth space radio paths for frequency range 9-30 GHz/ A. W. Dissanayake, D. P. Haworth, P. A. Watson // Ann. Telecommunication. — 1980. — Vol. 35, №11-12, pp 398-404.

6. Hogers, R., Herben, M., Brussaard, G. Depolarisation analysis of the 12.5 and 30 GHz Olympus beacon signals/ R. Hogers, M. Herben, G. Brussaard // Proc. 1st OPEX Workshop, ESTEC, Noordwijk, The Netherlands. – 1991. – pp. 2.4.1-2.4.12.

СИСТЕМА БЕСПРОВОДНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ УСЛУГАМ

Казимиренко В.Я.[1], Нарытник Т.Н.[2]
[1]Национальный технический университет Украины «КПИ»
[2]СП «Институт электроники и связи Украинской академии наук»
E-mail: vkazim2@gmail.com[1], director@mitris.com.[2]

The task of providing user access to information services in Ukraine is very serious. The article proposes a technical solution that enables secure access multiservice (access to digital television and related services that are based on data) to the population across the country.

Введение

Проблема предоставления информационных услуг на территории Украины является актуальной задачей. Если в больших городах и некоторых районных центрах проблема коммуникаций в принципе решена с помощью развертывания оптоволоконных первичных сетей, то в периферийных районных центрах и практически на всех сельских территориях есть в основном лишь телефонные сети общего пользования, пропускная способность которых не позволяет обеспечить качественный доступ к информационным ресурсам населению этих территорий. Это также не дает возможность развернуть предоставление услуг дистанционной учебы, профессиональных консультаций и т. п.

Таким образом, важной задачей становится предоставление доступа к информационным услугам, прежде всего, населению сельских районов, путем выбора оптимального способа передачи информации в зоне обслуживания.

Общая конфигурация зоны обслуживания (ЗО) представляет собой совокупность зон с двумя типами застройки. Это территория с городской и пригородной застройкой - зона обслуживания первого типа (ЗО1) и с сельской застройкой - зона обслуживания второго типа (ЗО2). В ЗО1 условия передачи включают у себя как наличие отраженных лучей (каналы модели Райса - принятие основного луча при наличии отраженных; и каналы модели Релея - принятие отраженных лучей (при отсутствии основного), так и прием в условиях прямой видимости (канал модели Гаусса). В ЗО2 условия передачи обычно ограничиваются каналом модели Гаусса.

То есть, целью работы является разработка системы для предоставления абонентам беспроводного доступа к информационным ресурсам. Поскольку актуальной задачей является покрытие услугами небольших городов, поселков с прилегающими территориями (в больших городах обычно есть сети разного типа – кабельные, эфирные и другие), то система, которая предлагается, должна отвечать следующим требованиям:

- обеспечивать максимально полное покрытие зоны обслуживания, которая включает у себя территорию с городской застройкой радиусом до 10...12 км (может включать у себя каналы модели Релея, Райса) и зону пригородной застройки и сельскую (канал модели Гаусса). При этом суммарный радиус ЗО желательно иметь до 50…60км;
- позволять расширение зоны обслуживания как по размеру, так по полноте охвата пользователей в ЗО путем выбора способа передачи.

Согласно этому техническому решению система беспроводной передачи данных (СБПД) состоит из подсистемы DVB - S и подсистемы 802.16. Эта система, в зависимости от конфигурации, может включать в себя также подсистему телевизионного вещания и системный сервер, обеспечивающий доступ к внешним информационным и коммуникационным службам, отвечающий за организацию и поддержание подсетей, коммутацию информационных потоков в подсети.

Характеристики подсистемы DVB-S

Подсистема *DVB-S* базируется на системе телерадиоинформационной интегрированной микроволновой «Митрис-ИНТ» БЯФИ.464423.118.

Подсистема предоставляет доступ к информационным ресурсам, обеспечивая в зависимости от исполнения прием и передачу:

– прямой канал по стандарту DVB-S;

– обратный канал по специально разработанному протоколу.

Частотный диапазон прямых и обратных каналов определяется полученными разрешениями и как правило находится ориентировочно внутри диапазона 10…15ГГц.

Разнос центральных частот прямых каналов составляет 40 МГц, а обратных не более 3,5 МГц. При этом ширина спектра сигнала прямых каналов по уровню 3дБ в пределах 40 МГц, а обратных – в пределах 3,5 МГц.

Зона обслуживания разбивается на секторы (до 12), в каждом из которых размещаются абонентские станции (АС), число которых зависит от используемого частотного диапазона, требуемой скорости передачи, предоставляемой одному абоненту.

В зависимости от конфигурации прямой канал может доставляться ко всем АС в обслуживаемых секторах либо с помощью одной антенны с круговой диаграммой направленности, либо с помощью секторных антенн, обслуживающих каждая один либо несколько секторов.

Мощность сигнала на выходе передатчиков центральной (ЦС) и АС устанавливается в зависимости от полученного оператором разрешения, размера ЗО, ситуации на трассе. Реально устанавливаемые мощности не более 4Вт и 10мВт на выходе каждого передатчика прямого канала ЦС и АС, соответственно.

Доступ АС по обратному каналу реализуется с использованием технологии TDMA. Число временных слотов на один частотный канал составляет 127. Причем один слот выделяется для организации подключения АС.

Число прямых каналов зависит от используемой полосы частот и от числа секторов. В случае одной всенаправленной антенны число прямых каналов может достигать 20. Максимальная пропускная способность одного прямого канала 34 Мбит/с. Максимальная суммарная пропускная способность прямых каналов зависит от конфигурации и может достигать 1360 Мбит/с.

Максимальное число временных слотов, выделяемых одной АС – 127 и может динамически регулироваться от долей слота до максимума. Максимальная пропускная способность обратного канала, соответствующая одному слоту составляет не менее 20 Кбит/с. Учитывая реальную ситуацию (практическое отсутствие коммуникационной инфраструктуры в сельских районах, сравнительно малое ожидаемое число абонентов, их рассредоточенность и пр.), для передачи в прямом канале выбран протокол DVB-S. Использование такого протокола позволяет реализовать зону покрытия в Гауссовом канале радиусом до 50…60 км одной центральной станцией.

Характеристики подсистемы 802.16.

Подсистема 802.16 обеспечивает предоставление услуг абонентам в условиях городской, пригородной застройки (каналы моделей Райса, Релея, Гаусса). Подсистема создана на базе системы WiMax с полной поддержкой протокола 802.16 (конфигурация регламентированная как WiMax). Базовая система (ЖНКЮ.464429.018) указанной подсистемы проходила испытания в г. Томск (Россия). Система работала в диапазоне 5725…6425 МГц.

Не вдаваясь в описание стандарта, отметим реализованные характеристики, критичные для применения при реализации требуемого покрытия.

Ширина полосы излучаемого сигнала может назначаться оператором программно: 1,75 МГц; 3,5 МГц; 7,0 МГц или 10 МГц. Пропускная способность канала связи прямо пропорциональна ширине полосы сигнала.

На пропускную способность абонентского канала связи оказывают влияние несколько факторов:

- тип дуплексирования (временное / частотное);
- ширина канала (1,75 МГц; 3,5 МГц; 7,0 МГц или 10 МГц);
- расстояние до базовой станции и общая помеховая обстановка в зоне приема;
- наличие прямой видимости.

При изменении качества связи: вследствие изменения погодных условий или условий распространения сигнала, вызванных многолучевой интерференцией, базовая

станция автоматически снижает или повышает степень модуляции индивидуально для каждого абонента, обеспечивая при этом требуемый пороговый уровень ошибок в канале.

Пропускная способность 37,5 Мбит/с в полосе 10 МГц обеспечивается при хорошем качестве канала связи и модуляции QAM-64. На максимальном удалении от базовой станции при модуляции BPSK-1/2 максимальная пропускная способность составит примерно 4 Мбит/с.

Расчетные значения зон покрытия для прямой и непрямой видимости показаны на рисунке 1 а) и 1 б) соответственно.

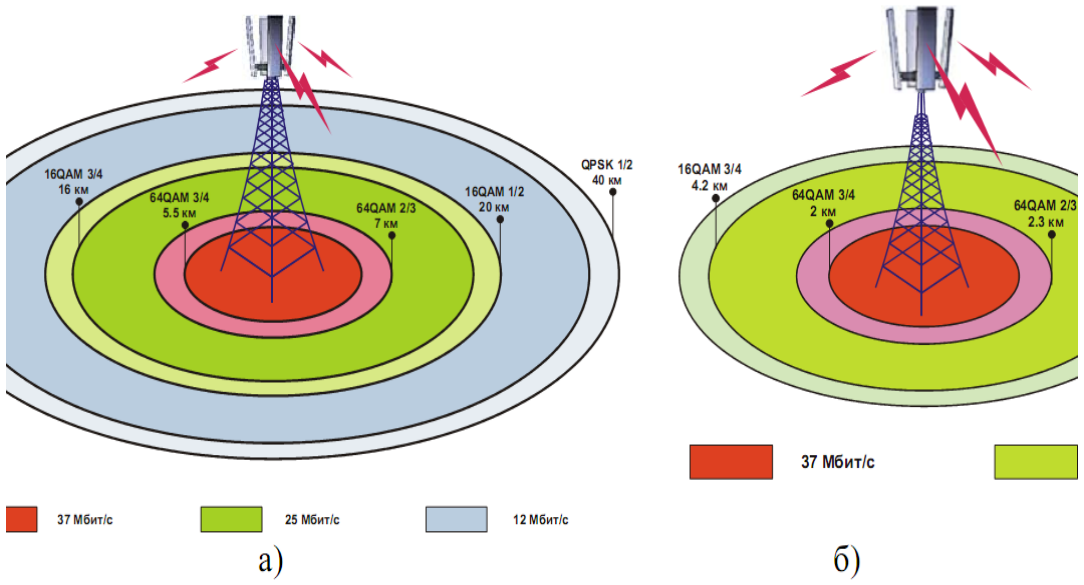


Рис.1. Зоны покрытия: а – при прямой видимости; б – при работе на отражениях

Характеристики подсистемы телевизионного вещания

Подсистема базируется на системе отечественной разработки БЯФИ 464423.118 (технические условия ТУ У 32.2 – 19123337-14-2004). Система прошла испытания в базовом варианте при эксплуатации в ряде регионов Украины и в варианте подсистемы в образце, поставленном в Кувейт.

Передача ведется по стандарту DVB-S, то есть согласуется с протоколом в прямом канале подсистемы DVB-S и возможно разделение между этими подсистемами, как частотного диапазона, так и линейных трактов передатчика и приемника прямого канала.

Помехоустойчивость этой подсистемы практически равна помехоустойчивости подсистемы DVB-S, что позволяет предоставлять услуги на одинаковых территориях. То есть зоны покрытия этих подсистем совпадают.

Возможности системы в целом

Указанная система позволяет решить вопрос покрытия территории Украины предоставлением услуг, базирующихся на передаче данных и цифрового телевидения как по каналу модели Гаусса, так по каналам Райса и Релея, т.е. обслуживать абонентов на территории с сельской застройкой и с городской и пригородной. Таким требованиям отвечают территории, включающие, например, районный центр и прилегающие к нему села. Районный центр вполне может обслуживаться с достаточным качеством и информационной емкостью в радиусе до 5…8 км.

Территория, прилегающая к районным центрам, может обслуживаться на расстоянии до 50…60км от ЦС.

Важным вопросом является расширение зоны покрытия подсистемами DVB-S и телевизионного вещания.

Расширение зоны покрытия должно приводить, во первых, к минимальному удорожанию системы и минимальному увеличению используемого частотного ресурса. Для этого рекомендуется использовать создание дополнительных зон покрытия посредством ретрансляции из основной зоны в дополнительную ЗО. Такое расширение реализуется посредством ретрансляционных станций, излучающих на той же частоте, что и в основной ЗО.

Во вторых, нужно обеспечивать максимальное совпадение ЗО и ЗП (зоны покрытия). Несовпадение может вызываться недопустимым влиянием взаимных помех от передатчиков различных ЗП, нелинейными искажениями, за счет излишне большого уровня сигнала на входе АС, который не компенсируется системой АРУ (автоматического регулирования усиления).

И хотя первый тип искажений при одночастотной модуляции полностью исключить часто не удастся, применение модуляции QPSK позволяет получить максимальную помехоустойчивость и помехозащищенность канала связи. Т. е. требуемое качество реализуется при минимальном значении отношения сигнал/шум (С/Ш) и при максимальном значении отношения сигнал/помеха (С/П) на входе приемника АС.

При разработке системы был предложен простой алгоритм разворачивания сети, позволяющий уменьшить число участков, подверженных искажениям первого типа.

Предложен также способ, позволяющий практически полностью исключить второй из указанных выше искажений, который в климатических условиях Украины полностью исключает влияние таких искажений, вызванных большим разбросом протяженностей каналов связи (от ЦС до самой удаленной АС и от ЦС до самой близкорасположенной АС). Разброс уровней сигнала на входах этих АС при радиусе ЗП 60км может достигать около 55дБ, что не компенсируется АРУ приемника.

Заключение

1. Данное техническое решение, система беспроводной передачи данных, базирующаяся на отечественных разработках, позволяет решить задачу обеспечения доступа к информационным ресурсам абонентов на территории Украины.

2. Области применения разработанного технического решения в образовании могут быть следующие:

- получение информации об учебном заведении, его образовательных программах, специальностях, условиях обучения и т.п.;
- получение через Интернет методических материалов;
- реализация дистанционного обучения через Интернет (двусторонняя связь учебного заведения со своими студентами);
- интерактивное тестирование знаний учащихся и студентов через Интернет;
- предоставление учебным заведением различных информационных сервисов своим студентам и сотрудникам (текущая информация, расписание, доски объявлений, форумы, электронная почта);
- архивные функции (хранение студенческих курсовых и дипломных работ в электронном виде, иной документации);
- доведение информации к пользователям на территории страны.

USING KALMAN FILTERING IN SOLVING ADAPTIVE MODULATION PROBLEMS IN MIMO CHANNELS

Loshakov V., Prof., Z.Vadia, Ms
Kharkov national technical university of radio electronics
(61166, Kharkov, Linen street,14, dep. Telecommunication system, tele. (057) 702-13-20),
E-mail: tkc@kture.kharkov.ua fax (057) 702-13-20

The Kalman filter is researched for estimating wireless channel matrix coefficients. A new adaptive modulation algorithm was developed for WiMAX technology over MIMO antenna, which controls the modulation type through different MIMO channels depending on the signal to noise ration of the channels. The computer simulation for the adaptive modulation in MIMO channels by using Kalman filter estimation was done and the results were obtained.

Introduction. Recently the method of adaptive modulation for WiMAX technology was analyzed and a new method of adaptive modulation was proposed in previous work [1] and it was called the adaptive modulation in MIMO channels.

The multi-fading channels are one of the biggest problems in wireless channels, which causes the fading in receiving signals in time and frequency domains. The solution for multi-fading was using multi-antenna diversities in the transmitter and receiver which was called MIMO antenna. Although MIMO antenna is very effective solution for multi-fading, but still the fading gain in different MIMO channels causes unequal receiving in signal to noise ratio in different receiving antennas, which makes the used adaptive modulation in WiMAX technology not very effective in controlling the bit error rate. This problem of unequal receiving in MIMO was the reason for proposing the use of Adaptive modulation in MIMO channels, where this method takes the advantage of unequal receiving and uses a modulation with high number of positions like QAM16 or with low number of positions like BPSK depending in the signal to noise ration in the channels.

The adaptive modulation in MIMO channels in order to function, it needs to trace the change in channel matrix, where it performs that by using pilot signal. In order to estimate the correct channel matrix from the pilot signals that it is close to the real value of the channel, the system has to estimate the noise level, and the best to do this task is Kalman filter.

Adaptive modulation in MIMO channels system model. The system functional scheme model which uses adaptive modulation in MIMO channels for closed and open loop 2x2 MIMO are shown in figure 1.The model for open loop MIMO uses Alamouti space time code, while for closed loop MIMO the model uses singular value decomposition channel pre-coding. Also the adaptive modulation algorithms used in the model for open and closed MIMO are different. The model uses the advantage of channel ranging which it is a feature in WiMAX technology, where by using channel ranging the transmitter will be able to estimate the channel state information by using the download channel, and by using the channel ranging the model will be able to estimate the received signal to noise ratio and by doing that it will be able to choose the modulation type that can give the needed bit error rate. In the model Kalman filter is used to trace the change in the channel matrix and also to estimate the channel matrix by minimizing the effect of noise.

$$\hat{h}_{nm}(n) = a\hat{h}_{nm}(n-1) + k(n)\left[y_{nm}(n) - ac\hat{h}_{nm}(n-1)\right] \quad (1)$$

$$k(n) = \frac{c\left[a^2 p(n-1)\sigma_g{}^2\right]}{\sigma_v{}^2 + c^2\sigma_g{}^2 + c^2 a^2 p(n-1)} \quad (2)$$

$$p(n) = \frac{1}{c}\sigma_v{}^2 k(n) \quad (3)$$

Where $\hat{h}_{nm}(n)$: Estimated channel coefficient;
$y_{nm}(n)$: Measured channel coefficient;

n: row index; m: column index; $k(n)$: Kalman gain; $p(n)$: Root mean square error; ${\sigma_v}^2$: Noise root mean square; ${\sigma_g}^2$: Process root mean square; a: Signal oscillation element; c: Measurement oscillation element.

The Kalman filter is auto recursive loop, which is used by many systems to estimate the change in random process, where in our case the Kalman filter is used to estimate the change in the channel matrix. The main Kalman filter [1][2] equations are equations 1, 2 and 3. Equation 1 represents the main loop, which estimates the next channel coefficient $\tilde{h}_{nm}(n)$, by using the previous value $\tilde{h}_{nm}(n-1)$, and the Kalman gain $k(n)$. The next Kalman gain value is estimated by using the previous root mean square error $p(n-1)$, and by estimating the next Kalman gain the next $p(n)$ value can be estimated. The mathematical model for the adaptive modulation in MIMO channels is shown in figure 2, the model is for 2x2 MIMO system which means that four channels in the system, so four Kalman filters where used in the model. The Kalman filters read the measured channel coefficients $y_{nm}(n)$ from the channel estimation system, which uses the pilot carriers to estimate the channel matrix, and feed the estimated channel matrix to the adaptive modulation algorithm block.

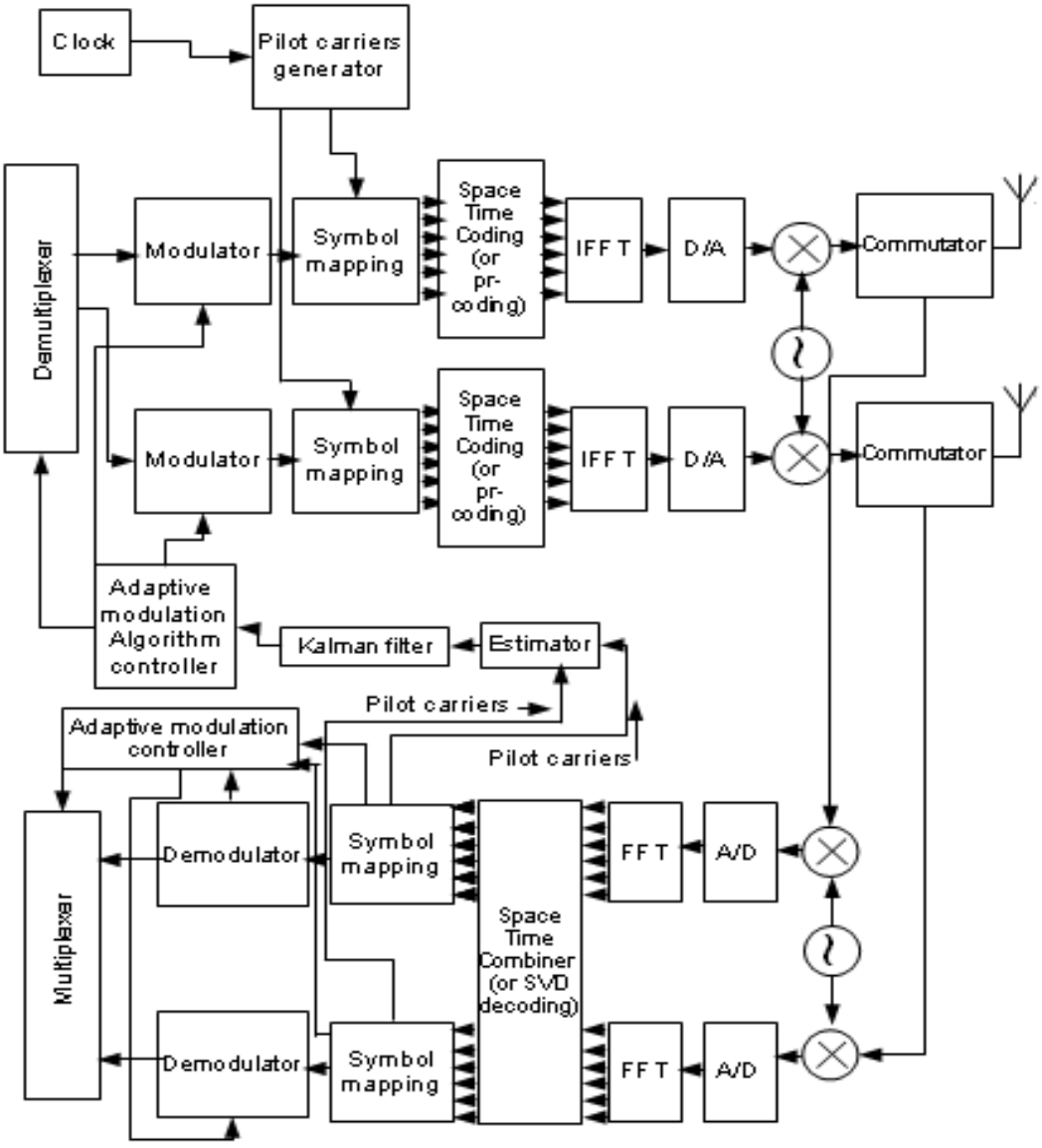


Fig. 1

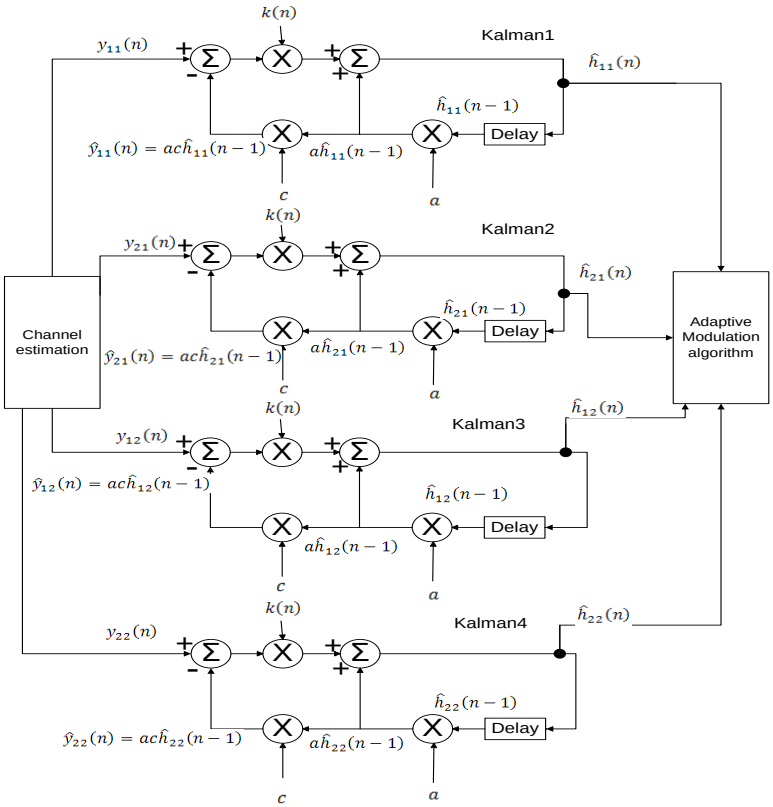
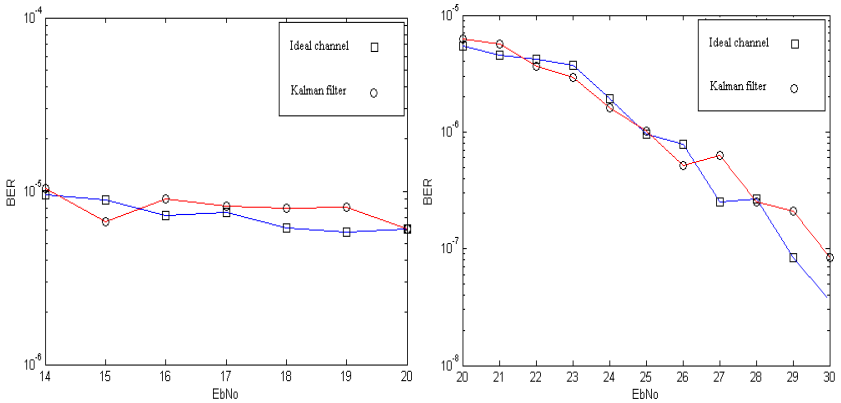


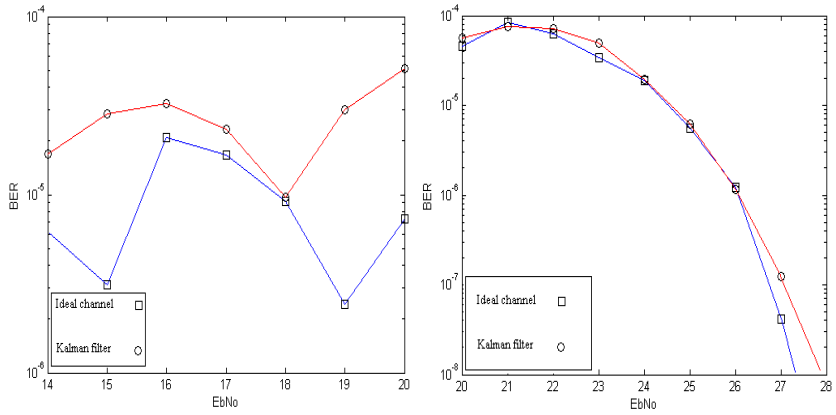
Fig.2

Simulation results. The simulation results for the above model are shown in figures 1 and 2. The results were made with ideal knowledge of the channel matrix and by using Kalman filtering estimation. Figure 3 is for open loop MIMO, while figure 4 is for closed loop MIMO. The results are made with two ranges of signal to noise ratio, the first is of QAM16 which is from 14dB to 20dB, and the second is for QAM64 which is from 20dB to 30dB. The results showed that the performance of Kalman filter with adaptive modulation in MIMO channels is optimal, and it has the same bit error rate of ideal channel knowledge.



(a) (b)

Fig.3 Simulation results for Kalman filter performance used with open loop MIMO (a) With QAM16 range (b) With QAM64 range



(a) (b)

Fig.4 Simulation results for Kalman filter performance used with closed loop MIMO (a) With QAM16 range (b) With QAM64 range

References.

1. Loshakov V., Z. Vadia. Adaptive modulation of signals in MIMO channels. Telecommunications Problems. № 1 (1). 2010.

2. Mohinder S. Grewal, Angus P. Andrews. Kalman filtering theory and practice using matlab. John Wiley & Sons 2001.

3. Greg Welch, Gary Bishop. An Introduction to the Kalman Filter // Department of Computer Science University of North Carolina. July 24, 2006.

RESULTS OF EXPERIMENTAL RESEARCH QUALITY OF COMMUNICATIONS IN WiMAX SYSTEM

V. Loshakov, prof., Z. Vadia, Ms, H.Al Janabii, Ms
Kharkov national technical university of radio electronics
(61166, Kharkov, Linen street,14, dep. Telecommunication system, tele. (057) 702-13-20),
E-mail: tkc@kture.kharkov.ua fax (057) 702-13-20

An expirement for WiMAX subscriber access technology was made. The eqyipmet used in the expirement were mobile WiMAX adapters and WiMAX base station. The expirement were perfomed by using a softwear program called IxChariot, and the results for different radio access parameters were obtained.

Introduction. The mobile WiMAX is a new technology, and its performance practically for internet access is not effectively tested. The purpose of experiment is the analysis of radio channel parameters of WiMAX physical layer from the point view of quality of service performance. In the experiments the analysis of multimedia services parameters for VoIP, IPTV and P2P were presented.

Experiment structure and the used elements. The software used in the experiments is IxChariot. IxChariot is a software tool used for estimating networks real performance parameters, such as throughput, time delay, loss of packages, jitter, MOS for VoIP and MDI for video in real conditions, and it is used by leading companies and test laboratories for control and certifications of the newest network devices. Measurements of performance in IxChariot are made by transfer of real data stream between the devices connected to a network.

The equipments used in the experiment are two WiMAX modems, and also two models were used in the experiment. The first model is USB portable modem for laptop computer use Alcatel-Lucent 9799 figure1(a), and the second model is for desktop indoor use Greenpacket DV 230 figure1(b).The internet service provider for WiMAX technology that is used in the experiment was Intellecom company which is started its services in Kharkov city in 2010 for fixed and mobile WiMAX services.

(a) (b)

Fig.1

The experiment network structure shown in figure1 is consisted of two computers, where one of them contains IxChariot program and it controls the operations, and the other one contains the end point and acts as mirror for the traffic. Also two WiMAX mobile adapters and WiMAX base station where used.

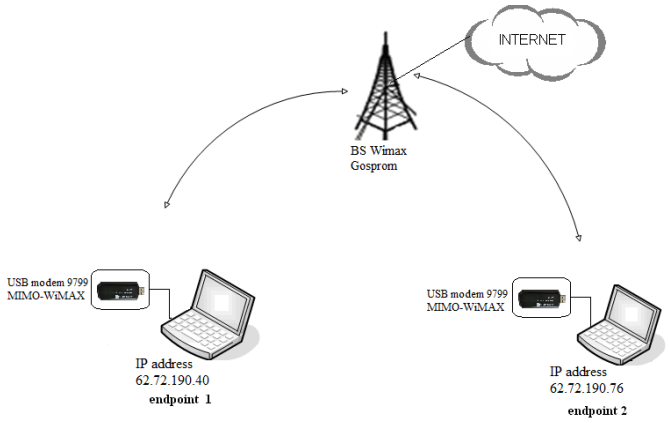
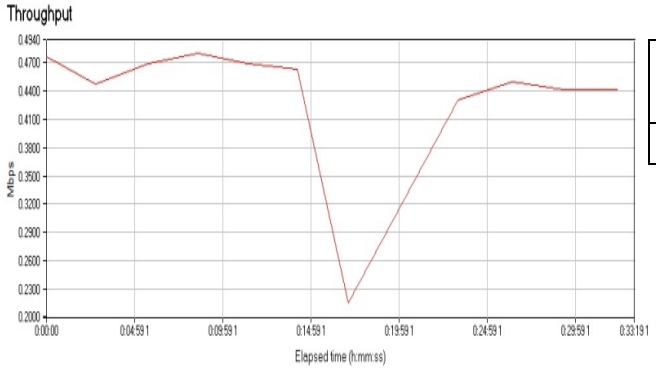


Fig.2

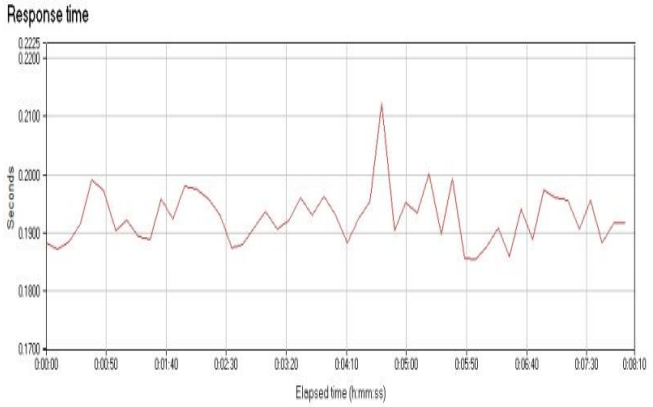
Experiment Results.

The experiment main results are shown in figures 3, 4, 5, 6 and 7 also the average, minimum and maximum values for the parameters are shown beside. The first measured parameter is high performance throughput in figure3. In figure4 one way time response is measured from one computer subscriber to the second subscriber. In figure 5 and 6 the throughput for IPTV and VOIP are measured, where for IPTV MPEG traffic was used, while for VOIP mp3 traffic was used. In figure 7 the Jitter was measured.



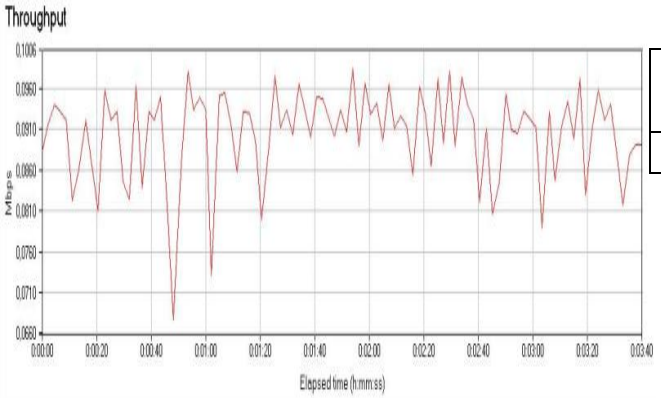
Average (Mbit/sec)	Minimum (Mbit/sec)	Maximum (Mbit/sec)
0.412	0.215	0.48

Fig.3 High performance throughput



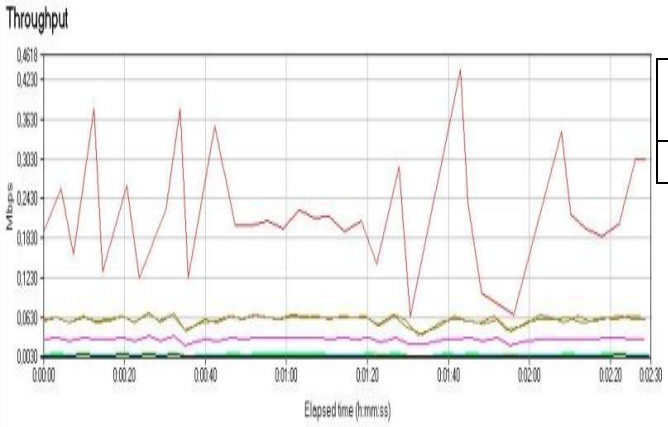
Average (Seconds)	Minimum (Seconds)	Maximum (Seconds)
0.193	0.186	0.212

Fig.4 one way time response



Average (Mbit/sec)	Minimum (Mbit/sec)	Maximum (Mbit/sec)
0.09	0.068	0.098

Fig.5 IPTV throughput



Average (Mbit/sec)	Minimum (Mbit/sec)	Maximum (Mbit/sec)
0.344	0.003	0.438

Fig.6 VOIP throughput

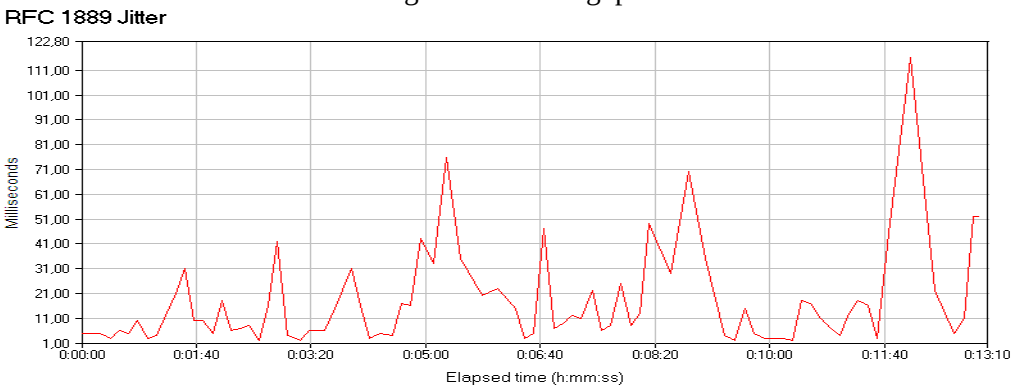


Fig.7 Jitter

RFC 1889Jitter Average (ms)	RFC 1889Jitter Minimum (ms)	RFC 1889Jitter Maximum (ms)	Jitter(delay variation) Maximum (ms)
16.765	2	116	802

МЕТОД УВЕЛИЧЕНИЯ БЫСТРОДЕЙСТВИЯ УСТРОЙСТВА ГРОЗОЗАЩИТЫ ПРИЁМНИКОВ РАДИОТЕХНИЧЕСКИХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Шостко И.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр.Ленина 14, каф. ТКС, т. 702-13-20
e-mail: tkc@kture.kharkov.ua)

A new method for increasing the speed of spark gap protects the receiver telecommunication systems by preionization discharge gap of infrared laser light.

Для защиты приёмников радиотехнических и телекоммуникационных систем от ЭМИ применяют устройства грозозащиты (УГЗ) на основе разрядников. Для обеспечения надежного и быстрого пробоя разрядника при воздействии мощного электромагнитного импульса (ЭМИ) в некоторые разрядники вводится дополнительный источник электронов. Такой источник электронов может быть получен за счет вспомогательного поджигающего разряда на постоянном токе, возникающего между дополнительным электродом, введенным в разрядник, и одним из основных его электродов.

Электроны, освобождаемые при этом поджигающем разряде, проходят к зазору разрядника и ускоряют его пробой при воздействии мощного ЭМИ. Поджигающий разряд генерирует шум, как и все газоразрядные приборы. Если в разряднике поддерживается достаточно интенсивный поджигающий разряд, то уровень шума может оказаться настолько высоким, что это приведет к снижению чувствительности приемника.

Более эффективным способом обеспечения быстрого пробоя разрядника является предварительная ионизация его межэлектродного промежутка с помощью источника лазерного излучения. Для ионизации межэлектродного промежутка необходимо выполнение закона Эйнштейна для фотоэффекта в его классической формулировке:

$$h \cdot \nu > E_0 , \qquad (1)$$

где $h\nu$ — энергия кванта излучения,

ν — частота излучения,

h - постоянная Планка,

E_0 - потенциал ионизации (энергия связи электрона в атоме).

Соотношение (1) соответствует утверждению, что энергия кванта $h\nu$ должна превышать энергию связи электрона E_0 для того, чтобы связанный электрон оказался свободным. Соответственно для частоты излучения существует "красная граница" - $\nu_{гр} = \frac{E_0}{h}$. Когда частота меньше граничной, ионизация невозможна. Поэтому для атомов и молекул, находящихся в основном состоянии, ионизация была возможна лишь под действием ультрафиолетового излучения. Действительно, потенциалы ионизации атомов и простых молекул, находящихся в основном состоянии, лежат в интервале $E_0 \approx 4 - 25$эВ, энергия фотона излучения видимого диапазона частот $h\nu \sim 2$эВ, для ультрафиолетового диапазона $h\nu \sim 10$эВ (λ=0,1 мкм). Следовательно, если непрерывно подсвечивать межэлектродный промежуток излучением ультрафиолетового лазера произойдёт ионизация газа, что ускорит пробой разрядника. Однако стоимость ультрафиолетового лазера с требуемыми для ионизации параметрами значительно превышает стоимость самого УГЗ. Для снижения себестоимости УГЗ рассмотрена задача применения с этой целью полупроводникового инфракрасного лазера большой мощности, при длительности переднего фронта импульса $\tau < 1$ пс.

Предлагается использовать эффект нелинейной ионизации. Известно, что с ростом интенсивности лазерного излучения характер взаимодействия излучения с атомами и молекулами качественно меняется: существенную роль начинают играть многофотонные процессы [1], в том числе процесс многофотонной ионизации. Ионизация происходит

при поглощении атомом в одном элементарном акте нескольких фотонов. При этом выполняется закон Эйнштейна, в следующей формулировке:

$$k \cdot h \cdot \nu > E_0 \qquad (2)$$

Соотношение (2) соответствует утверждению, что для отрыва электрона от атома необходимо поглощение энергии khν, превышающей энергию связи E_0 электрона в атоме. При этом энергия khν может представлять собой энергию как одного, так и нескольких фотонов, поглощенных в одном элементарном акте. В случае поглощения многих фотонов процесс ионизации является нелинейным по числу поглощенных фотонов. В соответствии с соотношением (2) при большой интенсивности излучения можно ожидать реализации процесса многофотонной ионизации при $h \cdot \nu < E_0$.

При реализации многофотонной ионизации можно подбором частоты лазерного излучения достичь резонансного эффекта роста вероятности нелинейной ионизации. Это позволяет управлять степенью ионизации в зависимости от частоты и интенсивности лазерного излучения. Требуемая интенсивность излучения обеспечивается в фокусе телескопической системы линз, размещённых внутри резонатора лазера.

Распределение интенсивности излучения во времени при импульсном режиме генерации лазера носит гауссовский характер. Длительности переднего фронта импульса могут иметь величину от 10^{-8} до 10^{-13} с в зависимости от режима генерации лазера. Условия для многофотонной ионизации реализуются на фронте импульса [1].

Обращаясь к ионизации газа лазерным излучением, надо иметь в виду, что при малом давлении газа определяющим процессом является нелинейная ионизация. При большом давлении определяющим является процесс ионизации электронным ударом. При столкновении колеблющегося электрона с нейтральным атомом возникают ионизация атома, и происходит лавинное размножение электронов. Именно такой процесс приводит к явлению оптического пробоя газа лазерным излучением с достаточно большой длительностью импульса [2]. Граница между областями значений давления газа, где определяющим является нелинейная ионизация или электронный удар, зависит от многих параметров, характеризующих как газ, так и излучение. Для частот излучения, лежащих в оптическом диапазоне, длительностей импульса больше нескольких наносекунд и напряженности поля меньше атомной (это типичные условия взаимодействия лазерного излучения с веществом) справедливо соотношение $\tau \cdot n \cdot F^2 \geq 10^{23}$, при выполнении которого возникает оптический пробой газа за счет электронного удара. В этом соотношении τ — длительность импульса в секундах, n — плотность газа в $см^{-3}$, F — напряженность поля излучения в $В \cdot см^{-1}$. Однако при малой длительности лазерного импульса τ < 1 пс оптический пробой не возникает, так как не успевает развиться электронная лавина. При таких длительностях лазерного импульса и любом давлении газа реализуется лишь нелинейная ионизация атомов.

Требуемая частота повторения импульсов определяется временем деионизации газа в разряднике. Длительность фронта импульса должна стремиться к предельно реализуемому минимуму.

Литература:

1. Делоне Н. Б. Нелинейная ионизация атомов лазерным излучением // Соросовский Образовательный Журнал. – 2001. – том 7. – № 11. – С. 94–101.

2. Райзер Ю. П. Пробой газов под действием лазерного излучения — "лазерная искра" // Соросовский Образовательный Журнал. – 1998. – № 1. – С. 89–94.

ВЛИЯНИЕ ИНДЕКСА ПОЛЯРИЗАЦИИ СИГНАЛА НА ПРОПУСКНУЮ СПОСОБНОСТЬ ПРИЕМНОГО КАНАЛА SISO СИСТЕМ

Мартынчук А.А., Скороход А.Н.
Харьковский национальный университет радиоэлектроники
050-402-52-97, alexmartynchuk@rambler.ru

The given work is devoted to the modern developments in the field of solution the main problems of telecommunications, such as increase of bit rate at fix bit error rate of the stationary and mobile SISO system by polarisation-orthogonal receiving aerials. Mismatch on polarisation and a degree of polarisation are researched. The output bit rate can be increased due to adaptive polarisation-orthogonal antenna.

Введение. Анализ уровня развития современных систем беспроводной связи показывает, что существует необходимость повышения пропускной способности соответствующих каналов, например, в сотовых системах связи, высокоскоростных локально-вычислительных сетях и др. Значительный интерес вызывает использование в общем случае нескольких антенн на излучение и при приеме – MIMO (multiinput/multioutput) систем, или в более распространенных и дешевых для конечного пользователя при беспроводном доступе простых системах SISO (single-input, single-output). Пропускная способность может быть увеличена с помощью расширения полосы частот, повышения излучаемой мощности, применением специальных методов кодирования. Однако вопросы возможности применения поляризационно-ортогональных антенных приемных элементов SISO систем освещены в литературе недостаточно [1, 2]. В частности, для стационарных и мобильных систем в этом случае *актуальными* являются исследование влияния рассогласования по поляризации и степени поляризации принимаемых электромагнитных волн на пропускную способность SISO системы и разработка предложений повышения пропускной способности, что и определяет *новизну* исследования.

Целью исследования является разработка предложений повышения пропускной способности SISO системы.

Задачами исследования являются: разработка математической модели изменяемых поляризационных параметров принимаемых волн; обобщение влияния рассогласования по поляризации и степени поляризации волн на пропускную способность приемного канала SISO системы; исследование возможностей повышения пропускной способности за счет использования поляризационно-ортогональных приемных антенн.

Сущность. Известно, что при полном соответствии поляризационных параметров падающей электромагнитной волны поляризационным параметрам приемной антенны мощность принятого сигнала будет максимальной. Однако в реальной ситуации наблюдаются некоторые несоответствия поляризационных параметров волны параметрам приемной антенны. Пусть некоторый информационный поток $S(t)$ излучается передающей антенной на вертикальной поляризации (рис. 1). Принимаемый сигнал в общем случае не будет строго линейно поляризованным ввиду конечной развязки по поляризации реальных излучателей, изменяемых условий распространения радиоволн мобильных систем, влияния переотражений, многолучевости, погодных условий (рис. 2).

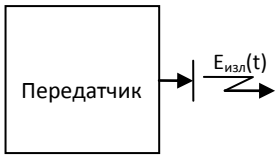


Рис. 1. Формирование сигнала

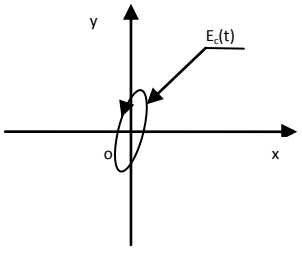


Рис. 2. Принимаемый сигнал

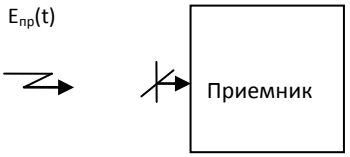


Рис. 3. Поляризационно-ортогональная антенна

В общем случае эллиптически поляризованная волна с изменяемыми параметрами поляризации, которые характеризуются степенью или индексом поляризации, улавливается антенной линейной поляризации. Рассогласование изменяемых поляризационных параметров падающей волны и приемной антенны вертикальной поляризации приводит к энергетическим потерям, что ограничивает пропускную способность канала. Значительно уменьшить потери предлагается путем использования поляризационно-ортогональной антенны на приемной стороне (рис. 3).

Математическая модель изменяемых поляризационных параметров принимаемых волн. Реальный излучаемый сигнал характеризуется параметрами поляризационного эллипса или поляризационной диаграммы, что представляет собой проекцию годографа, координат конца вектора напряженности электрического поля на картинную плоскость, т.е. на плоскость, ортогональную направлению распространения волны. Параметрами поляризационных диаграмм являются угол эллиптичности α, знак которого определяет направление обхода эллипса со стороны наблюдателя, и угол ориентации большой полуоси эллипса β, отсчитываемый от опорного горизонтального орта [1]. Тогда, опуская множители круговой частоты, затухания и дальности, вектор напряженности электрического поля вблизи передающей антенны (рис. 1) может быть представлен в виде поляризационного вектора излучаемого сигнала

$$\dot{\vec{E}}_{изл}(t) = H_{\alpha}^{T*} \cdot H_{\beta}^{T} \cdot \left(S(t) \cdot \vec{p}_1^{\,0}\right)^T, \tag{1}$$

где $H_{\alpha} = \begin{pmatrix} \cos(\alpha) & -j\sin(\alpha) \\ -j\sin(\alpha) & \cos(\alpha) \end{pmatrix}$ – матрица эллиптичности, $\alpha = -45^0 ... +45^0$;

$H_{\beta} = \begin{pmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{pmatrix}$ – матрица ориентации, $\beta = -90^0 ... +90^0$;

$\vec{p}_1^{\,0} = \begin{pmatrix} 1 & 0 \end{pmatrix}^T$ – горизонтальный орт линейного поляризационного базиса.

Заметим, что ввиду конечной развязки по поляризации реальной передающей антенны в (1) имеем

$$\alpha = \alpha_{изл} = 0 \pm \Delta\alpha_{изл} = arctg\left(\frac{E_{крос\_изл}}{E_{осн\_изл}}\right), \tag{2}$$

где $E_{крос\_изл}$ – кросс-поляризационная составляющая излучаемого поля (горизонтальная); $E_{осн\_изл}$ – основная составляющая излучаемого поля (вертикальная).

Невертикальность угла ориентации передающей антенны $\Delta\beta$ учитывается в (1) следующим образом

$$\beta = \beta_{изл} = 90^0 \pm \Delta\beta_{изл}. \tag{3}$$

Вследствие особенностей распространения радиоволн, вектор напряженности принимаемого сигнала у приемной антенны покажем в виде

$$\dot{\vec{E}}_{пр}(t) = \dot{\vec{E}}_{изл}(t - \iota_0) \cdot \dot{K}_{r0}(t) + \sum_{i=1}^{n} \dot{R}_i(t - \iota_i) \cdot \dot{K}_{ri}(t - \iota_i) \cdot \dot{\vec{E}}_{изл}(t - \iota_i), \tag{4}$$

где n – общее количество переотражений при распространении; $\dot{K}_{r0}(t)$ и $\dot{K}_{ri}(t - \iota_i)$ – множители затухания прямой и переотраженных волн; ι_0 и ι_i – множители запаздывания прямой и переотраженных волн; $\dot{R}_i(t - \iota_i)$ – матрица коэффициентов отражений.

Поляризационные параметры приемной антенны опишем с помощью поляризационного вектора (5) при углах эллиптичности и ориентации поляризационной диаграммы приемной антенны в соответствии с выражениями

$$\dot{\vec{p}}_a = H_{\alpha}^{T*} \cdot H_{\beta}^{T} \cdot \vec{p}_1^{\,0}, \tag{5}$$

$$\alpha = \alpha_{пр} = 0 \pm \Delta\alpha_{пр} = arctg\left(\frac{E_{кросс\_пр}}{E_{осн\_пр}}\right),\ \beta = \beta_{пр} = 90^0 \pm \Delta\beta_{пр}.$$

Учитывая выражения (4) и (5), найдем сигнал на выходе приемной антенны

$$\dot{U}_{пр}(t) = \vec{p}_a^{T*} \cdot \vec{\dot{E}}_{пр}(t) \cdot K_a + \dot{U}_{ш}(t) = \dot{U}_c(t) + \dot{U}_{ш}(t), \quad (6)$$

где K_a – коэффициент, учитывающий потери и преобразующую роль приемной антенны (эффективная длина для вибраторов); $\dot{U}_{ш}(t)$ – тепловой шум приемного канала.

Если потенциальное значение отношения мощности сигнала к мощности шума

$$h^2 = \frac{P_c}{P_{ш}}, \quad (7)$$

то реальное зависит от коэффициента поляризационного приема [1]

$$h^2_{вых} = h^2 \cdot K_{пр}, \quad (8)$$

который определяется как

$$K_{пр} = \cos^2\delta, \quad (9)$$

где δ – угол между поляризационными векторами сигнала (4) и антенны (5), который представляет собой, по существу, рассогласование по поляризации между сигналом и антенной и находится в соответствии с выражением

$$\delta = \arccos(\vec{\dot{E}}^T_{пр} \cdot \vec{p}^*_a). \quad (9)$$

На практике удобнее использовать величину потерь мощности сигнала при рассогласовании, т.е. несовпадении поляризационных параметров принимаемой волны и антенны

$$K_{потерь} = 10 \cdot \log\left(\frac{1}{\cos^2\delta}\right), \text{ дБ}. \quad (10)$$

Поэтому, реальное отношение мощности сигнала к мощности шума на выходе рассматриваемого канала передачи можно представить в виде

$$h^2_{вых} = 10 \cdot \log\left(\frac{P_c}{P_{ш}}\right) - K_{потерь}, \text{ дБ}. \quad (11)$$

Заметим, что потери будут минимальными при совпадении поляризационных параметров антенны и принимаемой волны

$$\alpha_a = \alpha_{пр} \quad , \quad \beta_a = \beta_{пр}. \quad (12)$$

Указанное вынуждает управлять поляризационными параметрами приемной антенны с помощью фазовращателей и аттенюаторов [1], что предъявляет высокие требования к стабильности и широкополосности таких устройств.

Обобщение влияния рассогласования по поляризации и степени поляризации волн на пропускную способность приемного канала SISO системы.

Под степенью поляризации электромагнитной волны понимают зависимость во времени поляризационных параметров на интервале некоторого времени наблюдения, например, сеанса передачи. Если с течением времени поляризационные параметры остаются неизменными, то говорят о полностью поляризованных сигналах, если изменяются с максимальной степенью хаотичности – то неполяризованные. В этом случае говорят об индексе либо степени поляризации падающей электромагнитной волны как отношении мощности полностью поляризованной составляющей поля к ее полной мощности [1]

$$m = \frac{P_{пп}}{P_c} = 1 - \frac{P_{нп}}{P_{пп} + P_{нп}}, \quad (13)$$

где $P_{пп}$ – полностью поляризованная составляющая полной мощности сигнала P_c; $P_{нп}$ – неполяризованная (хаотическая) составляющая полной мощности сигнала.

Реальные сигналы в свободном пространстве являются, вообще говоря, частично

поляризованными и индекс поляризации принимает значения $m = 0...1$. Поэтому, будем считать на практике, что при $1 \ge m \ge 0{,}95$ волна является полностью поляризованной, при $0{,}95 > m > 0{,}05$ – частично поляризованной, и при $0{,}05 \ge m \ge 0$ – хаотически поляризованной.

Индекс поляризации можно рассчитать с использованием параметров Стокса [1] либо оценить в реальных условиях высокого энергетического параметра. При этом следует получить ковариационную матрицу вектора напряженности принимаемого сигнала у приемной антенны (4) по выборке из k нормально распределенных временных отсчетов. При гипотезе нулевого математического ожидания имеем

$$\dot{M} = \frac{1}{k-1}\sum_{i=1}^{k} \vec{\dot{E}}_{np}(t) \cdot \vec{\dot{E}}_{np}^{T*}(t). \qquad (14)$$

Учитываем, что эта ковариационная матрица (КМ) является эрмитовой, а значит и положительно определенной. Поэтому, она относится к классу диагонализируемых матриц. Имеем

$$\dot{M} = \vec{\dot{B}} \cdot \Lambda \cdot \vec{\dot{B}}^{T*}, \qquad (15)$$

где $\dot{B} = \left(\vec{\dot{b}}_1 \quad \vec{\dot{b}}_2 \right)$ – матрица собственных векторов, зависящая от H_α и H_β;

$\Lambda = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ – матрица собственных значений, спектр КМ, причем, $\lambda_1 \ge \lambda_2$.

Заметим, что ранг КМ соответствует количеству ненулевых элементов матрицы собственных значений и свидетельствует степени поляризации принимаемой волны. При этом если:

$\mathrm{Rank}(\dot{M}) = 1$ при $\lambda_1 = P_c$ и $\lambda_2 = 0$, то волна является полностью поляризованной;

$\mathrm{Rank}(\dot{M}) = 2$ при $\lambda_1 \ne 0$ и $\lambda_2 \ne 0$, то волна является частично поляризованной;

$\mathrm{Rank}(\dot{M}) = 2$ при $\lambda_1 = \lambda_2$, то волна является хаотически поляризованной.

Ввиду свойства инвариантности КМ, имеем

$$P_c = \mathrm{trace}\left(\dot{M}\right) = \mathrm{trace}\left(\Lambda\right) = \lambda_1 + \lambda_2. \qquad (16)$$

Несложно показать, что если хаотическая составляющая полной мощности сигнала в (13) распределена равновероятно и одинаково вдоль горизонтального и вертикального орта линейного поляризационного базиса, то

$$\Lambda = \begin{pmatrix} P_{пп} + \dfrac{P_{нп}}{2} & 0 \\ 0 & \dfrac{P_{нп}}{2} \end{pmatrix}. \qquad (17)$$

Поэтому, учитывая (13) и свойство (16), получим оценку индекса поляризации

$$\hat{m} = \frac{\lambda_1 - \lambda_2}{\lambda_1 + \lambda_2} = \frac{\Delta\lambda}{P_c}. \qquad (18)$$

Таким образом, индекс поляризации можно получить по данным оценочной КМ реального принимаемого сигнала у приемной антенны в условиях высокого энергетического параметра.

Однако для реального канала передачи, в типовых условиях энергетического параметра оценка индекса поляризации на выходе приемных каналов будет зависеть также и от энергетического параметра, от отношения мощности сигнала к мощности шума. Считая шум стационарным и нормально распределенным в (6), основываясь на предыдущих выкладках, можно получить оценку индекса поляризации реального канала передачи с учетом влияния шумов

$$\hat{m}_p = \frac{m}{1 + m \cdot h^2}. \qquad (19)$$

где m – индекс поляризации самой волны, без учета влияния шумов.

Откуда найдем истинный индекс поляризации самой волны

$$m = \frac{\hat{m}_p}{1 - \hat{m}_p \cdot h^2}. \qquad (20)$$

Итак, коэффициент поляризационного приема канала передачи на основании (9), (13) и (17) определим в соответствии с формулой

$$K_{кан} = \frac{1 + m \cdot (2\cos^2 \delta - 1)}{2}, \qquad (21)$$

а энергетический параметр канала передачи при этом будет

$$h^2_{вых} = h^2 \cdot K_{кан}. \qquad (22)$$

Определим пропускную способность приемного канала SISO системы с учетом влияния рассогласования по поляризации и степени поляризации волн с использованием соотношения Шенона [2, 3]

$$C = \Delta F \cdot \log_2\left(1 + \frac{P_c}{P_ш}\right) = \Delta F \cdot \log_2\left(1 + h^2 \cdot K_{кан}\right), \qquad (23)$$

где ΔF – ширина полосы пропускания канала.

Или в общем виде

$$C = \Delta F \cdot \log_2\left(1 + h^2 \cdot \frac{1 + m \cdot (2\cos^2 \delta - 1)}{2}\right). \qquad (24)$$

Итак, полученное выражение (24) определяет зависимость пропускной способности приемного канала SISO системы от рассогласования по поляризации – угла δ и степени поляризации волны m при различных значениях потенциального энергетического параметра h^2.

Покажем также вероятность ошибок передачи информации такого канала [2]

$$P_{ош} = 1 - F\left(\sqrt{k \cdot h^2 \cdot \frac{1 + m \cdot (2\cos^2 \delta - 1)}{2}}\right), \qquad (25)$$

где k – коэффициент, связанный с видом модуляции (например, $k = 4$ для двоичного бинарного фазового кодирования); $F(x)$ – функция Лапласа.

Исследование возможностей повышения пропускной способности за счет использования поляризационно-ортогональных приемных антенн. Рассмотрим двумерную функцию коэффициента поляризационного приема (21) и ее сечения (рис.4,5). Очевидно, что потери существенно возрастают при индексе поляризации $m \geq 0{,}8$ и большом угле рассогласования $80^0 \ldots 90^0$, в то же время, когда при $m \leq 0{,}5$ такая зависимость уменьшается. Слабо поляризованные волны при $m \leq 0{,}05$ характеризуются потерями при приеме около 3дБ и инвариантностью к углу рассогласования.

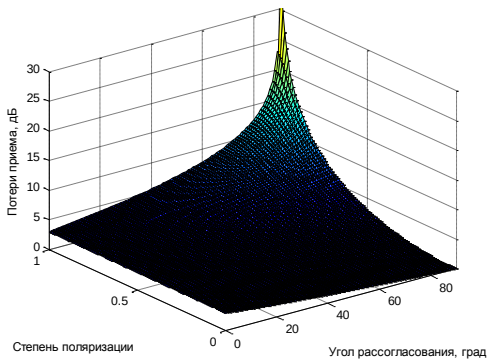


Рис. 4. Двумерная функция коэффициента поляризационного приема (потери)

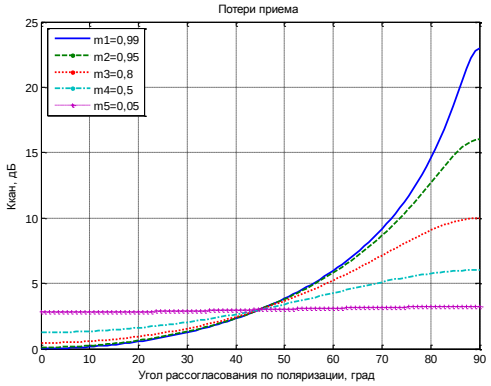


Рис. 5. Зависимости коэффициента поляризационного приема

Так, для типовых антенн с развязкой по поляризации 10…15дБ и индекса поляризации $m \geq 0{,}95$, что характерно для стационарных систем, потери могут составлять величину до 16дБ, в то время, когда для мобильных систем при индексе поляризации $m = 0{,}5$ – до 6дБ. Рассмотрим зависимости пропускной способности приемного канала (24) от рассогласования по поляризации при фиксированных значениях степени поляризации волны m (рис. 6). При этом значение энергетического параметра $h^2 = 20$ дБ и ширина полосы пропускания канала $\Delta F = 10$ МГц.

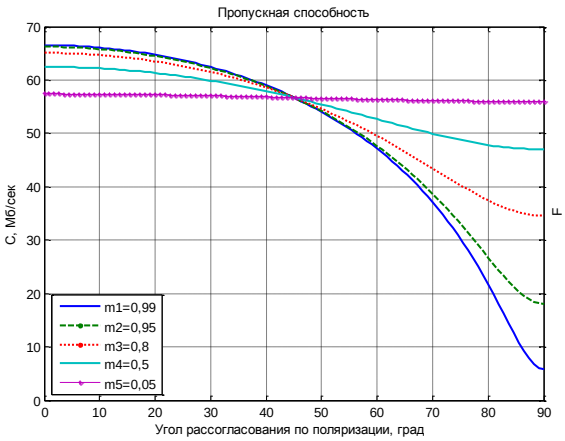


Рис. 6. Пропускная способность при различном индексе поляризации m ($h^2 = 20$ дБ)

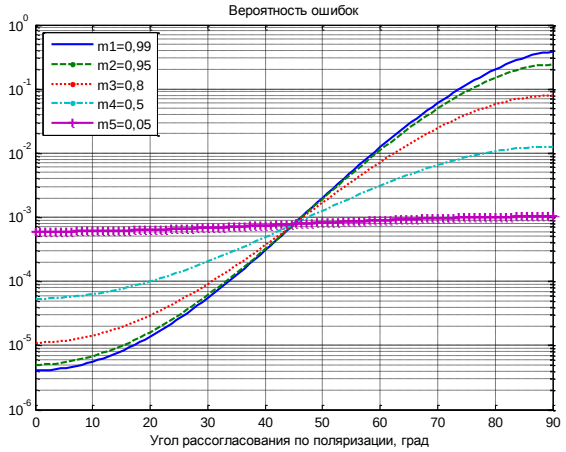


Рис. 7. Вероятность ошибок передачи при различном индексе поляризации m

Заметим, что пропускная способность сильно зависит от угла рассогласования при индексе поляризации $m \geq 0{,}8$. Для типовых антенн при индексе поляризации $m \geq 0{,}95$ пропускная способность канала может уменьшиться почти в 4 раза, а при индексе поляризации $m = 0{,}5$ только на 30%. Вероятность ошибок передачи F при различном индексе поляризации m представлено на рис. 7. Отметим, что увеличение угла рассогласования более 10^0 приводит к значительному возрастанию ошибок, а при $m \leq 0{,}8$ ошибки становятся неприемлемыми. Таким образом, наличие угла рассогласования по поляризации сигнала и антенны более 10^0 при индексе поляризации $m \leq 0{,}8$ существенно ухудшают пропускную способность, и вероятность ошибок реального канала передачи в целом. На практике, для повышения пропускной способности и снижения вероятности ошибок канала передачи целесообразным является использование поляризационно-ортогональных приемных антенн с адаптивной подстройкой их поляризационных параметров, что позволит уменьшить угол рассогласования по поляризации и увеличить индекс поляризации за время обучения и подстройки.

Выводы. Разработанная математическая модель изменяемых поляризационных параметров принимаемых волн позволяет исследовать влияния рассогласования по поляризации и степени поляризации волн на пропускную способность приемного канала SISO системы и исследовать возможности повышения пропускной способности за счет использования поляризационно-ортогональных приемных антенн, что представляет собой существенную практическую значимость.

Литература:

1. Родимов А.П., Поповский В.В. Статистическая теория поляризационно-временной обработки сигналов и помех. – М.: Радио и связь, - 1984. – 272 с.

2. Многоканальная электросвязь и телекоммуникационные технологии: Учебник для студентов высших учебных заведений / Под общ. ред. В. В. Поповского. — Харьков: ООО «Компания СМИТ», 2006. — 596 с. — На русск. яз.

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ MIMO СИСТЕМЫ ПУТЕМ ИСПОЛЬЗОВАНИЯ ПОЛЯРИЗАЦИОННО-ОРТОГОНАЛЬНЫХ АНТЕНН

Мартынчук А.А., Назмутдинов А.А.
Харьковский национальный университет радиоэлектроники
050-402-52-97, alexmartynchuk@rambler.ru

The given work is devoted to the modern developments in the field of solution the main problems of telecommunications, such as increase of bit rate at fix bit error rate for the stationary and mobile MIMO system by double polarization-orthogonal receiving antennae and simple polarization-orthogonal transmission antenna. The output bit rate can be increased due to adaptive polarization-orthogonal antennae and decreased mismatch on polarization

Введение. Повышение пропускной способности каналов беспроводного доступа может быть достигнуто путем расширения полосы частот, повышения излучаемой мощности, применением специальных методов кодирования, включающих и методы пространственно-временного кодирования и мультиплексирования, к которым и относят MIMO системы. Однако, вопросы возможности применения поляризационно-ортогональных антенных элементов MIMO систем для реализации поляризационного пространственно-временного кодирования освещены в литературе недостаточно [1,2]. В частности, для стационарных и мобильных систем в этом случае *актуальной* является задача исследования возможности и эффективности использования поляризационного пространственно-временного кодирования для повышения пропускной способности каналов беспроводного доступа MIMO системы, что и определяет *актуальность* исследования.

Целью исследования является разработка предложений повышения пропускной способности MIMO системы.

Задачами исследования являются: разработка математической модели сигнала на выходе многоканального приемника с ортогональными поляризационными каналами MIMO системы; исследование пропускной способности при использования поляризационного пространственно-временного кодирования.

Сущность. Пусть некоторый информационный поток $S(t)$ в кодере передатчика разделен на два подпотока $S(t)=\left(S_1(t)\quad S_2(t)\right)^T$, которые после ортогонального кодирования либо ортогонального модулирования одновременно излучаются передающей антенной на вертикальной поляризации $S_1(t)$ и на горизонтальной $S_2(t)$ (рис. 1).

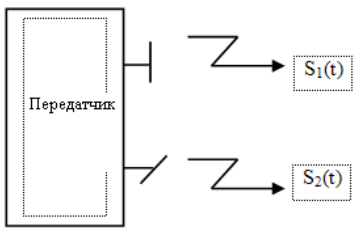


Рис. 1. Излучение ортогональных сигналов

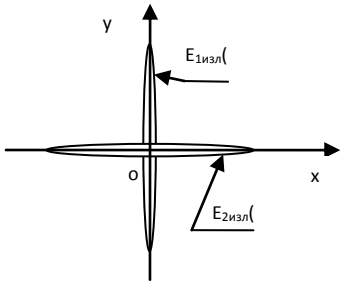


Рис. 2. ПД излучаемых сигналов

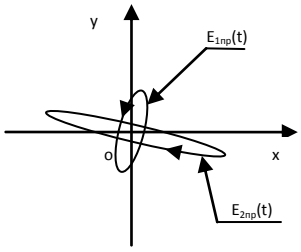


Рис. 3. ПД принимаемых сигналов

Излучаемые сигналы в свободном пространстве реальных поляризационно-ортогональных излучателей передающих антенн ввиду их конечной развязки по поляризации характеризуются параметрами поляризационных диаграмм (ПД), такими как угол эллиптичности α и угол ориентации β поляризационного эллипса (рис. 2). ПД принимаемых сигналов ввиду изменяемых условий распространения радиоволн мобильных систем, влияния переотражений, многолучевости, погодных условий, могут сколь угодно отличаться от идеальных линейно-поляризованных (рис. 3) и являются

частично поляризованными [1]. Поэтому, целесообразным является полный поляризационный прием таких сигналов (рис.4) в многоканальном приемнике.

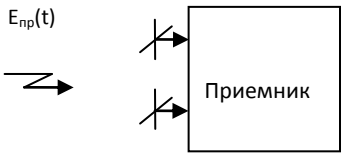


Рис. 4. Поляризационно-ортогональные антенны приемника

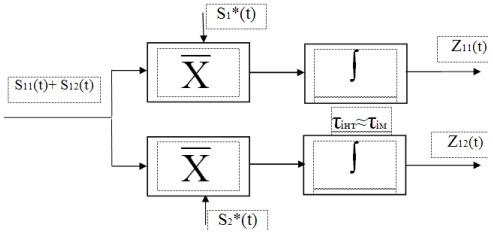


Рис. 5. Выделение ортогональных сигналов в одном поляризационном канале

Сигналы с ортогональным кодированием выделяются в четырех поляризационных каналах многоканального приемника, один из которых представлен на рис. 5. В каждом из поляризационных каналов происходит разделение основных ($z_{11}(t)$ либо $z_{22}(t)$) и перекрестных ($z_{12}(t)$ либо $z_{21}(t)$) по поляризации составляющих ортогональных сигналов. В результате дальнейшей адаптивной к поляризационным изменениям обработки полученного поляризационного вектора сигналов выделяются составляющие $S_1(t)$ и $S_2(t)$ в декодере и происходит формирование выходного информационного потока $S(t)$.

Математическая модель сигнала на выходе многоканального приемника с ортогональными поляризационными каналами MIMO системы. Вектор напряженности электрического поля вблизи передающей антенны (рис. 1) может быть представлен в виде поляризационного вектора

$$\dot{\vec{E}}_{изл}(t) = H_{\alpha}^{T*} \cdot H_{\beta}^{T} \cdot (S_1(t) \quad 0)^T + H_{\alpha}^{T*} \cdot H_{\beta}^{T} \cdot (0 \quad S_2(t))^T, \qquad (1)$$

где $H_{\alpha} = \begin{pmatrix} \cos(\alpha) & -j\sin(\alpha) \\ -j\sin(\alpha) & \cos(\alpha) \end{pmatrix}$ – матрица эллиптичности, $\alpha = -45^0 ... +45^0$;

$H_{\beta} = \begin{pmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{pmatrix}$ – матрица ориентации, $\beta = -90^0 ... +90^0$;

$\alpha = \alpha_1; \alpha_2$ и $\beta = \beta_1; \beta_2$ – углы эллиптичности и ориентации ПД первого и второго излучателя передающей антенны соответственно.

Вследствие особенностей распространения радиоволн, вектор напряженности принимаемого сигнала у приемной антенны покажем в виде

$$\dot{\vec{E}}_{пр}(t) = \dot{\vec{E}}_{изл}(t - \iota_0) \cdot \dot{K}_{r0}(t) + \sum_{i=1}^{n} \dot{R}_i(t - \iota_i) \cdot \dot{K}_{ri}(t - \iota_i) \cdot \dot{\vec{E}}_{изл}(t - \iota_i), \qquad (2)$$

где n – общее количество переотражений при распространении; $\dot{K}_{r0}(t)$ и $\dot{K}_{ri}(t - \iota_i)$ – множители затухания прямой и переотраженных волн; ι_0 и ι_i – множители запаздывания прямой и переотраженных волн; $\dot{R}_i(t - \iota_i)$ – матрица коэффициентов отражений.

Поляризационные параметры приемных антенн опишем с помощью поляризационного вектора каждого излучателя при известных углах эллиптичности и ориентации ПД. Для первого, например, имеем

$$\dot{\vec{p}}_{a1} = H_{\alpha 1}^{T*} \cdot H_{\beta 1}^{T} \cdot \vec{p}_1^{\,0}, \qquad (3)$$

$$\alpha_1 = \alpha_{пр} = 0 \pm \Delta\alpha_{пр1} = arctg\left(\frac{E_{крос\_пр1}}{E_{осн\_пр1}}\right), \; \beta_1 = \beta_{пр1} = 90^0 \pm \Delta\beta_{пр1},$$

где $E_{крос\_пр1}$ – кросс-поляризационная составляющая поля (горизонтальная);

$E_{осн\_пр1}$ – основная составляющая поля (вертикальная);

$\Delta\alpha_{пр1}$ – угол эллиптичности ПД, определяющий конечную развязку по поляризации реальной антенны;

$\Delta\beta_{пр1}$ – угол невертикальности, ошибки установки антенны;

$\vec{p}_1^{\,0} = (1 \quad 0)^T$ – единичный поляризационный орт первого излучателя первой антенны.

Сигнал на выходе каждого излучателя приемной антенны представим в виде

$$\dot{U}_{пр}(t) = \vec{p}_a^{\,T*} \cdot \vec{\dot{E}}_{пр}(t) \cdot K_a + \dot{U}_{ш}(t) = \dot{U}_c(t) + \dot{U}_{ш}(t), \tag{4}$$

где K_a – коэффициент, учитывающий потери и преобразующую роль приемной антенны (эффективная длина для вибраторов); $\dot{U}_{ш}(t)$ – тепловой шум приемного канала.

Сигналы с выхода первого канала первой поляризационно-ортогональный антенны (рис. 5) представим в виде

$$\vec{\dot{z}}_{1к} = (\dot{z}_{111} \quad \dot{z}_{121})^T. \tag{5}$$

На выходе второго канала первой поляризационно-ортогональный антенны имеем

$$\vec{\dot{z}}_{2к} = (\dot{z}_{211} \quad \dot{z}_{221})^T. \tag{6}$$

Сигнал третьего и четвертого каналов второй поляризационно-ортогональный антенны будет соответственно

$$\vec{\dot{z}}_{3к} = (\dot{z}_{112} \quad \dot{z}_{122})^T, \tag{7}$$

$$\vec{\dot{z}}_{4к} = (\dot{z}_{212} \quad \dot{z}_{222})^T. \tag{8}$$

Результирующий комплексный поляризационный вектор сигнала на выходе многоканального приемника покажем в виде составляющих векторов

$$\vec{\dot{z}}_{с\_вых} = \left(\vec{\dot{z}}_{1к}^{\,T} \quad \vec{\dot{z}}_{2к}^{\,T} \quad \vec{\dot{z}}_{3к}^{\,T} \quad \vec{\dot{z}}_{4к}^{\,T}\right)^T \tag{9}$$

и в общей форме

$$\vec{\dot{z}}_{с\_вых} = (\dot{z}_{111} \quad \dot{z}_{121} \quad \dot{z}_{211} \quad \dot{z}_{131} \quad \dot{z}_{112} \quad \dot{z}_{122} \quad \dot{z}_{212} \quad \dot{z}_{222})^T. \tag{10}$$

Считаем, что прием происходит в условиях влияния внутренних шумов приемных каналов, поэтому, область дискретных значений результирующего сигнала (10) можно представить n-мерной плотностью распределения ($n = 8$) с нулевым средним, которую будем считать приближающейся к нормальному закону [1]

$$P(\vec{\dot{z}}_{с\_вых}) = \left((2\pi)^r \left|\dot{M}\right|\right)^{-\frac{1}{2}} \exp\left\{-\frac{1}{2}(\vec{\dot{z}}_{с\_вых})^{T*} \dot{M}^{-1} (\vec{\dot{z}}_{с\_вых})\right\}, \tag{11}$$

где $\dot{M}^{-1}$ – матрица, обратная ковариационной матрице (КМ).

КМ заменяем ее текущей оценкой, которую получаем по результатам приема векторного сигнала (10)

$$\dot{M} \approx \hat{\dot{M}}(t) = \frac{1}{k-1} \sum_{i=1}^{k} \vec{\dot{z}}_{ic\_вых}(t_i - T_{усp}) \cdot \vec{\dot{z}}_{ic\_вых}^{\,T*}(t_i - T_{усp}), \tag{12}$$

причем, величина k – должна быть достаточной с точки зрения ошибок оценки и стационарности процесса.

С другой стороны, оценка КМ соответствует некоторому количеству усредняемых отсчетов, а значит и некоторому периоду времени усреднения $T_{усp}$, которое представляет собой величину, зависящую от времени корреляции сигнала $\iota_{с\_кор}$ с учетом изменения поляризационных параметров. Заметим, что выражение (12) представляет собой адаптацию к текущим поляризационным изменениям сигнала при $T_{усp} \ll \iota_{с\_кор}$.

В реальных условиях КМ (12) будет плохо обусловленной, а значит выражение (11) будет некорректным. Поэтому, целесообразным является переход от поляризационного вектора сигнала (10) к вектору его независимых главных компонент. Для этого отметим,

что КМ является эрмитовой, а значит и положительно определенной. Поэтому, она относится к классу диагонализируемых матриц. Имеем

$$\dot{M} = \vec{\dot{B}} \cdot \Lambda \cdot \vec{\dot{B}}^{T*}, \tag{13}$$

где $\dot{B} = \left(\vec{\dot{b}}_1 \quad \vec{\dot{b}}_2 \quad \vec{\dot{b}}_3 \quad \vec{\dot{b}}_4 \quad \vec{\dot{b}}_5 \quad \vec{\dot{b}}_6 \quad \vec{\dot{b}}_7 \quad \vec{\dot{b}}_8 \right)^T$ − матрица собственных векторов КМ;

$\Lambda = diag(\lambda_1 \quad \lambda_2 \quad \lambda_3 \quad \lambda_4 \quad \lambda_5 \quad \lambda_6 \quad \lambda_7 \quad \lambda_8)$ − матрица собственных значений, спектр КМ, причем, $\lambda_1 \geq \lambda_8$.

Поэтому, вектор главных компонент найдем так

$$\vec{\dot{z}}_{c\_вых\ r}(t_i) = \dot{B}^{T*} \cdot \vec{\dot{z}}_{c\_вых}. \tag{14}$$

Теперь плотность вероятности распределения можно представить r-мерной $(r \leq n)$ плотностью распределения с нулевым средним

$$P(\vec{\dot{z}}_{c\_вых\ r}) = \left((2\pi)^r \left| \dot{M}_r \right| \right)^{-\frac{1}{2}} \exp\left\{ -\frac{1}{2} (\vec{\dot{z}}_{c\_вых\ r})^{T*} \dot{M}_r^{-1} (\vec{\dot{z}}_{c\_вых\ r}) \right\}. \tag{15}$$

Заметим, что априори истинный ранг КМ сигнала (12) без учета влияния шумов и степени поляризации уже известен и равен двум $r = 2$, так как информационный поток $S(t)$ в кодере передатчика был разделен на два ортогональных, а значит и независимых подпотока $S(t) = (S_1(t) \quad S_2(t))^T$. Поэтому, использование метода главных компонент позволит найти преобразующую матрицу приемника (рис.4) для выделения составляющих информационного потока в виде

$$S(t) \Rightarrow \begin{pmatrix} S_1(t) \\ S_2(t) \end{pmatrix} = \vec{\dot{z}}_{c\_вых\ r}(t_i) = \left(\vec{\dot{b}}_1 \quad \vec{\dot{b}}_2 \right)^{T*} \cdot \vec{\dot{z}}_{c\_вых}(t). \tag{16}$$

Итак, обработка (16) вместе с адаптацией (12) позволит существенно уменьшить поляризационные потери на рассогласование по поляризации частично поляризованного сигнала и антенны. Естественной платой за это является усложнение приемного канала и устройств обработки.

Исследование пропускной способности при использования поляризационного пространственно-временного кодирования. Определим пропускную способность и вероятность ошибок типового двухканального приемного канала MIMO системы с использованием вибраторных антенн [2]. При этом учитываются типовые поляризационные потери реального канала, например, $K_{кан} = 3дБ$ за счет влияния рассогласования по поляризации и степени поляризации волн. Полоса частот 20МГц. Кодирование − простое бинарное фазовое. Вероятность ошибок оценивалась статистическим методом Монте-Карло с помощью разработанной математической модели и программы канала MIMO с поляризационно ортогональными антеннами и с учетом поляризационных искажений сигнала при излучении, приеме и при распространении. Количество моделируемых бит информации 10^6, количество тестов 25. Для сравнения определим пропускную способность (рис. 6) и вероятность ошибок (рис. 7) предлагаемого приемного канала с поляризационным ортогональным кодированием и без поляризационных потерь и реального канала с поляризационными потерями $3дБ$.

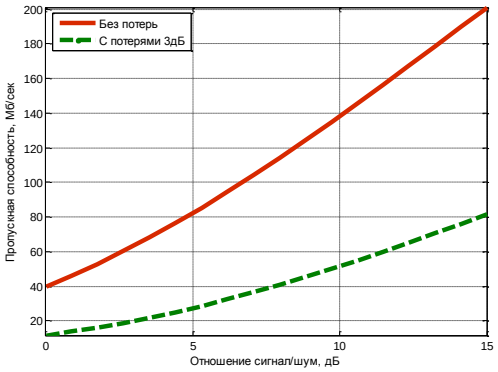


Рис. 6. Сравнения пропускной способности

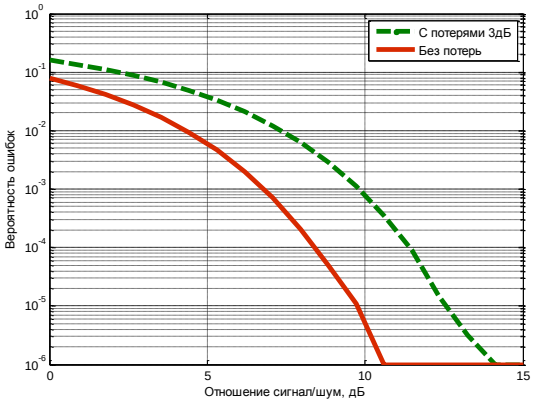


Рис. 7. Вероятности ошибок передачи

Заметим, что если пропускная способность реального канала с поляризационными потерями $3äÁ$ и при отношении сигнал/шум $10дБ$ достигает величины $55МБ/сек$ при вероятности ошибок $F \le 3 \cdot 10^{-4}$, то для предлагаемого канала с поляризационным ортогональным кодированием пропускная способность уже может быть увеличена примерно в 2,5 раза, до $140МБ/сек$ и при меньшей вероятности ошибок $F \le 6 \cdot 10^{-5}$.

Предложениями повышения пропускной способности MIMO системы являются следующие: организация разделения передаваемого потока на два ортогональные подпотока и излучение каждого из них на ортогональных поляризациях; организация полного поляризационного приема двумя поляризационно-ортогональными антеннами; оценка времени корреляции поляризационных параметров принятого сигнала; адаптивная оценка КМ принятого векторного сигнала; нахождение спектра и собственных векторов КМ и их анализ; составление матрицы преобразования из двух первых собственных векторов КМ; преобразование принятого векторного сигнала в его главные компоненты; восстановление информационного потока путем использования главных компонент принятого векторного сигнала.

Выводы. Разработанная математическая модель сигнала на выходе многоканального приемника с ортогональными поляризационными каналами MIMO системы позволяет предъявить требования к структурной схеме устройств обработки для обеспечения ортогонального поляризационного пространственно-временного кодирования. Результаты исследования свидетельствуют о возможности увеличения пропускной способности в 2,5 раза при меньшей вероятности ошибок благодаря разработанным предложениям, что представляет собой существенную практическую значимость. Дальнейшим направлением исследований является разработка требований к предельным нестабильностям технических характеристик устройств обработки, к параметрам разноканальности и разнофазности поляризационных каналов передачи с ортогональным поляризационным пространственно-временным кодированием.

Литература:

1. Родимов А.П., Поповский В.В. Статистическая теория поляризационно-временной обработки сигналов и помех. – М.: Радио и связь, - 1984. – 272 с.

2. Многоканальная электросвязь и телекоммуникационные технологии: Учебник для студентов высших учебных заведений / Под общ. ред. В. В. Поповского. — Харьков: ООО «Компания СМИТ», 2006. — 596 с. — На рус. яз.

ANALYSIS FEATURES PARAMETERS OF POLARIZATION ORTOGONAL ANTENNAE FOR MIMO SYSTEM

Мартынчук А.А., Абдуллах Икрам Кадир
Харьковский национальный университет радиоэлектроники,
61145 г. Харьков, ул.Клочковская 186-Б кв.205, тел. моб.: 050-402-52-97,
Email: alexmartynchuk@rambler.ru

In this article was derived method of finding the field components of the antenna signal and background noise, or processing in antenna with full polarization receiver. This will result to increase of bit rate of MIMO system on the basis of the use of polarization properties of signals, in the case of a real product. MIMO technology with orthogonal polarizing channels additional provides increase signal to noise ratio and therefore increase in bit rate in wireless.

Introduction. In radio, multiple-input and multiple-output, or MIMO is the use of multiple antennae at both the transmitter and receiver to improve communication performance.

Main disadvantage of Wi-Fi system with MIMO technology is loss of energy due to polarization effects, and then parameter of receiver antenna isn't equal to parameter of signal. It is interesting to increase bit rate (BR) and decrease bit error rate (BER) in wireless communication by use the orthogonal polarization antennae. In this case the total loss of energy may decrease.

Essence. MIMO technology with orthogonal polarizing channels additional provides increase signal to noise ratio and therefore increase in bit rate in wireless [1].

In radio, multiple-input and multiple-output, or MIMO is the use of multiple antennae at both the transmitter and receiver to improve communication performance. It is one of several forms of smart antenna technology (fig. 1).

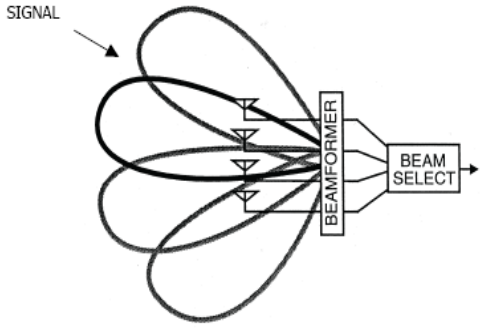


Fig. 1. Multiple antenna

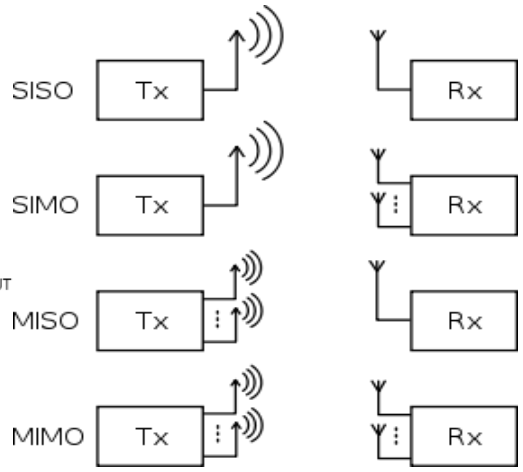


Fig. 2. MIMO smart antenna technology

MIMO technology has attracted attention in wireless communications, because it offers significant increases in data throughput and link range without additional bandwidth or transmit power. It achieves this by higher spectral efficiency (more bits per second per hertz of bandwidth) and link reliability or diversity (reduced fading). Because of these properties, MIMO is an important part of modern wireless communication standards such as IEEE 802.11n (Wi-Fi), 4G, 3GPP Long Term Evolution, WiMAX.

The signal on the receiving party is recorded as follows:

$$X = H \cdot S + Z, \quad (1)$$

where S – matrix of transmitted signals;

Z – matrix of a self-noise of the receiving elements of the antenna;

X – matrix of the received signals;

H – transformer matrix of the signals.

Most the simple and widespread matrix H is the Allamouti matrix.

Real antennae in MIMO technology can be represent like two input (top) and one output (bottom) antennae in Fig. 3 and this antennae can use at orthogonal polarization for better signal to noise ratio (SNR).

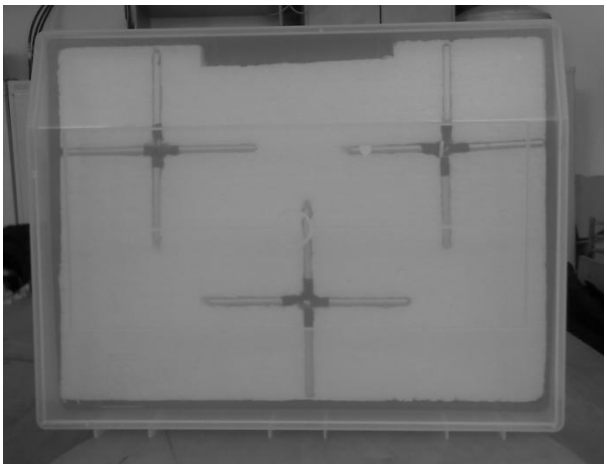


Fig. 3 – Real experimental polarization antenna for MIMO

Its explain result of analysis differences of signal and noise polarizing parameters. Polarization is spatial - temporal characteristics of electromagnetic waves, it notes the spatial pattern of targeting vector voltage electric or magnetic field over the rotor vibration. For homogeneous plane wave vector voltage electric and magnetic fields lie in the plane perpendicular to the direction of wave motion. Depending on whether parameters change (angle of orientation - β and angle of ellipse α) with the influence of polarization diagrams at time or remain constant, electromagnetic waves are divided into three groups: 1- completely polarized (polarization factor m=1); 2 - partially polarized (0<m<1); 3 – neutral or chaotic (m=0). Consider the wave of elliptical polarization in the free linear basis and E_x E_y orthogonal projection of the electric field vector E in form

$$E_x(t) = E_0 \cdot \exp\{j(\omega \cdot t + \varphi_x)\}, \tag{2}$$

$$E_y(t) = E_0 \cdot \exp\{j(\omega \cdot t + \varphi_y)\}. \tag{3}$$

Represent wave in matrix form:

$$\vec{E}_w(t) = \left(E_x(t) \quad E_y(t)\right)^t. \tag{4}$$

Polarization ellipse is defined by its shape (α), orientation axis (β) relative coordinate system selected and direction of rotation vector of the ellipse. The total form of wave is next

$$\vec{E}_w(t) = \begin{pmatrix} \cos(\beta) & \sin(\beta) \\ -\sin(\beta) & \cos(\beta) \end{pmatrix} \cdot \begin{pmatrix} \cos(\alpha) & -j\sin(\alpha) \\ -j\sin(\alpha) & \cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} E_0 \\ 0 \end{pmatrix} \cdot \exp\{j(\omega \cdot t + \varphi_0)\}. \tag{5}$$

Input signal for real experimental polarization antenna for MIMO (fig. 3) is represented by

$$\vec{E}_{in}(t) = \left(E_{1x}(t), \quad E_{1y}(t), \quad E_{2x}(t), \quad E_{2y}(t)\right)^t. \tag{6}$$

Difference of polarization parameters between antennae and real signal described by loss of energy factor

$$P_{loss} = \cos^{-1}\left(\vec{E}_s, \quad \vec{E}_{in}\right). \tag{7}$$

Depends on Bit Rate (C) to SNR and polarization loss at real as shown in fig. 4 solved by formula

$$C = F \cdot \log_2(1 + SNR). \tag{8}$$

Results of comparison real experiment and computerized result. Results of comparison real experiment of Alamouti/MRC algorithms [2] with 2x2 multiplexing without orthogonal

polarization antennae are in Fig. 4. We find, that BER is close to 0.01 at 10dB SNR for spatial multiplexing – QPSK and ML receiver (maximum likelihood).

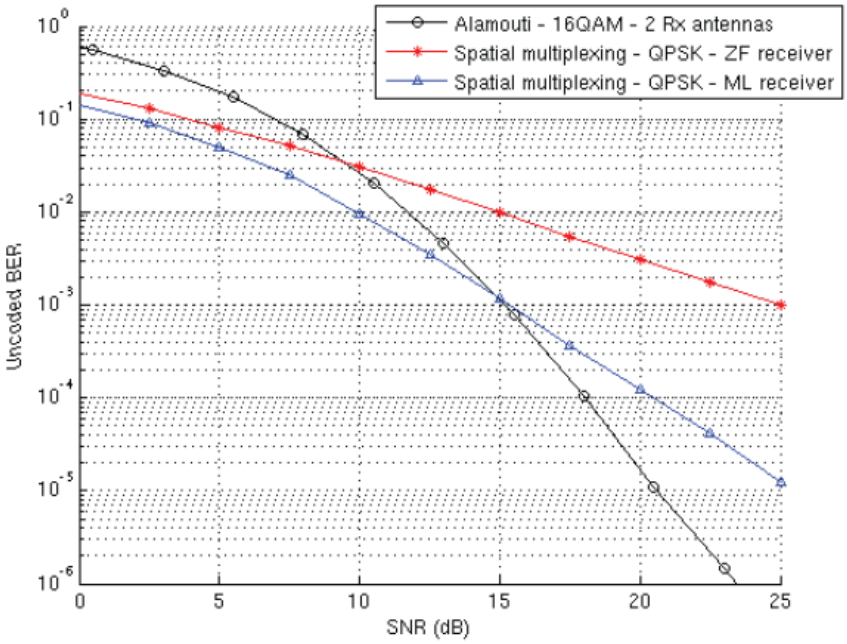


Fig. 4. Comparision of Alamouti/MRC with 2x2 multiplexing

Computerized results with orthogonal polarization antennae with parameters – angle of orientation – β=70^0 and angle of ellipse α=15^0 and polarization factor m=0.9) are in Fig. 5. Here we will show the spatial multiplexing – QPSK and ML receiver (PM 6dB loss) without orthogonal polarization antennae [3] and (PM) with orthogonal polarization antennae. We find that BER are close to 0.098 at 10dB SNR and polarization loss energy at 6 dB. We find too, that BER are close to 10^{-5} with orthogonal polarization antennae and without polarization loss energy.

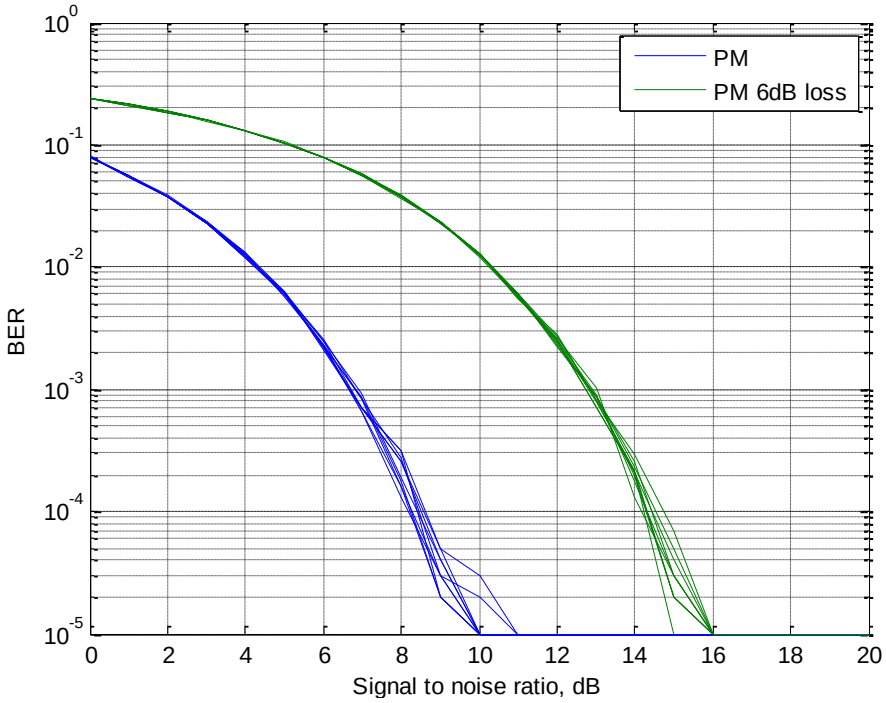


Fig. 5. Depends on BER to SNR

BR computerized results for same conditions are show in Fig.6. Analysis of the graphs are indicates that at SNR 10 dB BR is close to 11Mb/s with polarization losses of energy then BR is equal to 20MB/s without loss of energy by polarization due to use polarization orthogonal antennae.

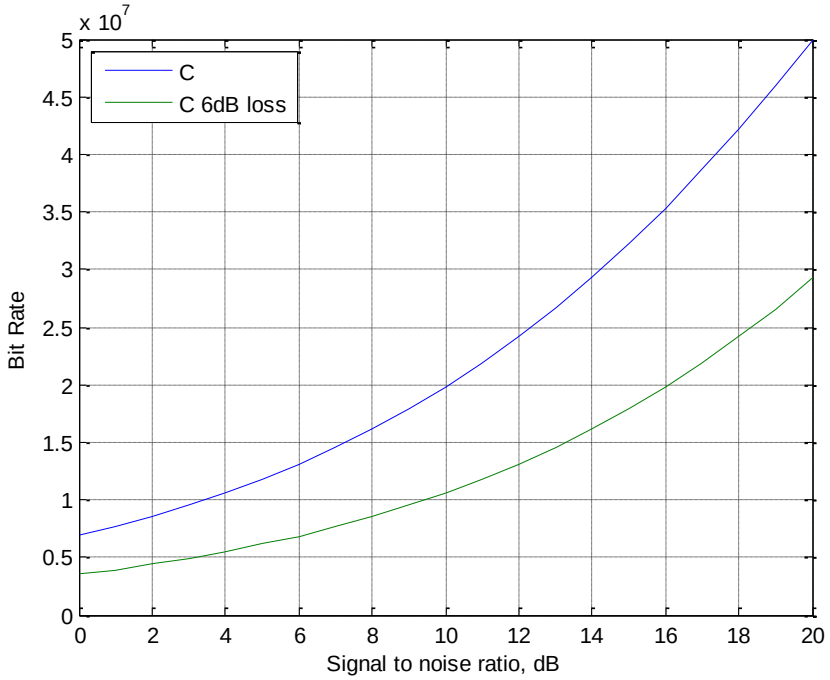


Fig. 6. Depends on BR to SNR

Conclusions. Result of experiment meaning that better BR without loss of energy at full polarization antennae. If BR is equal to 11Mb/s at SNR 10 dB at real and loss of energy at 6dB, then BR is equal to 20MB/s at SNR 10 dB and without loss of energy by polarization.

Basic suggestions on the use of polarization orthogonal aerials for increase Bit Rate in MIMO systems may be following:

need to use orthogonal polarization Antennae in conditions «without a line-of-sight»; in this case the total loss of energy may decrease;

need to knowing polarization parameters of signal in conditions «without a line-of-sight»;

the antennae construction needs to include double orthogonal polarization antennae;

the related algorithms are needed to use for channel additional antennae of orthogonal polarizations.

References

1.Бакулин М.Г., Крейнделин В. Б., Шлома А. М. Новые технологии в системах мобильной радиосвязи. — М:Ин.связь.издат, 2005.

2.W. Heath, Jr. and A. J. Paulraj, "Switching Between Diversity and Multiplexing in MIMO Systems," IEEE Trans. Commun., vol. 53, no. 6, pp. 962 – 968, June 2005.

3.Вишневский В.М. Широкополосные беспроводные сети передачи информации/В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И. В. Шахнович. – М.: Техносфера, 2005 – 592 с.

КЛАСИФІКАЦІЯ ТА АНАЛІЗ МЕТОДІВ РОЗПОДІЛУ ЧАСТОТНИХ КАНАЛІВ В БАГАТОКАНАЛЬНИХ MESH-МЕРЕЖАХ

Гаркуша С.В.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Леніна, 14, каф. телекомунікаційних систем, тел. (057) 702-55-92,
E-mail: sv.garkusha@mail.ru

Examined the existing methods of distribution the frequency channels in the multichannel mesh-networking standard, IEEE 802.11. The requirements for the structure and content of a mathematical model the frequency distribution of channels in a mesh-networks.

Вступ

Поява економічно ефективних безпроводових mesh-мереж (Wireless Mesh Networks, WMNs), на основі технології IEEE 802.11, істотно змінила процес організації безпроводових мереж доступу. На сьогоднішній день вже існують достатні докази того, що поточна модель доступу користувачів з використанням інфраструктури в режимі IEEE 802.11 добре підходить для мереж, що розгортаються в домашніх умовах і в межах невеликих підприємств. Дані мережі охоплюють обмежену територію з невеликим числом користувачів. Також зазначена модель підходить для мереж з високою щільністю точок доступу (Access Point, AP), які призначені для зв'язку користувачів на великій території. Транспортна мережна архітектура mesh-мереж має низку переваг, до яких слід віднести: надійність, масштабованість, рентабельність і простоту в розгортанні. Проте використання на рівні доступу до середовища (Media Access Control, MAC) протоколу IEEE 802.11 одноканального режиму, в більшості випадків призводить до обмеження пропускної спроможності мережі.

Найчастіше безпроводові mesh-мережі складаються із станцій, що мають у своєму складі по одному радіоінтерфейсу (РІ). Це призводить до того, що такі mesh-мережі не мають можливості ефективно масштабуватися, з метою збільшення доступної пропускної спроможності. Додатки до стандарту IEEE 802.11s дозволяють використовувати на кожній mesh-станції, як одного, так і декількох РІ. При цьому кожен з РІ може бути налаштований на окремий частотний канал (ЧК), утворюючи при цьому багатоканальний режим роботи. Наявність декількох РІ і відповідний розподіл ЧК між ними дозволяє знизити рівень інтерференції, яка призводить до значного уповільнення роботи з'єднання або навіть його відмови, збільшує пропускну здатність мережі, знижує затримки при передачі пакетів і ймовірність їх втрати. Зауважимо, що в стандарті IEEE 802.11s не визначено жодних алгоритмів розподілу ЧК між РІ mesh-станцій, що робить неможливим роботу mesh-мережі в багатоканальному режимі.

У зв'язку з цим актуальною є задача, пов'язана з вибором або розробкою моделей і методів розподілу ЧК між РІ станцій в багатоканальних mesh-мережах стандарту IEEE 802.11. Метою дослідження є забезпечення багатоканального режиму роботи і забезпечення необхідного рівня продуктивності безпроводової mesh-мережі за наявності декількох РІ на кожній з mesh-станцій мережі, а також при використанні доступного числа ЧК, що не перекриваються, для окремо взятої технології безпроводового зв'язку.

Класифікація методів розподілу частотних каналів в багатоканальних mesh-мережах стандарту IEEE 802.11

В даний час ведеться ряд досліджень, спрямованих на розробку методів розподілу ЧК в багатоканальних mesh-мережах. Вибір методу розподілу ЧК в багатоканальній mesh-мережі доцільно проводити виходячи з поставлених завдань. Необхідно зауважити, що всі відомі методи збігаються за певними ознаками, в результаті чого необхідно провести їх класифікацію. Дана класифікація проводиться з метою вибору найбільш ефективного методу розподілу ЧК в багатоканальних mesh-мережах (рис. 1).

По виду розглядаємої топології всю множину методів розподілу ЧК можна розділити на методи, які використовують деревоподібну топологію мережі, і методи, що

розбивають мережу на кластери. У методах, що використовують деревоподібну топологію мережі (наприклад [1]), кожна mesh-станція може працювати в двох режимах: «батьківської» станції і «дочірньої» станції. Станція є «батьківською», якщо вона розташована в ієрархії дерева на один рівень вище від «дочірньої» станції і відповідає за призначення ЧК між своїми «дочірніми» станціями. «Дочірня» станція може бути підключена до однієї «батьківської» станції. У методах, що розбивають всю множину станцій на кластери [2], в рамках кожного кластера виділяється керуюча станція - лідер, яка і відповідає за розподіл ЧК всередині кластера. Таким чином, в рамках кластера всі станції за винятком лідера рівноправні.

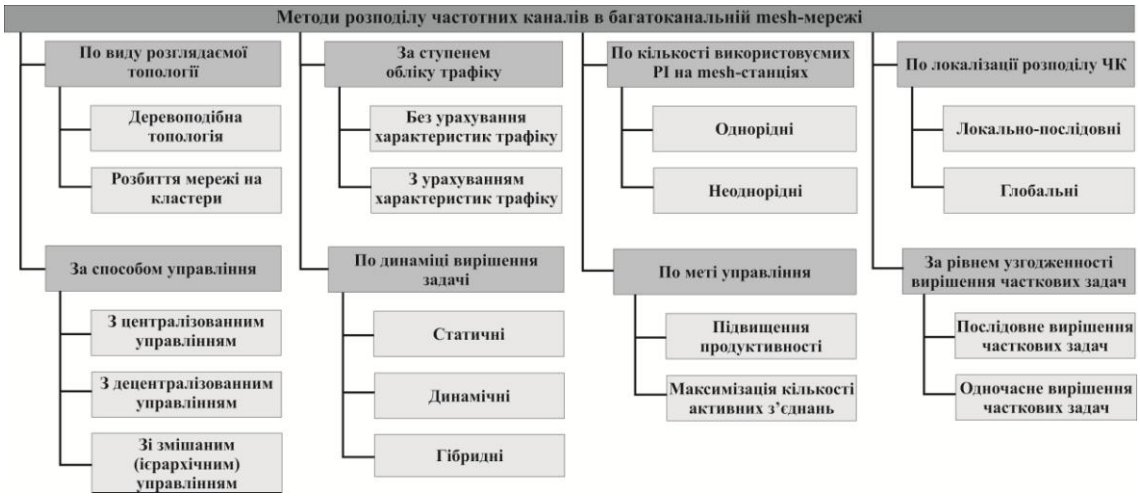


Рис. 1. Класифікація методів розподілу частотних каналів в багатоканальних mesh-мережах

Також всю множину методів по розподілу ЧК можна класифікувати за ступенем обліку трафіку, що циркулює в mesh-мережі. Розрізняють методи, які забезпечують розподіл ЧК з урахуванням характеристик трафіку, що передається в мережі [3], а також методи, в рамках яких подібний облік не проводиться [2, 4].

Крім цього, методи можна класифікувати по кількості використовуємих РІ на станціях безпроводової mesh-мережі. Можна виділити методи розподілу ЧК в однорідних mesh-мережах [2, 4], коли кількість РІ на всіх mesh-станціях мережі однакова. Також виділяються методи, які використовуються для неоднорідних mesh-мереж [2], коли кількість РІ на різних mesh-станціях мережі може відрізнятися.

Методи розподілу ЧК можна також класифікувати за способом управління. При цьому можна виділити методи з централізованим управлінням [5], при якому весь контроль за розподілом ЧК виконується єдиною станцією. Також виділяються методи з децентралізованим управлінням [1, 2, 4], коли кожна станція може приймати рішення про призначення ЧК на свої РІ самостійно. Крім того, виділяються методи зі змішаним (ієрархічним) управлінням, в яких за призначення ЧК можуть відповідати кілька станцій мережі, наприклад, всі лідери кластерів, а їх робота координується mesh-станцією - лідером мережі [2].

Методи розподілу ЧК в багатоканальній мережі можна також розділити по динаміці вирішення задачі розподілу ЧК. При цьому виділяються методи статичного розподілу ЧК [1, 2, 4, 5], коли призначення ЧК здійснюється одноразово , як правило, на етапі проектування mesh-мережі, або перепризначення ЧК на РІ відбувається досить рідко. Також виділяються методи динамічного розподілу ЧК [6], коли канали перерозподіляються в реальному часі - за вимогою або періодично. Необхідно також виділити гібридні методи [7], коли частина ЧК переключається з певним періодом, а частина ЧК переключається за вимогою.

Методи розподілу ЧК можна класифікувати по меті управління. При цьому виділяються методи, орієнтовані на максимізацію кількості активних двонаправлених з'єднань між станціями mesh-мережі [4]. Також існують методи, що виконують розподіл ЧК з метою підвищення продуктивності безпроводової mesh-мережі в цілому [2, 3]. У ході розподілу ЧК можуть використовуватися й інші критерії.

Крім того, проаналізовані методи можна класифікувати по локалізації розподілу ЧК. При цьому можна виділити локально-послідовні методи, що знаходять рішення з розподілу ЧК послідовно для кожної окремо взятої станції або групи станцій mesh-мережі [1, 3-5]. Також виділяються так звані глобальні методи [2], які знаходять рішення з розподілу ЧК між усіма mesh-станціями мережі в цілому.

Нарешті, всю множину проаналізованих методів можна класифікувати за рівнем узгодженості вирішення часткових задач розподілу ЧК. При цьому в ролі часткових можуть виступати наступні задачі [2, 5]:

1) розбиття mesh-мережі на кластери;

2) розподіл PI mesh-станцій між кластерами;

3) закріплення ЧК за кожним з PI mesh-станцій.

При цьому виділяються методи, в яких загальна задача розподілу ЧК вирішується шляхом послідовного вирішення окремих задач [5]. Також можна виділити методи, в рамках яких задача розподілу ЧК вирішується в цілому, забезпечуючи одночасне і максимально узгоджене вирішення часткових задач [2].

Наведена класифікація (рис. 1) дозволила констатувати наявність достатньо широкого спектру підходів до постановки та вирішення задачі розподілу ЧК в багатоканальних mesh-мережах стандарту IEEE 802.11. Важливо розуміти, що ефективність того чи іншого методу багато в чому визначається покладеною в його основу математичною моделлю, яка максимально адекватно описує процес розподілу ЧК. Відповідно до проведеного огляду, в якості основних можна сформулювати наступні вимоги до структури та змісту математичної моделі розподілу ЧК в mesh-мережах, що доповнюють перелік вимог, наведених у роботі [2]:

- інваріантність розглядаємої топології mesh-мережі;
- орієнтація переважно на динамічний характер рішення задачі розподілу ЧК;
- облік типу і характеру циркулюючого в mesh-мережі трафіку;
- облік неоднорідності сучасних mesh-мереж за рахунок використання обладнання різних модифікацій, серій і підприємств-виробників;
- орієнтація на максимізацію продуктивності mesh-мережі в цілому;
- забезпечення узгодженого рішення задачі розподілу ЧК одночасно для всіх станцій mesh-мережі.

Крім того, важливо розуміти, що чим більше особливостей і закономірностей у побудові і функціонуванні mesh-мережі опише математична модель, тим ефективнішим буде технологічне рішення, спрямоване на вирішення задачі розподілу ЧК. «Недоліки» в математичному описі, як правило, супроводжуються ускладненням відповідного протоколу. Наприклад, якщо в рамках математичної моделі та методу при вирішенні задачі розподілу ЧК не запобігти виникненню ефекту «прихованої станції», то для боротьби з цим явищем потрібно буде залучати додаткові витрати, але вже технологічного рівня - CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) і RTS/CTS (Request To Send / Clear To Send), що основані на таймерах і тимчасових відмовах від передачі, та супроводжуються зниженням продуктивності mesh-мережі в цілому.

Тому використовуєма модель повинна забезпечувати [2]:

- узгоджене вирішення задач кластеризації, виділення PI на mesh-станціях і закріплення за ними ЧК, що не перекриваються;
- облік технологічних особливостей мережі, які визначають дальність зв'язку, інтенсивність надходження в мережу абонентського трафіку, кількість використовуємих ЧК, що не перекриваються, тощо;
- запобігання виникнення ефекту «прихованої станції»;

- облік територіальної віддаленості mesh-станцій, їх активності, потужності, кількості підтримуємих mesh-станцією PI і т.д.

Вищенаведеним вимогам найбільш повно відповідає модель розподілу ЧК, представлена в роботі [2]. Однак трьохіндексний характер моделі визначає високу розмірність задачі з розподілу ЧК в mesh-мережі, вирішення якої необхідно забезпечувати в реальному часі. Тому актуальною є задача, пов'язана з модифікацією раніше відомої моделі з метою зниження її розмірності і очікуваним підвищенням масштабованості технологічних рішень щодо розподілу ЧК в багатоканальній mesh-мережі.

Висновки

Однією з основних задач у багатоканальних mesh-мережах є задача розподілу частотних каналів між радіоінтерфейсами mesh-станцій. У зв'язку з цим проаналізовані існуючі методи розподілу частотних каналів в багатоканальних mesh-мережах і наведена їх класифікація. При цьому встановлено, що методи розподілу частотних каналів в багатоканальних mesh-мережах можна класифікувати: по виду розглядаємої топології, за ступенем обліку трафіку, за кількістю радіоінтерфейсів на mesh-станціях, за способом управління, за динамікою вирішення задачі розподілу частотних каналів, по цілі управління, за локалізацією розподілу частотних каналів, за рівнем узгодженості вирішення часткових задач розподілу частотних каналів. Також, в результаті аналізу відомих рішень встановлено, що практично всі з них використовують в якості основи деякі евристики.

Література:

1. *Raniwala A., Tzi-cker Chiueh*. Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network // Proc. of INFOCOM. – 2005. – Vol.3. – P. 2223-2234.
2. *Лемешко А.В., Гоголева М.А.* Модель структурной самоорганизации многоканальной mesh–сети стандарта IEEE 802.11 [Электронный ресурс] // Проблеми телекомунікацій. – 2010. – № 1 (1). – С. 83–95. – Режим доступа к журн.: http://pt.journal.kh.ua/2010/1/1/101_lemeshko_mesh.pdf.
3. *Naveed A., Salil S. Kanhere, Sanjay K. Jha*. Topology Control and Channel Assignment in Multi-radio Multi-channel Wireless Mesh Networks // Proc. of MASS. – 2007. – P. 1-9.
4. *Das A.K, Alazemi H.M.K., Vijayakumar R., Roy S.*, Optimization models for fixed channel assignment in wireless mesh networks with multiple radios // IEEE SECON. – 2005. – P. 463–474.
5. *Raniwala A., Gopalan K., Chiueh T.* Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks // ACM Mobile Computing and Communications Review. – 2004. – Vol.8. – P. 50–65.
6. *Bahl P., Chandra R., Dunagan J.* SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks // Proc of ACM Mobicom. – 2004. – P. 216–230.
7. *Kyasanut P., Vaidya N.* Routing and Link-layer Protocols for Multi-Channel Multi-Interface Ad Hoc Wireless Networks // Mobile Comp. and Commun. Rev. – 2006. – Vol.10, No.1. – P. 31–43.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РАДІОІНТЕРФЕЙСУ БЕЗПРОВІДНИХ СИСТЕМ НАСТУПНОГО ПОКОЛІННЯ

Яремко О.М., Максимюк Т.А., Кричко Д.І.
Національний університет "Львівська політехніка"
79013, Львів, вул.Професорська,2, каф. "Телекомунікації"
E-mail: taras_maks@ukr.net, тел.(032) 258-24-44

In this report, we provide a comparative study of state-of-the-art in Orthogonal Frequency Division Multiplexing techniques. Two main categories, OFDM/QAM which adopts baseband Quadrature Amplitude Modulation and rectangular pulse shape, and OFDM/OQAM which uses baseband offset QAM and various pulse shapes. OFDM/QAM can provide high data rate communication and effectively remove intersymbol interference by employing guard interval, which costs a loss of spectral efficiency and increases power consumption. In order to achieve better spectral efficiency, OFDM/OQAM using well designed pulses with proper Time Frequency Localization is of great interest.

Another way to wireless systems efficiency increasing, is MIMO antennas implementation. In up-to-date wireless systems the most common using acquired MIMO 2x2 and 4x4 schemes.

Вступ

Протягом останніх десятиріч системи безпровідного зв'язку характеризуються інтенсивним розвитком. Тому актуальним є дослідження принципів побудови та функціонування сучасних безпровідних систем, в тому числі систем наступного покоління. Сьогодні робота над розробкою концепції систем радіозв'язку наступних поколінь ведеться під загальноприйнятим терміном LTE (Long Term Evolution).

Системи LTE передбачають використання радіоінтерфейсу HSOPA(High Speed OFDM Packet Access), що базується на технології OFDM, а також застосування багатоантенних систем MIMO. Зокрема, в 3GPP Release 7 [1] передбачається використання до 4 антен на приймання та передавання.

Особливості технології OFDM

Технологія ортогонального частотного мультиплексування OFDM (Orthogonal Frequency Division Multiplexing) передбачає формування багаточастотного сигналу, який складається з певної кількості піднесучих частот, які відрізняються на величину, вибрану з умови ортогональності сигналів на сусідніх піднесучих коливаннях.

Метою такого перетворення є усунення впливу багатопроменевого розповсюдження радіохвиль та впливу міжсимвольної інтерференції, за рахунок захисного часового інтервалу. Захисний інтервал тривалістю 0.2 від тривалості символу суттєво погіршує спектральну ефективність, яка для OFDM/QAM системи становить:

$$\eta = (1-\frac{T_g}{T_s})\log_2 M, \frac{біт/с}{Гц}, \quad (1)$$

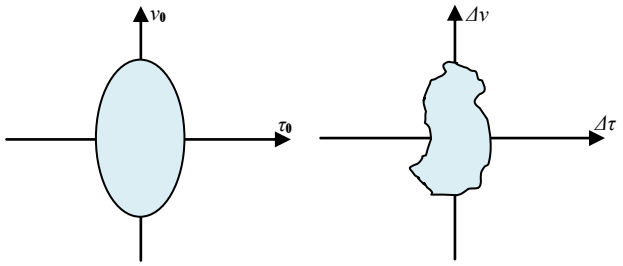
де T_g – тривалість захисного інтервалу, T_s – тривалість OFDM символу, M – кількість позицій для M-QAM модуляції.

В роботі проаналізовано можливість реалізації системи без захисних інтервалів, якщо використати прототип (функція на яку перемножується модульований символ при формуванні OFDM сигналу) з кращою локалізацією енергії, у порівнянні із прямокутним імпульсом, що використовується в OFDM/QAM. Локалізація сигналу – частотно-часовий параметр який визначає тривалість передаваного символу, та його ширину спектру. Чим краща локалізація, тим ефективніший розподіл корисної енергії, і відповідно краща спектральна ефективність.

Умова ідеальної локалізації записується наступним чином [2]:

$$\frac{\tau_0}{\Delta\tau} = \frac{\nu_0}{\Delta\nu} \quad (2)$$

де τ_0,ν_0 – часова і частотна локалізація відповідно, а $\Delta\tau$,$\Delta\nu$ – часова і частотна дисперсія каналу зв'язку. На рис.1 показано ідеальну локалізацію та частотно-часову дисперсію безпровідного каналу. Як видно з рисунку, умови в каналі не дозволяють передавати енергію без втрат, тому виникає необхідність пошуку прототипів, які б забезпечили оптимальну локалізацію.



а) б)

Рис.1 Локалізація сигналу(а) та частотно-часова дисперсія безпровідного каналу зв'язку (б)

Властивості локалізації вузькосмугових сигналів в глобальному контексті підкоряються обмеженням теореми Балліана-Лоу [3]. Згідно з властивістю некомутативності частотно-часової площини, неможливо незалежно маніпулювати тривалістю і шириною спектру сигналу, для досягнення найкращої локалізації, оскільки:

$$\tau_0 \cdot \nu_0 < 1 \tag{3}$$

Оскільки при використанні модуляції OFDM/QAM, умова (3) не виконується:

$$\tau_0 \cdot \nu_0 = 1, \tag{4}$$

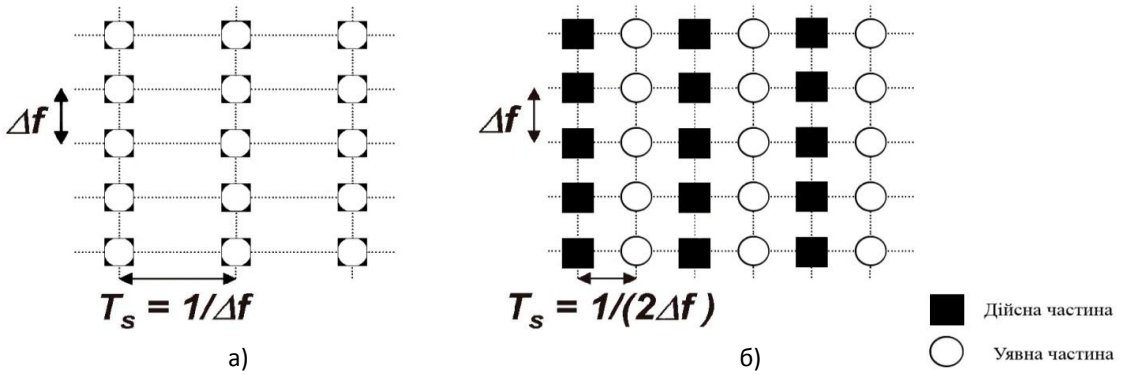
застосування добре локалізованих прототипів (функція "півкосинус", функція Гауса, або IOTA-функція) є неможливим.

Одним з варіантів вирішення даної проблеми є застосування квадратурно амплітудної модуляції із зсувом - Offset QAM (OQAM) [4]. За рахунок ущільнення сигналу за часом OQAM значно розширює можливості локалізації сигналу.

При формуванні сигналу OFDM/OQAM символи QAM (c_{mn}) розділяються на дві складові: дійсну частину $\mathrm{Re}\{c_{mn}\} = a_{mn}$ і уявну $\mathrm{Im}\{c_{mn}\} = b_{mn}$, причому уявна частина зсувається в часі на величину $T_s/2$ щодо дійсної (рис.2).

Тобто кількість переданої інформації не змінюється, а просто ділиться на дві частини протягом того ж інтервалу часу.

$$T_s = 1/2\Delta f \tag{5}$$



а) б)

Рис.2. Частотно-часова матриця сигналів OFDM/QAM (а), і OFDM/OQAM (б)

З рис.2 видно, що при застосуванні OFDM/OQAM подвоюється символьна швидкість, вдвічі зменшується кількість інформації на один модуляційний символ, а швидкість передавання інформації залишається незмінною.

При використанні квадратурно-амплітудної модуляції із зсувом виконується умова теореми Балліана-Лоу, за рахунок меншого інтервалу між символами:

$$\tau_0 \cdot \nu_0 = 1/2 \tag{6}$$

Це дозволяє використовувати прототипи з кращою локалізацією, і відповідно не використовувати захисні інтервали.

В табл. 1 наведено основні відмінності між QAM і OQAM при їх застосуванні в системах з OFDM.

Таблиця 1

Ключові відмінності модуляції зі зсувом і традиційної QAM

Параметр	**OFDM/QAM**	**OFDM/OQAM**
Символ	Комплексний	Дійсний
Захисний інтервал	Потрібний	Не потрібний
Тривалість символу	T_s+CP(захисний інтервал)	$T_s/2$
Прототип	Прямокутний імпульс	IOTA-функція, “півкосинус” функція Гауса
Реалізація	ШПФ	ШПФ + багатофазна фільтрація

Моделювання та дослідження ефективності радіоінтерфейсів безпровідних систем наступного покоління

За рахунок прототипу з кращою локалізацією, Offset OAM має кращі показники енергетичної та спектральної ефективності. Теоретично це має дати певний виграш в завадозахищеності, тому були проведені дослідження на основі створеної імітаційної моделі. Отримано залежності імовірності появи бітових помилок від співвідношення “сигнал/шум” для різних варіантів M-QAM та M-OQAM (рис. 3).

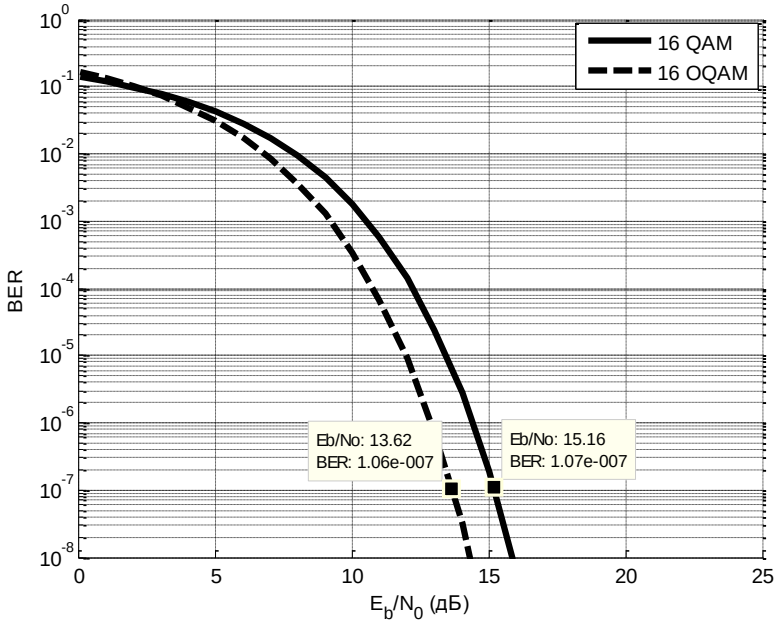


Рис.3. Залежність BER від Eb/No для кількості позицій модульованого сигналу M=16

Якщо прийняти, що коефіцієнт появи бітових помилок залишиться сталим, то можна забезпечити ту ж саму якість передавання в умовах гірших радіоканалів, або збільшити дальність дії радіоканалу.

Впровадження OQAM модуляції в поєднанні з OFDM, дозволяє суттєво підвищити швидкість передавання за рахунок усунення захисних інтервалів. Формула (1) в такому випадку запишеться так:

$$\eta' = \log_2 M, \frac{біт/с}{Гц} \qquad (7)$$

Відповідно швидкість передавання OFDM символів, зросте в k разів:

$$k = \frac{\eta'}{\eta} \qquad (8)$$

В системі OFDM/QAM, захисний інтервал зазвичай становить 0.2 T_s. Отже для даного випадку k=1.2.

Для підвищення швидкості передавання поряд з OFDM в системах LTE пропонується використовувати багатоантенні системи Multiple Input Multiple Output(MIMO). На основі імітаційної моделі проведено аналіз різних алгоритмів обробки вхідних сигналів системами з просторовим рознесенням та досліджено варіанти конфігурації таких систем. В табл.2 наведено пікові значення швидкості передавання найпоширеніших конфігурацій MIMO: 2x2, та 4x4 у порівнянні з однією антеною, для випадку 64 OQAM модуляції.

Таблиця 2

Пікові значення швидкості передавання OFDM системи, Мбіт/с

Смуга	1.4 МГц	3 МГц	5 МГц	10 МГц	15 МГц	20 МГц
Кількість піднесучих	72	180	300	600	900	1200
Одна антена	6,06	15,16	26,16	53,66	80,16	107,66
MIMO 2x2	12,71	30,26	50,54	102,74	153,63	206,13
MIMO 4x4	21,32	56,69	96,33	193,93	292,53	390,13

Висновки

Проведені дослідження показують перевагу застосування модуляції із зсувом над традиційною QAM в системах LTE. Зокрема, при забезпеченні аналогічного показника BER при використанні OQAM можна на 12% знизити співвідношення "сигнал/шум", у порівнянні з QAM модуляцією.

Крім того, модуляція зі зсувом, дозволяє не використовувати захисні інтервали між OFDM символами за рахунок кращої частотно-часової локалізації сигналу. Це дає змогу підвищити швидкість передавання символів на 20%.

Для ефективнішої роботи системи доцільно вдосконалювати алгоритми обробки сигналів багатоантенними системами, а також смарт-антенами. Використання систем MIMO дозволяє суттєво збільшити швидкість передавання в системі за рахунок одночасного передавання інформації кількома антенами, а також підвищити її завадозахищеність.

Згідно з одержаними результатами можна зробити висновок про те, що оптимальне поєднання OFDM/OQAM та технології MIMO дозволить підвищити ефективність функціонування безпровідних систем наступного покоління.

Література:

1. 3GPP TR 25.913 Requirements for Evolved UTRA and Evolved UTRAN, Release 7, V7.3.0, 2006.
2. T. Strohmer and S. Beaver, Optimal OFDM Design for Time-Frequency Dispesive Channels, IEEE Transactions on Communications, vol. 51, pp. 1111-1123, Jul. 2003.
3. John J. Benedetto, Christopher Heil, and David F. Walnut, Differentiation and the Balian–Low Theorem, Journal of Fourier Analysis and Applications, Volume 1, Number 4: 355–402.,1994.
4. 3GPP TR 25.892 Feasibility Study for OFDM for UTRAN enhancement, Release 6, V2.0.0, 2004.

К ВОПРОСУ ПОВЫШЕНИЯ КАЧЕСТВА ОБРАБОТКИ АКУСТИЧЕСКИХ СИГНАЛОВ

Пастушенко Н.С., Пастушенко А.Н.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: tkc@khture/kharkov/ua, факс (057) 702-55-92

Procedures and results of processing of real audible tones which testify to substantial increase of a signal/noise ratio of an analyzed timed sequence are resulted.

Известные методы анализа цифровых данных в виде временных рядов ориентированы на обработку линейных и стационарных сигналов. Только в конце прошлого тысячелетия начали развиваться методы анализа нелинейных, но стационарных и детерминированных систем, и линейных, но нестационарных данных (Вейвлет анализ, распределение Wagner-Ville и др.). Между тем, большинство регистрируемых сигналов от реальных физических систем в той или иной мере являются нелинейными и нестационарными. Несмотря на ограничения, доказанные достаточно давно в известных теоремах Бедрозиэна и Наттолла, анализ этих сигналов осуществляется традиционными методами, полагая справедливыми упрощения, особенно относительно базиса (как правило, гармонического) обрабатываемых данных.

Известно, что качество результатов цифровой обработки во многом зависит от возможностей регистрации (или восстановления) приемным устройством параметров аналитического (комплексного) сигнала и в первую очередь, его квадратурной составляющей. В ряде радиотехнических приложений (радиосвязь, активная радиолокация, радионавигация и т.д.) квадратурная составляющая (мнимая часть) может быть сформирована аппаратно, например, с помощью фазового детектора. В этом случае, как правило, известно и используется опорное колебание. При этом предполагается, что все составляющие частотных спектров вещественной и квадратурной частей аналитического сигнала имеют фазы, различающиеся на 90^{o}.

Регистрация вещественной и восстановление квадратурной составляющей, а также уточнение в процессе расчетов большинства параметров аналитического сигнала дает возможности использовать, например, преимуществ пространственно-временной обработки и достигать более высокого качества цифровой обработки данных в радиотехнических приложениях.

Вместе с тем, в ряде приложений, таких как акустика, сейсмология, пассивная радиолокация (радиоразведка, радиоперехват излучений), гидролокация регистрируется только вещественная часть сигнала с неизвестным несущим колебанием и она подвергается цифровой обработке, что существенно ограничивает ее возможности.

При необходимости квадратурная часть формируется с помощью фильтров (аппаратных или программных), которые выполняют функции фазовращателя или быстрого преобразования Фурье. Следует отметить, что эти процедуры базируются на преобразовании Гильберта.

Вместе с тем, со средины девяностых годов прошлого столетия делаются попытки разработки процедур обработки нелинейных нестационарных сигналов. Процедуры EMD-HSA (эмпирический метод декомпозиции – Гильбертов спектральный анализ) были предложены Норденом Е. Хуангом в 1995 в США (NASA) для изучения поверхностных волн тайфунов, с обобщением на анализ произвольных временных рядов коллективом соавторов в 1998 г. К сожалению, справедливость указанных процедур теоретически не доказана. Предложенные эмпирические процедуры ориентированы на формирование адаптивного базиса на основе обрабатываемых данных, а затем к этому базису применяется преобразование Гильберта. Такой подход позволяет более точно восстановить квадратурную составляющую анализируемого сигнала. К сожалению, имеют место значительные краевые эффекты и ошибка аппроксимации с помощью формируемого базиса, а также неточности, обусловленные преобразованием Гильберта.

В докладе анализируются возможности процедур EMD-HSA на примере обработки зашумленных акустических сигналов с целью повышения отношения сигнал/шум регистрируемого сигнала и более точного восстановления его квадратурной составляющей.

В качестве контрольного сигнала будем использовать акустический сигнал x_i, например, формируемый с помощью телефонной гарнитуры и программы «Звукозапись» из группы «Стандартные / Развлечения». Здесь i = 1,…,N – номер анализируемого отсчета, N – объем анализируемой выборки. Имея контрольный сигнал x_i, с помощью последовательности белого шума, можем получить аддитивную смесь x_i и шума (y_i) с требуемым отношением сигнал/шум, которую будем подвергать дальнейшей цифровой обработке.

Эмпирическая декомпозиция сигналов, предложенная Н. Хуангом, основана на предположении, что любые данные состоят из различных режимов (процессов) колебаний. В любой момент времени данные могут содержать различные сосуществующие режимы колебаний. Любой режим, линейный или нелинейный, стационарный или нестационарный, представляет простое колебание, которое имеет экстремумы и нулевые пересечения. Кроме того, колебание будет в определенной степени «симметрично» относительно локального среднего значения. Результат – конечные сложные данные.

Каждый из этих колебательных режимов может быть представлен «существенной функцией» (intrinsic mode function - IMF).

EMD - высокоадаптивный метод анализа нелинейных и нестационарных сигналов. Его главное преимущество в том, что базис, используемый при разложении (набор эмпирических мод) конструируется непосредственно из тех данных (того сигнала), с которым ведется работа. Это позволяет учесть все его локальные особенности, внутреннюю структуру, наличие нежелательных особенностей (шумы, тренды, аномальные выбросы, пропущенные значения). EMD обладает важными для практических приложений свойствами: ортогональность, локальность, полнота и адаптивность. Важно, что строго ни ортогональность, ни полнота пока не доказаны, и это является одной из важнейших теоретических проблем данного метода.

Эмпирическая мода – это такая функция, которая обладает следующими свойствами:

- общее число экстремумов должно равняться числу нулей с точностью до 1;
- среднее значение 2-х огибающих – верхней, интерполирующей локальные максимумы, и нижней – интерполирующей локальные минимумы должно быть равно нулю.

IMF представляет собой колебательный режим, как часть простой гармонической функции, но вместо постоянной амплитуды и частоты, как в простой гармонике, у IMF могут быть переменная амплитуда и частота, как функции времени. Любую функцию и любой произвольный сигнал можно разделить на семейство функций IMF, придерживаясь изложенной ниже методики.

Выделяем массивы максимумов и минимумов из анализируемого ряда y_i, которые служат исходными данными для вычисления с помощью кубического сплайна верхней и нижней огибающих сигнала. Далее определяется функция средних значений m_{1i} между огибающими. Затем из анализируемого сигнала вычитается m_{1i}. В результате находим первое приближение к первой функции IMF – c_{1i}, которая включает высокочастотные составляющие анализируемого сигнала.

Полученная IMF удаляется из анализируемого сигнала, а остаток обрабатывается по методике изложенной выше. Акустический сигнал, как правило, включает девять IMF. При этом в трех первых сосредоточен сигнал белого шума, который целесообразно отбросить. Шесть оставшихся IMF включают компоненты акустического сигнала, которые в последующем подвергаются преобразованию Гильберта с помощью известных процедур.

В качестве критерия качества восстановления акустического сигнала использовался коэффициент корреляции между последовательностями восстановленного и контрольного сигналов. Более сложно оценить качество восстановления квадратурной составляющей, поскольку отсутствует эта составляющая для контрольного акустического

сигнала. В тоже время, обрабатываемые компоненты акустического сигнала с помощью преобразования Гильберта являются более гладкими, что дает право надеяться на более точное восстановление квадратурной составляющей.

В заключение приводятся результаты обработки реальных акустических сигналов, которые свидетельствуют о значительном повышении отношения сигнал/шум анализируемой последовательности, а также предлагаются направления дальнейших исследований.

ИСПОЛЬЗОВАНИЕ КРИТЕРИЯ *PSNR* ДЛЯ ОЦЕНКИ КАЧЕСТВА ПЕРЕДАЧИ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИ В СИСТЕМЕ БЕСПРОВОДНОГО ДОСТУПА *WiMAX*

Ивженко А.В., Цопа А.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. основ радиотехники, тел. (057) 702-15-87,
E-mail: rty6061944@gmail.com

The given work is about of searching in field of transmission of multimedia data through wireless radio systems, based on *OFDM*-modulation technique, such like *WiMAX*. In this work is given a mathematical model of a system and a radio channel; block of estimation of errors. Based on the model`s results, proposed to add and apply *PSNR* measure in systems of transmission of multimedia data.

На сегодняшний день наиболее распространенной метрикой качества передачи данных в телесистемах является уровень битовой ошибки *BER* (*Bit Error Rate*). На основе данной метрики формируются требования к качеству обслуживания абонента *QoS* (*Quality of Service*) для различных систем передачи данных, в том числе и в системе радиодоступа *WiMAX* [1]. Однако, для беспроводных радиосистем, данная метрика измеряется весьма в широких пределах: от «10^{-3}» до «10^{-6}». Современные радиосети используют пакетную передачу данных, что позволяет одинаково легко передавать различную по виду информацию: аудио и видео данные, текстовые последовательности, комбинированную информацию и т.п. Для каждого из этих видов информации требования по качеству различны и здесь *BER* не всегда может выступать в качестве универсальной метрики.

В данной работе, на основе моделирования беспроводного канала связи и анализа механизмов адаптации системы к условиям канала при передаче различных изображений предложено внедрение метрики *PSNR* (*Peak Signal to Noise Ratio*) для оценки качества передачи видеоданных и статических изображений в беспроводных системах связи.

Для исследований была разработана математическая модель системы фиксированного абонентского радиодоступа *WiMAX* (стандарт *IEEE 802.16-2009*), которая использует для передачи информации метод ортогонального частотного мультиплексирования *OFDM* (*Orthogonal Frequency-Division Multiplexing)* и квадратурную амплитудную модуляцию *QAM*.

Модель включает в себя несколько функциональных блоков, каждый из которых реализует свою отдельную функцию: передающая часть – блок ввода и определения типа данных, система исправления ошибок методом упреждения (*FEC*) на основе кодера Рида-Соломона (B_i, C_i), где B_i – количество байт после кодирования, C_i – количество байт данных; модулятор, формирователь символа *OFDM* с количеством поднесущих *nk*, канал связи и приемная часть – *OFDM* демодулятор, демодулятор, декодер, обработка и вывод полученных результатов. Структурная схема модели представлена на рис.1.

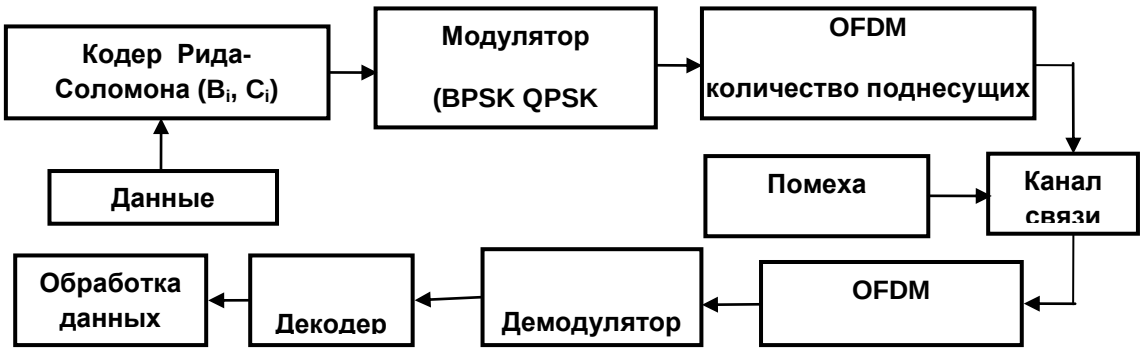


Рис.1 Структурная схема модели *WiMAX* канала связи

Так как наиболее жесткие требования предъявляются к передаче видео и отдельных изображений, то было решено, что модель будет оперировать именно с этими типами данных. Для того, чтобы оценить передачу различных данных, в работе использовались медицинские диагностические снимки, изображения текстовых последовательностей, массивы случайных данных, имитирующие по совей структуре изображения. В ходе исследований использовались 2 параметра качества передачи: *BER* и *PSNR*. Передача данных велась при изменении соотношения сигнал/шум от 0 до 30 дБ с шагом в *1дБ*. При моделировании использовались рекомендованные стандартом [1] адаптивные схемы кодирования и модуляции, применяемые в системе *WiMAX*. Данные о них сведены в табл. 1.

Таблица 1.

Соответствие длины кода Рида-Соломона различным видам модуляции

Тип модуляции	Размер незакодированного сообщения (байт)	Длина кода Рида-Соломона	Скорость кодирования
BPSK	12	(12,12,0)	-
QPSK	24	(32,24,4)	2/3
QPSK	36	(40,36,2)	5/6
16-QAM	48	(64,48,8)	2/3
16-QAM	72	(80,72,4)	5/6
64-QAM	96	(108,96,6)	3/4
64-QAM	108	(120,108,6)	5/6

Критерием качества передачи изображений был выбран уровень *PSNR = 37дБ*, что соответствует субъективной оценке *MOS* (Mean Opinion Score) равной 5(отлично) [2]. MOS – это метрика, основанная на экспертной оценке и учитывающая особенности человеческого зрения. Сравнение метрик *PSNR* и *MOS* приведено в таблице 2.

Таблица 2.

Соотношение *PSNR* и *MOS*

PSNR	*MOS*
>37	5
31-37	4
25-31	3
20-25	2
< 20	1

BER рассчитывался поочерёдным сравнением каждого бита исходного и переданного изображений. Определение уровня *PSNR* происходило по формуле:

$$PSNR = 20\log_{10}\left(\frac{MAX_i}{\sqrt{MSE}}\right) \quad (1)$$

где, *MSE (mean squared error)* среднеквадратичная ошибка: $MSE = \frac{1}{M * N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - K(i,j)\right]^2$, где *MAX* – это максимальное значение, принимаемое пикселем изображения; *M* – горизонтальное разрешение изображения; *N* – вертикальное разрешение изображения; *I* – изображение до передачи по каналу связи; *K* – изображение после прохождения канала связи; *i,j* – позиция по горизонтали и вертикали текущего бита.

Для цветных изображений с тремя компонентами *RGB* на пиксель применяется такое же определение *PSNR*, но *MSE* считается по всем трем компонентам (и делится на утроенный размер изображения).

В докладе приводятся результаты численного моделирования, которые показывают, что для различных типов данных (медицинские диагностические снимки и изображения, отображающие текст) уровень *BER* при приемлемом качестве картинки будет различным, при этом, разница может составлять несколько порядков. Напротив, добиваясь уровня *PSNR* в *37дБ*, всегда получали отличное качество изображения. Следовательно, имея показатели только *BER* нельзя точно охарактеризовать соответствие переданных данных оригиналу. Также результаты показали, что гарантировано высокое качество можно получить лишь в том случае, если уровень *BER* достаточно мал, начиная от 10^{-5} и 10^{-6}, что не всегда достижимо в реальных системах.

Получение таких значений возможно лишь при высоком соотношении сигнал/шум. На рис. 2. приведен график зависимости *PSNR* от *BER*. Прямая горизонтальная линия – уровень *PSNR* в *37 дБ*, который является критерием оценки качества передачи данных.

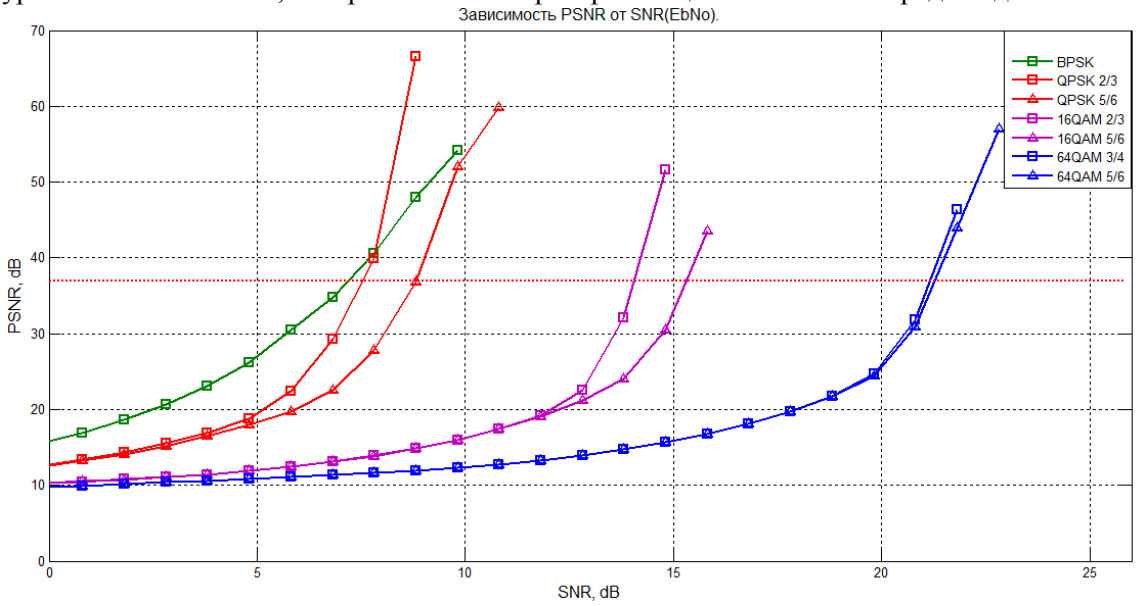


Рис.2 Зависимость *PSNR* от соотношения сигнал/шум в канале связи

В заключение доклада, предложено использовать *OFDM*-поднесущие, использующиеся для передачи пилот-тонов для доставки к приемнику заранее известных данных, соответствующего формата – такого же, как и в основном канале и измеряя *PSNR* вспомогательного канала, определять качество передачи в основном канале связи.

Литература:

1. IEEE 802.16e-2009. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

2. *P. Cherriman, L. Hanzo.* Robust H.263 Video Transmission over mobile channels in interference limited //Dept. of Electr. and Comp. Sc., Univ. of Southampton, SO17 1BJ, UK.

АНАЛИЗ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК РАДИОКАНАЛОВ СИСТЕМ WI-MAX

Коляденко Ю.Ю., Бойко Е.В., Хафиз Мухаммад И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем,
тел. (057)702-13-20)
e-mail: kolyadenko.home@rambler.ru, факс (057) 702-13-20

Abstract. Statistical characteristics of WI-MAX system radio channels using MIMO technologies with two proper subchannels under uncorrelated Rayleigh fading signal conditions were analyzed. The dependence of probability-density function of the channel array proper numbers was obtained and that determines the probability of bit errors in WI-MAX systems.

Введение

В настоящее время стремительными темпами происходит развитие современных телекоммуникационных сетей. Это особенно заметно по активным процессам международной стандартизации, производства оборудования и развертывания сетей. Среди них все большее распространение получают, например, такие технологии как персональные сети IEEE 802.15 (Bluetooth), локальные сети IEEE 802.11 (Wi-Fi), стандарт универсальных городских сетей IEEE 802.16 (WiMAX), в которых беспроводной широкополосный доступ используется очень широким спектром приложений – от традиционной передачи речи до современных мультимедиа-приложений.

Все упомянутые технологии используют соответствующие протоколы взаимодействия узлов сети для управления передачей пакетов по общему каналу связи. Наличие общего канала связи, коллективно используемого абонентами (зачастую очень большим их числом), является общей чертой современных и перспективных беспроводных телекоммуникационных систем. Значительный интерес представляют исследования централизованных телекоммуникационных систем, в которых имеется центральная станция, координирующая работу абонентских станций. Именно такая сетевая архитектура является основной в стандарте IEEE 802.16.

Для достижения высоких скоростей передачи данных в системах связи WI-MAX используют многоантенную технику. В системах с несколькими пространственными каналами как в передатчике, так и в приемнике используются несколько антенн. Их называют системами со многими входами и многими выходами (MIMO — Multiple Input Multiple Output). Считается, что при использовании MIMO системы можно получить скорости передачи информации, близкие к предельным, если параметры канала известны в передатчике, и при наличии достаточно высоких значениях отношения сигнал/помеха+шум, что определяет вероятность битовой ошибки. Вместе с тем, вероятность битовой ошибки полностью определяется статистическими свойствами собственных чисел канальной матрицы.

Отличительными особенностями этого стандарта являются высокая сложность протокола подуровня управления доступом к среде, отвечающего, в частности, за организацию доступа абонентов к общему каналу связи, а также многолучевость каналов радиосвязи, со случайным нестационарным изменением всех физических параметров

В связи с вышесказанным анализ статистических характеристик радиоканалов систем WI-MAX является актуальной научной задачей.

Основная часть

Для описания свойств многолучевого пространственного канала используется понятие импульсной характеристики. Поскольку существует несколько путей распространения радиоволн от передатчика к приемнику, то результирующий сигнал представляет собой сумму случайного числа сигналов, ослабление и временная задержка каждого из которых изменяются во времени случайным образом. В результате интерференции некоторые частотные компоненты результирующего сигнала ослабляются, а некоторые усиливаются, что приводит к неравномерности частотной характеристики. Системы связи

WI-MAX, использующие OFDM модуляцию (Orthogonal Frequency Division Multiplexing), обычно функционируют в условиях частотно-селективного канала. Свойства такого канала описываются канальной матрицей, состоящей из парциальных (из каждой передающей в каждую приемную антенну) коэффициентов передачи, которые являются случайными комплексными величинами, зависящими от частоты. Следовательно, преобразования сигналов при их передаче и приеме также оказываются различными для разных частот. Однако, если полный диапазон частот разделить на поддиапазоны с шириной меньшей интервала частотной когерентности канала, то внутри каждого из них пространственный канал можно считать частотно-неселективным и реализовать единую адаптивную обработку сигналов. Поэтому достаточно рассмотреть частотно-неселективный канал связи.

Наибольший интерес представляет релеевский многолучевой канал, когда прямой луч между передатчиком и приемником практически отсутствует. В этом случае возникают глубокие замирания сигнала, которые являются характерными для систем связи WI-MAX, работающих в городских условиях.

Адаптивная пространственная обработка сигналов при передаче и приеме в MIMO-системе может быть реализована с использованием сингулярного разложения канальной матрицы. Сформированные таким образом параллельные подканалы для передачи данных называются собственными, так как используют в качестве весовых векторов пространственной обработки собственные векторы канальной матрицы. Каждый собственный подканал соответствует одному из собственных векторов и собственных чисел. Максимальное количество подканалов, которое можно сформировать, определяется статистическими свойствами среды распространения радиоволн и равно рангу канальной матрицы. В случае некоррелированного релеевского канала вероятность вырождения канальной матрицы является ничтожно малой и ее ранг определяется минимальным числом передающих или приемных антенн.

Проведены исследования статистических характеристик собственных чисел канальной матрицы в MIMO-системе с конфигурациями ($N_t \times N_r$) в условиях некоррелированных релеевских замираний сигналов, где N_t – число передающих антенн на базовой станции, $N_r = 2$ – число приемных антенн у пользователя. В системах связи WI-MAX обычно используется число передающих антенн на базовой станции N_t =2, 4, 8.

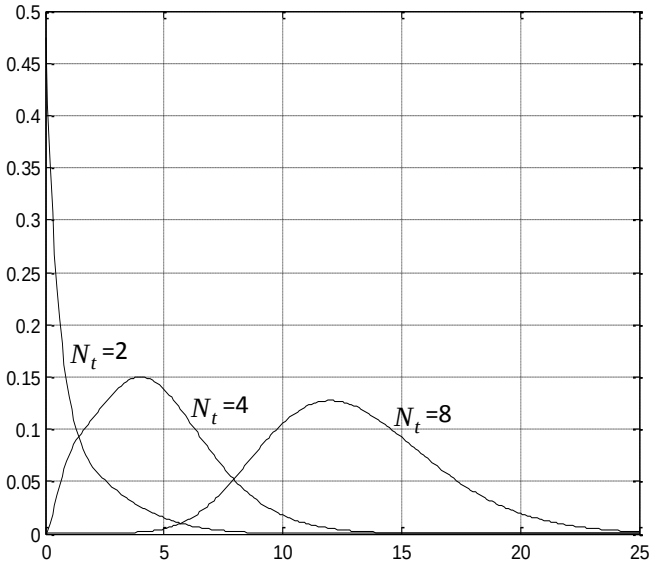


Рис. 1. Функции плотности вероятности максимальных собственных чисел канальной матрицы

Функция плотности вероятности максимальных собственных чисел канальной матрицы MIMO-системы определяется выражением:

$$p(\lambda) = \frac{\lambda^{N_t-2} e^{-\lambda}}{(N_t-1)!} \times \\ \times \left(\lambda^2 - 2\lambda(N_t-1) + N_t(N_t-1) + \sum_{nt=0}^{N_t-2} \frac{nt(nt-2N_t+1) + N_t(N_t-1)}{nt!} \lambda^{nt} \right). \quad (1)$$

Функция плотности вероятности минимальных собственных чисел канальной матрицы MIMO-системы определяется выражением:

$$p(\lambda) = \frac{\lambda^{N_t-2} e^{-2\lambda}}{(N_t-1)!} \sum_{nt=0}^{N_t-2} \frac{nt(nt-2N_t+1) + N_t(N_t-1)}{nt!} \lambda^{nt}. \quad (2)$$

На рис. 1. представлены функции плотности вероятности максимальных собственных чисел канальной матрицы с двумя приемными $N_r = 2$ и несколькими N_t=2, 4, 8 передающими антеннами.

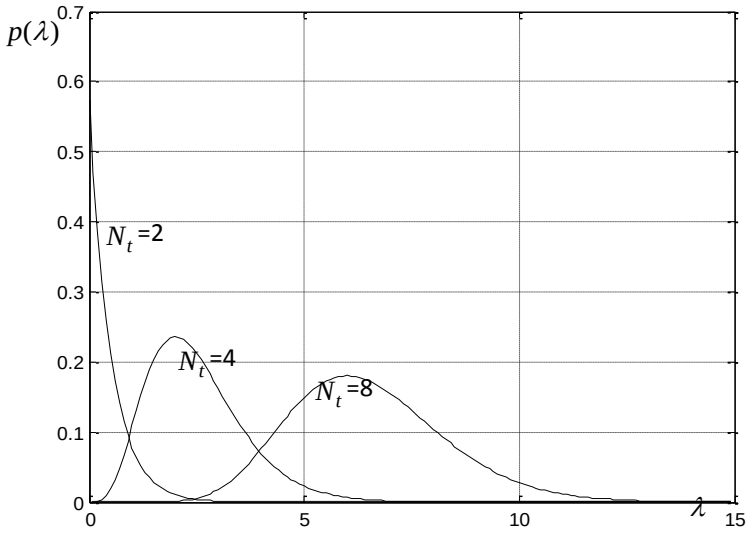


Рис. 2. Функции плотности вероятности минимальных собственных чисел канальной матрицы

На рис. 2. представлены функции плотности вероятности минимальных собственных чисел канальной матрицы с двумя приемными $N_r = 2$ и несколькими N_t=2, 4, 8 передающими антеннами. Из полученных графиков видно, что с увеличением количества передающих антенн средние значения, как для максимальных собственных чисел, так и для минимальных собственных чисел канальной матрицы увеличиваются.

Выводы

Проведены исследования статистических характеристик собственных чисел канальной матрицы в MIMO-системе с конфигурациями ($N_t \times N_r$) в условиях некоррелированных релеевских замираний сигналов, где N_t – число передающих антенн на базовой станции, $N_r = 2$ – число приемных антенн у пользователя. Исследования показали, что с увеличением количества передающих антенн средние значения, как для максимальных собственных чисел, так и для минимальных собственных чисел канальной матрицы увеличиваются. Увеличиваются так же их дисперсии, что влечет за собой увеличение вероятности битовой ошибки.

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ MIMO В ОТКРЫТЫХ ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ

Марчук А.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-20,
E-mail: tkc@kture.kharkov.ua ; факс (057) 702-13-20

The given work is devoted to the experimental researches of the open optical systems with MIMO technology. The experimental modeling system is created. Possibilities of increase the optical system capacity are investigational depending on the number of optical matrix elements, their size, distance between the transmitter and receiving optical system. Measured BER value in an optical communication network. Recommendations are worked out on the practical use of the investigational systems. The ways of further capacity increase of the experimental model of open optical system with MIMO technology are indicated.

Технология MIMO в последние годы внедряется в беспроводных телекоммуникационных сетях радиодиапазона для повышения пропускной способности или достоверности передачи информации в системах связи. Имеются публикации о применении этой технологии в оптическом диапазоне. Оптические системы передачи с технологией MIMO имеют большой потенциал по повышению пропускной способности, однако в настоящее время он не реализован в полной мере. Поэтому актуальной является задача исследования путей повышения скорости передачи информации в открытых оптических системах связи с технологией MIMO.

Целью настоящей работы является создание экспериментального макета оптической системы связи с технологией MIMO и исследование возможностей повышения пропускной способности в таких системах.

Схема экспериментальной установки представлена на рис.1. Последовательный поток бит кодируется в кодере К и поступает на преобразователь ППК-М последовательного потока в кадры – матрицы. Для метки начала кадра добавляется короткий символ, подаваемый одновременно на все оптические излучатели программой вставки циклического кода ВЦК. Сигналы отображающие элементы кадра – матрицы параллельно подаются на матрицу оптических излучателей МОИ. Для уменьшения интерференции применяется разнос лазеров в пространстве, а в случае источника в виде плоской LCD матрицы на группу излучающих точек, создающих белые и черные области. Канал связи КС – свободное пространство. На приемной стороне после устройства фокусировки Ф выполняются обратные преобразования сигналов в матрице оптических приемников МОП, далее программой обработки вставленного циклического кода ОЦК, затем в преобразователе ПК-МП кадров – матриц в последовательный поток бит и декодирование в декодере ДК.

В первом эксперименте в качестве оптического передатчика использована матрица LCD, а в качестве оптического приемника – матрица CCD. Во втором эксперименте матрица LCD заменена на матрицу из полупроводниковых лазеров.

Получены графики зависимостей вероятностей ошибок BER от размеров пятна бита, расстояния между оптическим передатчиком и приемником. Для таких систем задача сохранения BER на заданном уровне очень важна, так как с увеличением расстояния или при уменьшении «оптических размеров» бита снижается уровень различения между черным и белым пятном.

Образец изображения оптической матрицы MxN с переданными битами показан на рис.2. Каждый бит переданной информации представляет собой прямоугольник черного или белого цвета, передается «1» или «0», соответственно. Скорость передачи информации увеличилась почти в (MxN) раз по сравнению с однолучевой оптической системой. При визуальном сходстве с телевизионным кадром главным отличием системы является не построчная последовательная передача бит, а параллельная передача по MxN каналах.

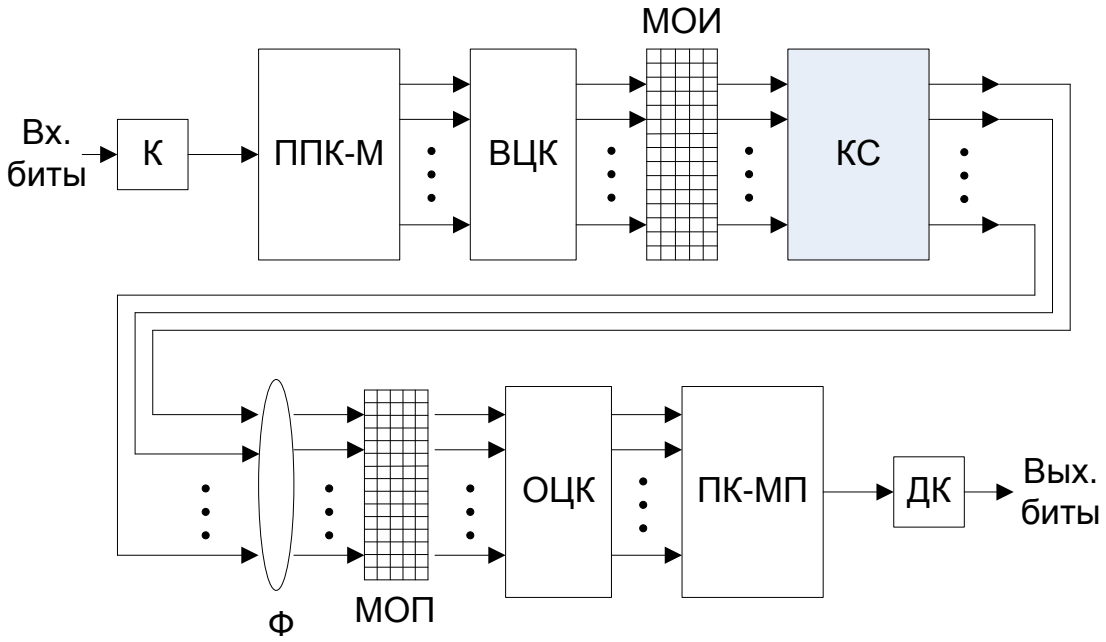


Рис.1. Схема экспериментального макета

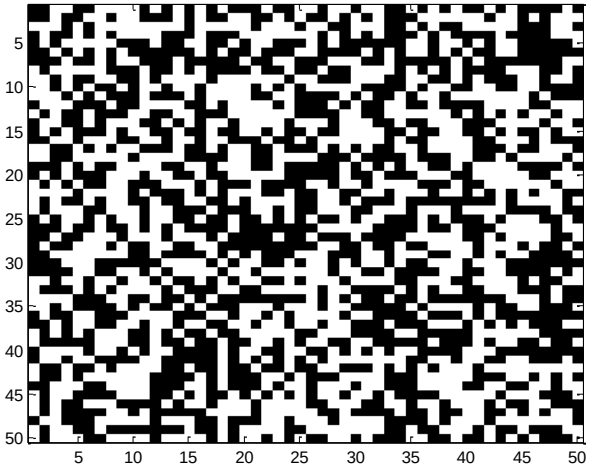


Рис.2. Образец изображения оптического кадра - матрицы данных системы MIMO 50x50

Замена оптической матрицы LCD на матрицу из простейших полупроводниковых лазеров, обеспечивающих небольшие скорости в 10 Мбит/с дает, например, для матрицы 10x10 скорость 1 Гбит/с при размерах оптической матрицы 2x2 см (расстояние между центрами излучающих апертур 2 мм). При размерах оптической матрицы 5x8 см скорость передачи информации составляет 10 Гбит/с. Замена лазеров на высокоскоростные позволит получить значительно больший выигрыш в пропускной способности для открытых оптических систем связи с технологией MIMO по сравнению с одноканальными. Вполне достижимы скорости в сотни Гбит/с на достаточно традиционных оптических элементах.

Разработаны рекомендации по проектированию и практическому использованию исследованных систем.

МЕТОД ПОЗИЦИОНИРОВАНИЯ УЗЛОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Иваненко В.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. «Сети связи», тел. (057) 70-21-429.
E-mail: zlata_ne@bk.ru

The given work contains a description of a method of increasing the accuracy of the coordinates on the received signal strength that has been developed. This method can be used in wireless sensor networks for positioning motes. The method is based on the use of additional similar motes in base stations. Information about the location of built-in units compared with the global location and calculates the correction factor.

Беспроводные сенсорные сети (БСС) представляют собой сеть из множества узлов – мотов, которые соединены посредством радиоинтерфейса. Они могут применяться в разнообразных областях промышленности, медицины, сельского хозяйства, охраны, предупреждения ЧС, в быту, в военных целях и т.д. для мониторинга и контроля состояния некоторого контролируемого параметра (рис. 1).

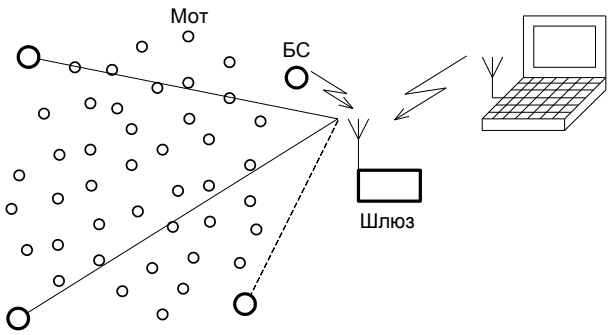


Рис. 1 – Фрагмент БСС

В БСС часто возникает необходимость знать местоположение одного или нескольких мотов, значение контролируемого параметра которых отклонилось от нормы. Также некоторые виды маршрутизации в БСС используют информацию о местоположении узлов для построения эффективных маршрутов.

Имеется множество способов позиционирования объектов, но, исходя особенностей БСС, эффективно используются только наиболее простые. Зачастую это определение координат мотов посредством GPS (Global Positioning System – Система глобального позиционирования) или RSSI (Received Signal Strength Indication − Индикация силы принимаемого сигнала) [1]. Использование на каждом узле БСС приемника GPS делает сеть слишком дорогой, т.к. именно стоимость мота определяет стоимость сети в целом, ввиду использования в сети большого количества узлов (может достигать десятков тысяч). Поэтому наиболее приемлемым является метод RSSI, который используется в беспроводных сетях повсеместно.

RSSI технология устанавливает местоположение объекта, определяя расстояния до БС по мощности принятого пилот-сигнала от БС при известной мощности переданного по затуханию за время распространения.

Величина затухания определяется как:

$$A = \left(\frac{4\pi df}{c}\right)^2, \qquad (1)$$

где d – расстояние между источником и приемником сигнала, f – частота сигнала, c – скорость света.

Из (1) можно выразить расстояние от источника сигнала (БС) до мота:

$$d = \frac{c}{4\pi f}\sqrt{A}\,. \qquad (2)$$

Отсюда, зная расстояния от всех БС, местоположение мота определяется, как точка пе-

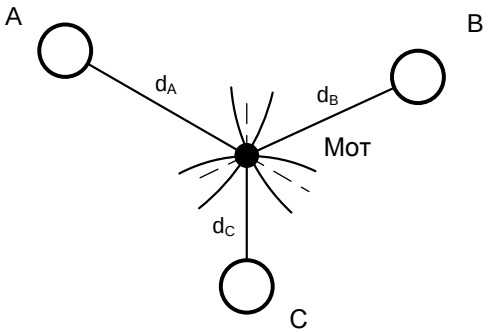


Рис. 2 - Позиционирование мота

ресечения окружностей (рис. 2).

Координаты мота являются решением системы уравнений [2]:

$$(x_m, y_m) = \begin{cases} d_A^2 = (x_A - x_m)^2 + (y_A - y_m)^2 \\ d_B^2 = (x_B - x_m)^2 + (y_B - y_m)^2 \\ d_C^2 = (x_C - x_m)^2 + (y_C - y_m)^2 \end{cases}, \quad (3)$$

где d_i - расстояние до i-ой БС,

x_m, y_m – искомые координаты мота,

x_i, y_i – координаты i-ой БС.

Для определения местоположения в двух координатах достаточно трех БС; увеличение числа БС повышает точность определения координат.

Данный метод позволяет относительно просто и достаточно точно определять локальные координаты объектов, либо (при заданных глобальных координатах на БС) путем решения системы уравнений (3) получить глобальные координаты объектов. Простота реализации алгоритма делает его применение эффективным в рамках использования на простых вычислительных системах критичных к энергосбережению. Недостатком данного метода является недостаточная точность определения местоположения при плотном размещении объектов небольших габаритов, которое характерно для БСС. Повышение точности позиционирования технологии RSSI позволит не усложнять аппаратную и программную части мота, а, следовательно, и его стоимость, что является критичным в БСС.

В основу разработанного метода положен метод повышения точности позиционирования технологии RSSI за счет применения n+1 БС (где n – минимально необходимое количество БС), в которых дополнительно установлены моты, однотипные используемым в сети. Тогда аналогично позиционированию мотов по технологии RSSI производится взаимное позиционирование БС: поочередно n БС в широковещательном режиме рассылают пилот-сигналы, а i-ая БС принимает сигналы на установленный в ней мот, который оценивает расстояния до каждой БС по (2) (рис. 3).

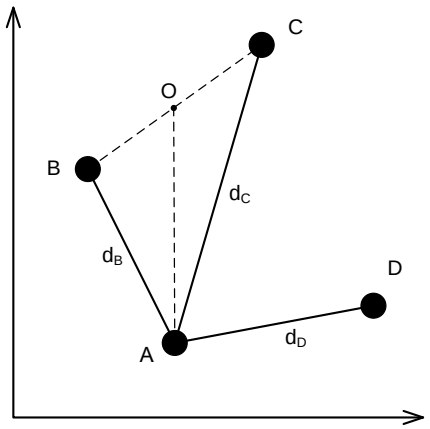


Рис. 3 – Вычисление поправочного коэффициента

Использование на позиционируемой БС дополнительного мота, аналогичного мотам сети, исключает появление ошибки (различия в уровнях принятого пилот-сигнала) из-за отличия характеристик приемопередатчиков мота и БС. Сравнение глобальных $d_Г$ (точных, от GPS) и локальных $d_Л$ (определяемых по технологии RSSI) расстояний от n БС до i-ой позволяет определить поправочный коэффициент для каждой БС:

$$k = \frac{d_Л}{d_Г}. \quad (4)$$

Полученный коэффициент (4) позволит скомпенсировать погрешность определения расстояния от мотов в направлении к ближайшей БС путем умножения полученных мотами сети расстояний в секторе сети в окрестности БС.

Информация о местоположении мотов, передающих информацию к БС A и B и находящихся в секторе BAO (рис. 3), корректируется поправочным коэффициентом $k_{AB} = \frac{d_{ЛAB}}{d_{ГAB}}$, а к БС A и C и находящихся в секторе OAC $k_{AC} = \frac{d_{ЛAC}}{d_{ГAC}}$. То есть моты,

определившие свои локальные координаты по технологии RSSI (x_i, y_i) сортируются в соответствии с неравенствами

$$\begin{matrix} k_{AB} \text{ для } y \le ax + b \\ k_{AC} \text{ для } y > ax + b \end{matrix}, \quad (5)$$

где уравнение прямой АО $y = ax + b$ является решением системы уравнений:

$$\begin{cases} y_O = ax_O + b \\ y_A = ax_A + b \end{cases}, \quad (6)$$

x_O, y_O – глобальные координаты точки О (в простейшем случае – середина отрезка),

x_A, y_A – глобальные координаты точки А.

Аналогично и для остальных БС.

В связи с тем, что предполагается, что все особенности распространения радиоволн в направлении от i-ой БС к остальным равномерны в секторах, полученных путем разбиения сети на окрестности БС, то целесообразна корректировка локальных координат мотов поправочным коэффициентом, рассчитанным для соответствующего сектора.

Таким образом, разработанный метод повышения точности позиционирования узлов в БСС позволяет достигнуть более точной локализации мотов, не усложняя при этом аппаратную и несущественно усложняя программную части.

Принципиальная возможность повышения точности определения координат отдельных объектов сети делает технологии локализации привлекательными благодаря удешевлению и уменьшению энергопотребления отдельных устройств (за счет отсутствия необходимости использовать датчики GPS), упрощению развертывания таких сетей (например путем разбрасывания устройств с самолета), возможности использовать сенсорные сети в труднодоступных местах. При этом следует отметить, что определение координат на сегодняшний день фактически является неотъемлемой частью многих беспроводных телекоммуникационных сетей, в частности сетей сотовой связи, однако несмотря на одинаковые принципы определения координат (геометрическая триангуляция) в силу специфики сети вопросы определения координат в них решаются по разному.

Литература:

1. Nafarieh A. "A Testbed for Localizing Wireless LAN Devices Using Received Signal Strength," [Text]/ A. Nafarieh and J. How. Communication Networks and Services Research Conference, Halifax, 2008, pp. 481-487.

2. Converting Signal Strength Percentage to dBm Values [Электронный ресурс]/ WildPackets, November, 2002. – 11 С. Режим доступа: http://www.wildpackets.com/elements/whitepapers/Converting_Signal_ Strength.pdf.

МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫМ ГОРОДОМ

Гладий Л.В., Халава Саид Фауаз
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем,
тел.(057) 702-55-92), E-mail: tcs@kture.kharkov.ua; факс: (057) 702-13-20

The concept an intelligent city is a new stage for development of an infrastructure of a city with considerable improvement of living conditions of its inhabitants. Service-oriented architecture- is one of the most perspective technologies of construction of the distributed global network. Its basic advantages are loosely coupled of applications, independence of the programming language and platform that is especially important for a heterogeneous network of a city. Reliability and ensuring availability of services is one of the most important characteristics of such network. In working it is offered to use a method dynamic replication for ensuring availability of services.

В настоящее время одним из наиболее перспективных направлений развития науки и техники является обеспечение комфортных и безопасных условий для жизни людей. Наиболее масштабным проектом, реализуемым в этом направлении, является проект «интеллектуальный город», в основе которого лежит идея создания единого информационного пространства, позволяющего осуществлять управление городом, обеспечивать безопасность жителей и объектов городского хозяйства, а также осуществлять мониторинг состояния главных городских объектов. Программа «интеллектуальный город» ориентирована на модернизацию и реконструкцию существующей инженерной сети, с целью создания единого глобального информационного пространства, в которое будут подключены службы различных городских объектов.

В качестве примера рассмотрим работу сети коммунальных служб города (рис.1).

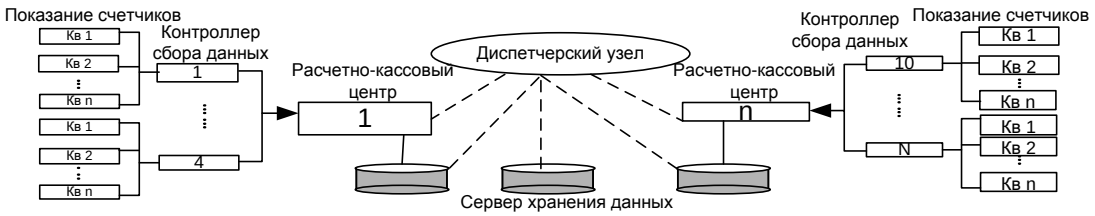


Рис. 1 – Структурная схема сети коммунальных служб города

В каждой квартире или доме устанавливается счетчик на холодную и горячую воду. Один раз в сутки показания со счетчика снимаются и передаются на контроллер сбора данных, где информация обрабатывается и передается в ближайший расчетно-кассовый центр. В расчетно-кассовом центре производится оценка показаний счетчиков и определяется оплата за предоставляемые услуги. Затем данная информация отправляется на личный счет клиента, который хранится на одном из серверов сети. Клиент посредством сети интернет может зайти на свой личный счет и проверить задолженность по оплате и сверить показания счетчиков. Также с помощью терминалов, банков и сети интернет он может произвести оплату предоставляемых ему услуг. Центральным узлом для всей системы является диспетчерский центр, который имеет доступ к базе данных клиентов и к расчетно-кассовым центрам, что упрощает процесс внесения изменений в систему и контроль ее состояния. Такая структура системы управления является более надежной сравнительно с централизированной, так как выход из строя любого узла сети не повлияет на работу всей системы.

Важным вопросом, решаемым при создании такой городской сети, является выбор ее архитектуры и метода управления. В связи с тем, что основными требованиями, выдвигаемыми к сети, является гибкость системы, отказоустойчивость, масштабируемость и надежность, то наиболее подходящим было бы использовать распределенную система

управления ресурсами сети. В качестве архитектуры предлагается использовать сервис-ориентированную архитектуру (SOA), основными преимуществами которой являются слабая связность приложений, независимость от языка и платформы, что является особенно важным для разнородной городской сети.

В самом общем виде сервис-ориентированная архитектура предполагает наличие трех участников: поставщика сервисов, потребителя сервисов и реестра сервисов [1]. Их взаимодействие представлено достаточно простой схемой: поставщик регистрирует сервисы в реестре, а потребитель обращается к реестру с целью получения адреса необходимого ему сервиса. После получения адреса потребитель может отправлять запросы к необходимому ему сервису напрямую. В том случае, если в базе данных локального реестра сервиса нет запрашиваемого ресурса, запрос пересылается удаленному реестру. Если и там сервис не будет обнаружен, потребителю будет отправлено сообщение об отсутствии данного ресурса в сети. Каждый реестр имеет свою область обслуживания, границы которой определяются зарегистрированными в нем сервисами, другими словами, при регистрации услуг предприятия или личного счета жителя города в реестре указывается, что данный реестр сервисов является для него локальным и ни в каком другом реестре он до этого не был и не будет зарегистрирован.

Использование SOA-архитектуры является хорошим решением для организации единой городской сети, однако сервис-ориентированная архитектура имеет один существенный недостаток – отсутствие методов обеспечения доступности сервисов, что может значительно повлиять на характеристики такой сети. Пока количество предоставляемых услуг будет не большое, вопросы доступности не будут иметь особого значения, но в дальнейшем при росте количества умных домов, возникновении таких услуг, как проверка датчиков состояния квартиры в реальном времени, возникновении новых услуг предоставляемых предприятиями города, ситуация может измениться. В связи с этим в данной работе будут рассмотрены существующие методы повышения надежности и, в частности, доступности, с целью адаптации их к SOA

Одним из таких методов является репликация, которая используется в архитектуре CORBA. Однако, как показывает практика, повсеместное использование репликации из-за необходимости обеспечения непротиворечивости данных может привести к перегрузкам сети и ухудшению ее характеристик. Поэтому применение данного метода необходимо рассматривать для каждого определенного случая отдельно. Примером такого случая может быть ситуация, когда к определенной услуге предприятия города за небольшой промежуток времени возрастает количество запросов. С целью уменьшения передаваемого трафика по сети, а так же повышения доступности сервиса разумным решением будет реплицировать его на локальный сервер вблизи запрашиваемых его пользователей. В качестве метода репликации предлагается использовать метод, основанный на динамической репликации, описание которой представлено в [2], при этом модифицировать его для применения в SOA.

В соответствии с алгоритмом динамической репликации (рис. 2) локальный реестр сервисов должен по истечению определенного промежутка времени проверять счетчики запросов к сервисам. Если счетчик обращений реестра $cnt(R,F_i)$ превысит порог репликации $rep(F)$, то реестр придет к решению о необходимости проведения репликации данного сервиса. Прежде чем проводить данную операцию, реестр просматривает свою базу данных на наличие сервера, который имеет ресурсы, необходимые для размещения данной реплики. Если такой сервер имеется, реестр посылает запрос к сервису F на создание копии, при этом в запросе он указывает месторасположение для будущей копии. После проведения операции репликации, реестру отправляется ответ, в котором указывается, была ли успешно выполнена данная процедура и адрес для регистрации реплики. Данная информация также будет отослана на удаленный реестр сервисов для создания отметки копии и указания ее адреса, в том случае, если реплицированный сервис не являлся локальным. Если в базе данных реестра доступного сервера не обнаружено, то репликация отменяется, и реестр переходит к проверке счетчика следующего сервиса. По окончанию

процедуры проверки все счетчики обнуляются. Если общее число обращений к реплике упадет ниже порога удаления, то с целью освобождения места на сервере запускается процесс ее удаления. Если счетчик обращений реестра *cnt(R,F$_i$)* меньше порога репликации *rep(F)* и больше порога удаления *del(F)* счетчик обнуляется и реестр переходит к обработке счетчика следующего сервиса.

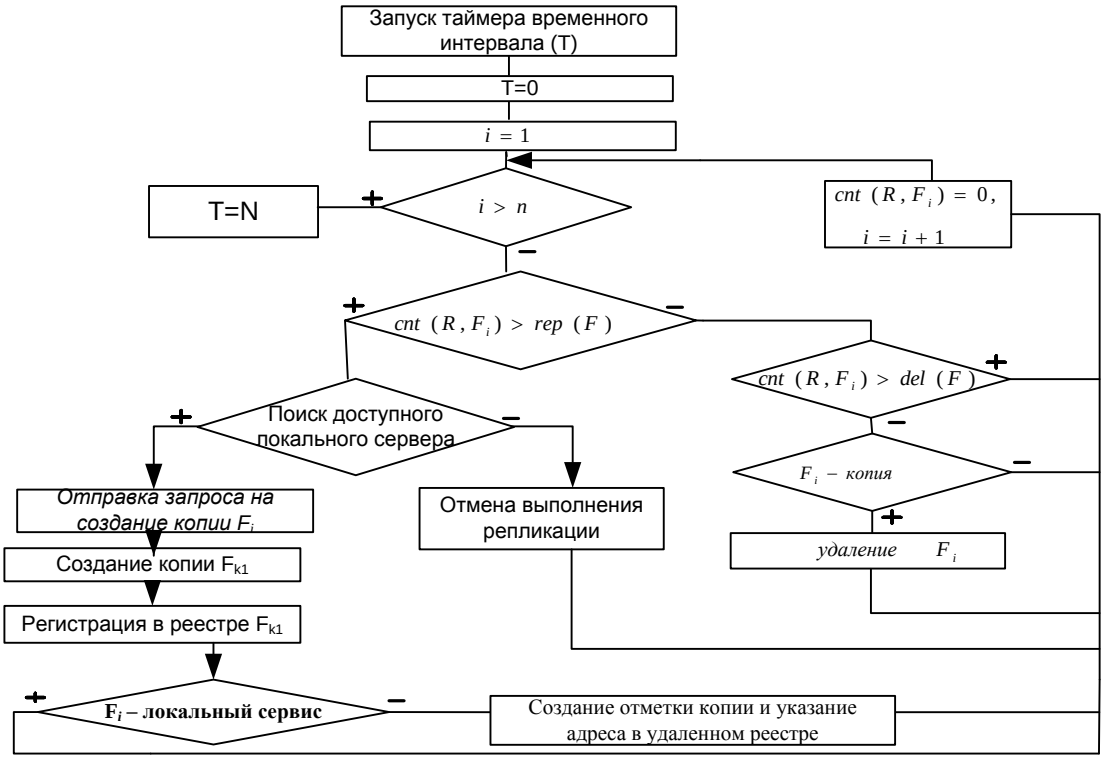


Рис. 2 – Алгоритм динамической репликации для SOA систем

Создание дополнительной реплики позволяет повысить доступность запрашиваемого сервиса, путем перераспределения запросов между репликами. Если во время прихода запроса сервис F будет занят или находится в нерабочем состоянии, запрос автоматически будет перенаправлен к реплике F_{k1}, при этом данное действие будет прозрачным для потребителя. Если сервис является удаленным, то, при приходе нового запроса на реестр, пользователю будет возвращен адрес сервиса F_{k1}. Основное преимущество использования репликации для удаленного сервиса состоит в том, что доступ к сервисам может выполняться локально, без поглощения сетевого трафика и задержек. Однако репликация сервиса не всегда может быть выполнима, это касается тех случаев, когда локальный сервер уже сильно перегружен или в нем отсутствует место на диске. В этом случае ищется альтернативный сервер или процесс репликации отменяется до окончания следующего временного интервала.

Как было указано ранее, важным вопросом при внедрении репликации является требование непротиворечивости данных. Согласно алгоритму динамической репликации, всегда существует первичная копия сервиса, которая даже при низком уровне обращений не удаляется, и которую имеет право изменить только поставщик. Поэтому для обеспечения непротиворечивости данных в SOA целесообразно использовать протоколы на базе первичной копии. Одним из наиболее распространенных протоколов такого вида является протокол первичного архивирования, рассмотренный в [2]. В данной работе предлагается модифицировать данный протокол с целью применения к сервис-ориентированным системам. Принцип работы данного протокола представлен на рисунке 4. Здесь используются следующие обозначения: 1) запрос на внесение изменений в сервис; 2) запрос к

реестру на наличие реплик и выдачу их адресов; 3) ответ реестра; 4) сигнал об обновлении резервных копий; 5) подтверждение обновления; 6) подтверждение внесения изменений.

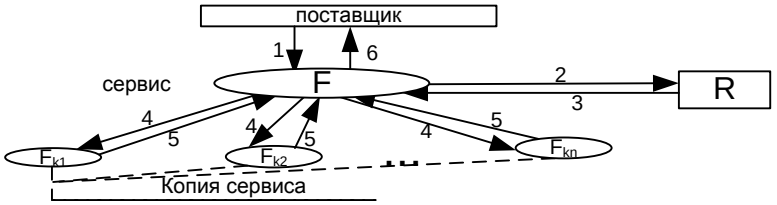


Рис. 4 – Протокол первичного архивирования

Поставщик для проведения операции изменения данных отправляет запрос к сервису, в который он хочет внести изменения. Данный сервис осуществляет обновления своих данных, после чего отправляет запрос к локальному реестру сервисов на наличие отметок копий и их адресов. Если таких копий не существует, процесс обновления завершается, и сервис вновь становится доступным. Если в ответе реестра будет указано наличие копии, то сервис отправит данные обновления всем его репликам. После прихода подтверждений об обновлении от всех реплик, сервис посылает поставщику подтверждение о внесении изменений, после чего данный процесс считается завершенным.

Процесс обновления происходит как одна атомарная операция или транзакция, что обеспечивает непротиворечивость всех копий сервиса. Недостатком данного протокола является то, что во время обновления потребитель, которых желает получить необходимый ему сервис, будет находиться в процессе ожидания. Однако, в том случае, если сервисы в SOA будут подвергаться модификации относительно редко, и право на их изменения будет иметь только поставщик, при небольшом количестве реплик время блокировки сервиса будет не значительным.

В случае роста количества реплик или же увеличения частоты их обновления можно будет использовать не блокирующий протокол обеспечения непротиворечивости. В отличие от предыдущего алгоритма, первичный сервис, сразу, после обновления своих данных, возвращает подтверждение поставщику и становится доступным пользователям. После этого он отправляет обновления всем своим репликам. Использование данного протокола практически не влияет на доступность сервисов при большом количестве реплик, но степень обеспечения непротиворечивости, а также защита от сбоев будет ниже. Предполагается, что поставщик, в зависимости от необходимой строгости обеспечения непротиворечивости данных, будет сам определять один из предложенных методов в соответствии с требованиями своего сервиса. Таким образом, при выборе оптимальной стратегии по применению репликации и модели обеспечения непротиворечивости, которая бы соответствовала особенностям систем, построенных на базе SOA, можно достигнуть высокой надежности и производительности сети.

Использование сервис-ориентированной архитектуры при построении единой городской сети позволит улучшить ее управляемость, быстродействие и надежность, а благодаря разработанному алгоритму репликации – и доступность сервисов.

Литература: 1. А.В. Богданов, Е.Н. Станкова, В.В. Мареев Сервис-ориентированная архитектура: новые возможности в свете развития GRID технологий / Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. – 32 с. 2. Э. Таненбаум, М. ванн Стеен. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ванн Стеен. — СПб.: Питер, 2003. — 877 с.

МЕТОДИКА АНАЛИЗА И ВЕРИФИКАЦИИ ТЕЛЕКОММУНИКАЦИОННЫХ ПРОТОКОЛОВ С ПОМОЩЬЮ Е-СЕТЕЙ И ФОРМАЛЬНЫХ ГРАММАТИК

Коровченко Е.Б.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-55-92,
E-mail: korov4enko@mail.ru

The given work is devoted to the developing the methods of analysis and verification of telecommunication protocols, that reduce development time protocol. Developed a method for analyzing the basic algorithmic properties of the protocol model, based on the use of formal grammars. It is proved that the use of formal grammar allows more rigorous analysis of properties of the model protocol.

Введение. Роль инфокоммуникационных технологий в современном обществе за последнее десятилетие стремительно возросла. Объем информации, передаваемой через информационно-телекоммуникационную инфраструктуру, удваивается каждые 2-3 года, что усиливает значение телекоммуникаций как на уровне отдельных компаний, так и в экономике мира в целом. Расширение набора предоставляемых сервисов обуславливает необходимость разработки новых телекоммуникационных протоколов, которые характеризуются достаточно высокой функциональностью, а следовательно и сложностью, что не может не отразиться на надежности протоколов, сроках и стоимости их проектирования, реализации и внедрения. В то же время со стороны пользователей наблюдается постоянный рост требований в области надежности функционирования телекоммуникационных систем и перечня предоставляемых сервисов, а со стороны компаний, предоставляющих данные услуги, – рост требований относительно времени реализации протоколов, с помощью которых предоставляются новые сервисы. Таким образом, в настоящее время наблюдается противоречие между все возрастающими требованиями к телекоммуникационным протоколам и возможностями средств проектирования, разработки и внедрения протоколов [1, 2]. Таким образом, разработка методов, вызволяющих повысить эффективность процесса разработки, и обеспечить корректное функционирование реализуемых телекоммуникационных протоколов является актуальной.

Основная часть. Особенностью разработки телекоммуникационных протоколов является то, что функциональность протокола известна заранее и на различных этапах жизненного цикла практически не дополняется. В связи с этими фактами наиболее широкое распространение при создании телекоммуникационных протоколов получила каскадная модель жизненного цикла [1]. Характерной чертой каскадной модели является завершение каждого этапа проверкой полученных результатов. В тоже время на каждом этапе жизненного цикла разработки телекоммуникационных протоколов возможно возникновение различных ошибок, оказывающих негативное влияние на последующие этапы жизненного цикла.

Для устранения ошибок, возникающих на разных этапах жизненного цикла телекоммуникационных протоколов можно выделить следующие способы:

- проверка соответствия требованиям;
- проверка непротиворечивости спецификации;
- проверка корректности функционирования протокола;
- проверка корректности распределения ресурсов;
- проверка соответствия реализации протокола его спецификации.

Исследования показывают, что наиболее весомыми в денежном и временном эквиваленте являются ошибки, допущенные на стадии формирования требований и разработки спецификации [2]. Проверка соответствия требованиям и проверка непротиворечивости спецификации позволяют обнаружить ошибки, допущенные на стадии разработки спецификации (рис. 1).

С помощью линейной темпоральной логики [3, 4] спецификация представляется в виде множества формул пути, описывающих каждый сценарий поведения протокола или определяющих требуемое состояние протокола в отдельно взятый момент времени. Использование такого подхода дает возможность рассматривать каждое состояние протокола, как одного из составляющих формулы пути (сценария поведения протокола) тем самым позволяет обнаружить ошибки, связанные с противоречивостью требований спецификации.

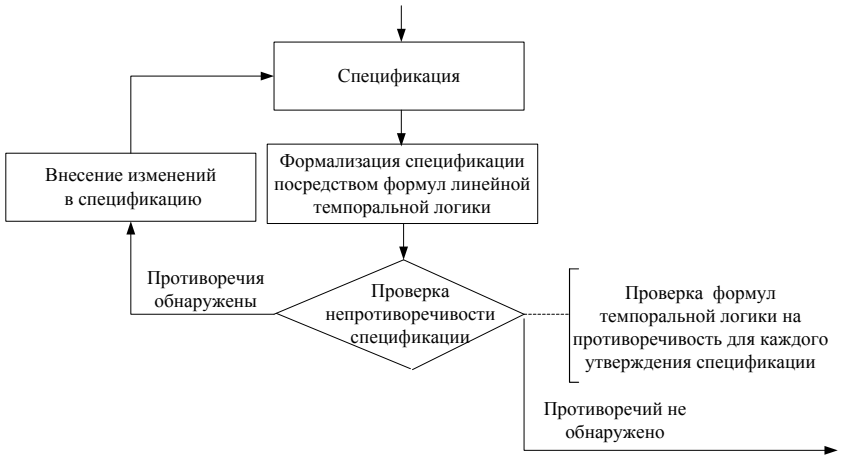


Рис. 1. Формализация спецификации протокола

Для анализа корректности поведения телекоммуникационных протоколов и оценки эффективности распределения ресурсов предлагается использовать формальные грамматики и аппарат Е-сетей [5, 6].Обобщенная схема анализа реализации протокола представлена на рис. 2.

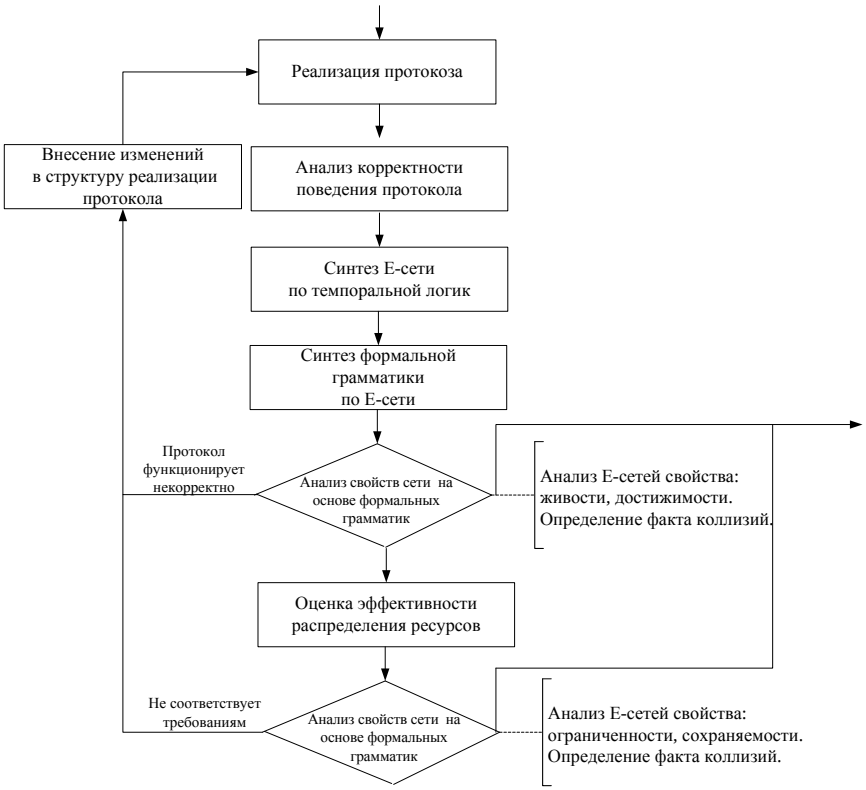


Рис.2. Этап реализации протокола

Исследования показали, что стоимость исправления ошибки, обнаруженной непосредственно на стадии внедрения протокола или в процессе его эксплуатации, является наивысшей для всего жизненного цикла протокола [2]. Применение различных методов верификации позволяет минимизировать возникновение такого рода ошибок. Большинство методов верификации основано на использовании теории автоматов, символьных вычислений, дедуктивного анализа [4, 7]. Данные методы обладают целым рядом недостатков, которые затрудняют их применение при анализе сложных современных протоколов. К таким недостаткам можно отнести: трудоемкость процесса верификации, определение ограниченного количества ошибок, возможный экспоненциальный рост пространства исследуемых состояний, при анализе сложных систем, невозможность описания параллельных процессов и пр. Наиболее эффективным методом при верификации телекоммуникационных протоколов является метод «проверки на моделях» (Model Checking) [4]. Классический подход метода Model Checking основан на полном переборе элементов формул темпоральной логики и нахождении соответствующих им позиций в модели протокола, а также установления соответствия взаимосвязей между состояниями модели и элементами формул темпоральной логики.

Основной проблемой возникающей при использовании метода «проверки на моделях» является проблема «комбинаторного взрыва» пространства исследуемых состояний, которая возникает при решении задачи верификации путем прямого перебора всего пространства состояний модели протокола [4].

В предлагаемой методике применяется модифицированный метод верификации Model Checking, который базируется на сравнении языков, описывающих поведение модели реализации и модели спецификации телекоммуникационного протокола (рис.3).

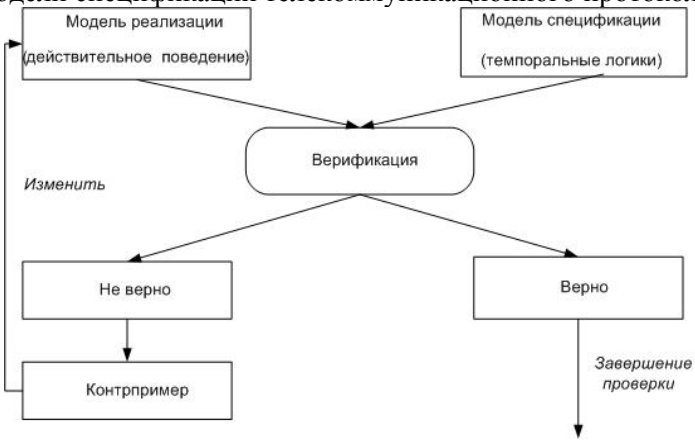


Рис.3. Модифицированный метод Model Checking для верификации телекоммуникационных протоколов

Метод сравнения формальных грамматик базируется на сравнении языков, описывающих поведение модели реализации и модели спецификации телекоммуникационного протокола. Преимуществом метода является его последовательное пошаговое выполнение. При таком подходе пространство исследуемых состояний ограничено множеством, порожденным процессе обхода одного из возможных сценариев поведения протокола. В случае нахождения расхождений между поведением модели спецификации и модели реализации протокола строиться контпример – цепочка, позволяющая установить последовательность действий, приводящих к возникновению ошибки.

Обобщенная схема, отражающая предлагаемый подход к разработке телекоммуникационных протоколов, представлена на рис. 4.

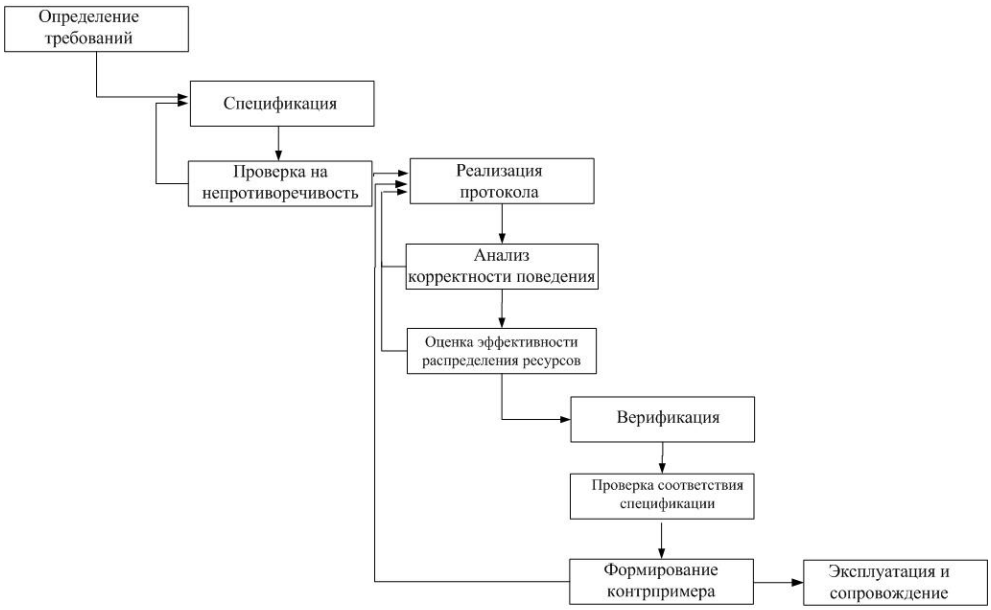


Рис.4. Методика анализа и верификации телекоммуникационных протоколов

Выводы. Проведенный анализ показал, что наиболее эффективной моделью жизненного цикла разработки телекоммуникационных протоколов является каскадная модель. Методы анализа, используемые в рамках каскадной модели, не позволяют обнаружить всех возможных ошибок и установить причины их возникновения. В рамках решения данной проблемы разработана методика, которая позволяет провести анализ непротиворечивости представленной спецификации; на основе анализа основных алгоритмический свойств Е-сетей (ограниченность, достижимость, живость, сохраняемость) выполнить анализ корректности поведения протокола и эффективности распределения ресурсов; синтезировать формальные грамматики, описывающие поведение протокола, с помощью которых провести верификацию как разрабатываемого протокола (на соответствие его спецификации), так и уже существующих различных версий одного и того же протокола (на поиск возможных ошибок совместного функционирования); в случае обнаружения ошибок в поведении протокола и или не соответствии его спецификации – выработать рекомендации по устранению данных проблем.

Литература: 1. Денищенко Г. Н., Коровкина Н. Л. Проектирование информационных систем. – М.: Интернет-университет информационных технологий, 2005. – 304 с. 2. The Standish Group (1995). The Scope of Software Development Project Failures. Dennis, MA: The Standish Group. 3. Stirling C. P. Modal and temporal logics for processes // LNCS 1043. – 1996. –P. 149–237.: 4. Лосев Ю.И. Применение методов анализа Е-сетей к моделям СОД / Ю.И. Лосев, С.И. Шматков, Е. В. Дуравкин // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2002. – Вып.132. – С. 149 - 151. 5. Коровченко Е.Б., Дуравкин Е.В. Формализация поведения протоколов информационного обмена, представленных моделями на основе аппарата Е-сетей [Електронний ресурс]// Проблеми телекомунікацій. – 2011. – № 1 (3). – С. 28 – 38. – Режим доступу до журн.: http://pt.journal.kh.ua/2011/1/1/111_duravkin_verification.pdf. 6. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking.: Пер. с англ./ Под ред. Р. Смелянского. – М.: МЦНМО, 2002. – 416 с. 7. Кулямин В.В. Методы верификации программного обеспечения// Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы". – 2008. – 117 с. Режим доступа: http://www.viva64.com/go.php?url=282

ИМИТАЦИОННАЯ МОДЕЛЬ САМООРГАНИЗАЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Теплицкая С.Н., Хуссейн Я.Т.
Харьковский национальный университет радиоэлектроники
Харьков, пр. Ленина, 14, каф. Телекоммуникационных систем,
тел. (057) 702-13-20, E-mail: tkc@kture.kharkov.ua

The imitating model of self-organizing of wireless sensory networks is offered. Distinctive feature of algorithm is use of accommodation of sensor controls, power stock in the sensory node, level of a ratio signal/noise. The qualitative and quantitative analysis of efficiency of functioning of the offered algorithm is carried out.

Сенсорная сеть (СС) является разновидностью телекоммуникационных сетей (ТКС) и предназначена для мониторинга различных ситуаций, элементов и явлений живой и неживой природы. С помощью СС обеспечивается наблюдение за процессами в науке и технике, в том числе и в самих телекоммуникациях. Они способствуют эффективному решению задач, специфичных для министерства чрезвычайных ситуаций, медицины катастроф и др. Построение надежных и эффективных сенсорных сетей – достаточно сложная задача. Она представляет собой компромиссное решение ряда ключевых задач, непосредственно связанных с основополагающими принципами их функционирования.

Достаточно часто СС приходится работать в неподготовленных условиях, при воздействии различных дестабилизирующих факторов, обеспечивая при этом высокую достоверность получаемой информации, надежность самой системы и автономность функционирования. В сложных системах, в связи с изменением обстановки, имеющихся ограничений или дефицитом оставшихся ресурсов, возникает необходимость изменения условий функционирования. Поэтому, важное значение играют методы самоорганизации в сенсорных сетях.

В работе предложена имитационная модель самоорганизации беспроводных сенсорных сетей. Процедура построения модели состоит из трех этапов: разбиение на кластеры, построение сети главных узлов (СГУ) и общей сети (СОУ). Исходніми данніми при построении модели являются количественные показатели: географическое расстояние, запас остаточной энергии и соотношение сигнал/шум в канале.

Рассмотрена модель СС со случайным гауссовым распределением мест размещения сенсорных узлов (СУ), радиус зоны действия которых R. Зона мониторинга при этом $D \gg R$. Необходимо разбить зону мониторинга на кластеры, в пределах которых обеспечивается надежная связь головного СУ со всеми оконечными, попавшими в данный кластер (сеть оконечных узлов – СОУ) и связь между головными узлами (СГУ).

Для определенности предполагается, что имеется $N = 30$ сенсорных узлов с радиусом $R = 20$ м, зона мониторинга: X=Y=200м, Z=3м. Передатчик СУ имеет мощность $P_{ПЕР}$, чувствительность приемника $P_{ПР} = S$, коэффициенты усиления антенн $G_{ПЕР} = G_{ПР} = 1$, то есть антенны не направлены. Места размещения назначались методом Монте-Карло. Полученное размещение далее надо кластеризовать таким образом, чтобы главный узел, размещенный в центре кластера, поддерживать надежную радиосвязь, обеспечивая при этом уровень сигнала в каждом из приемников оконечных узлов

$$P_{ПР_1} \geq S, \qquad (1)$$

где $P_{ПР} = P_{ПЕР} + G_{ПЕР} + \mathrm{G}_{ПР} + W_{CB}$ [дБ], здесь $G_{ПЕР} = \mathrm{G}_{ПР} = 0$, $W_{CB} = 10\lg\left(\frac{\lambda}{4 \cdot \pi \cdot d}\right)^2$ – ослабление сигнала в свободном пространстве на расстоянии d, $\lambda = c / f$, d – расстояние между головным и оконечными узлами.

Можно представить, что весь объем зоны мониторинга собран из шаров радиуса R, в центре которых находится главный узел. В этом случае для каждого из кластеров

может быть построена матрица расстояний D, каждый из элементов которой вычисляется по формуле:

$$d = \sqrt{\left(\frac{2R}{\sqrt{2}} \cdot k - \frac{R}{\sqrt{2}} - x_i\right)^2 + \left(\frac{2R}{\sqrt{2}} \cdot n - \frac{R}{\sqrt{2}} - y_i\right)^2 + \left(\frac{2R}{\sqrt{2}} \cdot f - \frac{R}{\sqrt{2}} - z_i\right)^2}, \quad (2)$$

где R – радиус действия сенсоры, k, n, f – количество кластеров по осям X,Y,Z, x, y, z – координаты *i*-го сенсора в кластере.

Данная матрица D в процессе функционирования СС изменяет как структуру, так и значения элементов. Это происходит вследствие потери некоторыми СУ своего энергетического потенциала, расходуемого пропорционально продолжительности работы на передачу (основной энергопотребляющий узел – выходной каскад передатчика). За каждый цикл работы СУ теряет определенное количество энергии:

$$E_S = P_{ПР} \cdot T \cdot \mathrm{n}, \quad (3)$$

где T – время, затрачиваемое на передачу одного информационного пакета, n – число СУ в данном кластере. Так для стандарта IEEE 802.15.4 рабочая частота $f = 868$ МГц, скорость передачи информации $V = 20$ кбит/с, что позволяет вычислить W_{CB} и $T = I/V$, где I – объем информационного пакета.

Остаточное количество энергии для каждого из узлов с учетом (6) определяется из разности:

$$Q_i^k(E) = Q_{k-1} - k \cdot E_i \quad , \quad (4)$$

где k – номер очередного цикла работы СС.

На основании этих матриц определяются количественные показатели как расстояние Махаланобиса от многомерного вектора $a = (D, Q)^T$ до множества $\mu = (d_{\min}, Q_{\max})$:

$$D_M(a) = \sqrt{(a-\mu)^T \cdot K(a,\mu)^{-1} \cdot (a-\mu)}, \quad (5)$$

где $K(a, \mu)$ – матрица ковариаций.

Исходя из количественных показателей осуществляется выбор головного узла в кластере. При каждом следующем цикле функционирования СС построение СГУ и СОУ корректируется исходя из текущей топологии (добавление сенсорных узлов или же отключение узла вследствие нулевой остаточной энергии) и используемых параметров выбора.

Следовательно, в предложенном алгоритме самоорганизация СС функционирует таким образом, что при выходе из строя головного узла, его роль автоматически переходит к любому конечному узлу, находящемуся в зоне действия кластера. Более того, если один из конечных узлов теряет связь со своим головным узлом, то он автоматически переходит в режим поиска любого другого конечного узла и при нахождении его сигнала образуется микро-сенсорная сеть. Таким образом, в СС за счет указанной самоорганизации возможно самовосстановление в случае какого-либо мгновенного воздействия на сеть, на пример, радиоэлектронного, когда со всеми узлами одновременно будет потеряна связь. Проведенное имитационное моделирование показало, что предложенная модель самоорганизации обеспечивает лучшие, чем алгоритм покрытия СРС и другие, характеристики жизненного цикла сенсорных узлов.

Секция № 3

ИНФОРМАЦИОННЫЕ СЕТИ СВЯЗИ

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АСИММЕТРИЧНЫХ АЛГОРИТМОВ NTRU, RSA И ECC

Бубырь А.П., Заросилова М.Г.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. Безопасности информационных технологий,
тел. (057) 702-14-25
E-mail: bubir@datasvit.net

This work is devoted to a comparative analysis of lattice-based public key algorithm NTRU and systems based on integer factorization (RSA) and the elliptic curve discrete log problem (ECC). Durability and speed of encryption/decryption operations were assessed. Conclusions about the advantages and disadvantages of the discussed cryptographic algorithms are given.

Большинство наиболее значимой информации на сегодняшний день передается с помощью глобальной сети Интернет, например: электронные письма, сообщения чатов, видеоконференции, данные электронной коммерции и онлайн-банкинга.

Использование криптосистем с открытым ключом — основной способ защиты таких данных. Наиболее широкое применение получили криптосистема RSA, основанная на сложности факторизации больших чисел, схема Диффи-Хеллмана, DSA, стойкость которых базируется на сложности решения задачи дискретного логарифмирования в поле, семейство алгоритмов на основе эллиптических кривых. Но все они имеют определенные недостатки, основные из которых — это либо сравнительно невысокая скорость работы (напр., алгоритмы на базе ЭК), либо сравнительно низкая стойкость при сопоставимых размерах ключей и параметров (схема Диффи-Хеллмана и другие алгоритмы, основанные на дискретном логарифме в поле), либо и то, и другое одновременно (RSA).

Решить проблему низкой скорости шифрования при сохранении высокого уровня стойкости призван алгоритм NTRU, который был разработан в середине 1990-х годов и впервые представлен на конференции CRYPTO'96. В 2008 году он был включен в стандарт IEEE 1363.1 «Lattice-based public-key cryptography», а модифицированная версия данного алгоритма была взята за основу стандарта ANSI X9.98-2010 «Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry». В этом алгоритме все операции производятся в кольце усечённых многочленов. Криптографическая стойкость NTRU основана на сложности задачи нахождения короткого вектора в заданной решётке.

Цель данной работы — сравнить скорость и стойкость NTRU и криптосистем на основе дискретного логарифма в группе точек ЭК и факторизации целых чисел (RSA).

Для упрощения сравнения стойкости различных алгоритмов стандартом X9.98 введены 4 обширных класса стойкости: «112 бит», «128 бит», «192 бита», «256 бит». Данные уровни стойкости отображают минимальную сложность атаки «грубая сила» - от 2^{112} до 2^{256} операций. Для различных алгоритмов с каждым из этих уровней связаны соответствующая минимальная длина ключа и размеры параметров.

Следующая таблица сравнивает размеры ключей для NTRU с эквивалентными размерами ключей для систем, основанных на проблемах факторизации целых чисел и дискретного логарифма в группе точек эллиптических кривых. Используются следующие обозначения:

- *IPub* - длина открытого ключа в битах
- *IPri* — длина личного ключа в битах

Для NTRU и систем, основанных на проблеме факторизации целых чисел (IF) размер шифротекста равен размеру открытого ключа.

Для систем, основанных на проблеме дискретного логарифма в группе точек эллиптических кривых (ECDL) размер шифротекста отличается в зависимости от схемы шифрования. Например, онлайновый 1-проходный протокол MQV из X9.63-2001 требует три передачи сообщений, при этом каждое сообщение имеет длину, равную длине откры-

того ключа. Оффлайновая 1-проходная схема транспортировки ключа из X9.63 требует одной передачи сообщения размером примерно в *IPub + 2k* бит.

Таблица 1. Сравнение размеров ключей для NTRU и других алгоритмов с открытым ключом

Уровень стойкости *k*, бит	NTRU		RSA	Эллиптические кривые
	IPub	*IPri*	*IPub, IPri*	*IPub, IPri*
112	4411	802	2048	224
	5951	980		
	7249	760		
128	4939	898	3072	256
	6743	1100		
	8371	840		
192	7183	1306	7680	384
	9757	1620		
	11957	1386		
256	9383	1706	15360	512
	12881	2332		
	16489	1738		

Таким образом, NTRU имеет все необходимые условия для обеспечения наивысшего уровня стойкости и по этому показателю не отстает от конкурентов.

Все криптографические системы, основанные на проблемах факторизации целых чисел, дискретного логарифма и дискретного логарифма в группе точек эллиптических кривых потенциально уязвимы к разработке квантового компьютера соответствующего размера, так как для такого компьютера известны алгоритмы, которые могут решить эти проблемы за полиномиальное время, зависящее от размера входных данных. Для NTRU на данный момент квантовых алгоритмов с полиномиальной сложностью не существует. В [2] предлагается квантовый алгоритм редукции в решетках, который может улучшить скорости редукции, но он остается экспоненциальным по сложности, а в [3] рассматриваются алгоритмы для некоторых проблем, связанных с решетками, которые, возможно, будут иметь субэкспоненциальную сложность. Следовательно, только криптосистемы, основанные на алгебраических решетках, остаются практически неуязвимыми для квантового криптоанализа.

Одним из главных преимуществ алгоритма NTRU также является очень высокая скорость выполнения операций зашифрования/расшифрования. По заявлениям компании Security Innovation, занимающейся разработкой NTRU, данный алгоритм до двухсот раз быстрее, чем алгоритмы на эллиптических кривых и RSA и при этом его реализация гораздо меньше (около 8 Кб). В таблице 2 приводятся сравнительные результаты измерений скорости NTRU, ЭК и RSA, полученные этой компанией (использовался процессор с тактовой частотой 2 ГГц).

Таблица 2. Сравнение скорости NTRU, RSA и ЭК, предложенное компанией-разработчиком

Уровень стойкости	Операций/секунда		
	NTRU	ЭК	RSA
112	10638	951	156
128	9901	650	12
192	6849	285	8
256	5000	116	1

В результате собственных измерений быстродействия реализации NTRU на платформе Java было установлено, что для набора параметров ees1499ep1 из X9.98 средняя скорость зашифрования составила 5,4 Мбайт/с, а расшифрования — 5,1 Мбайт/с.

Группой бельгийских ученых [4] были изучены возможности распараллеливания алгоритмов NTRU, RSA и ECC-NIST-224. Скорость работы данных алгоритмов была замерена как на ЦПУ, так и на графических процессорах с использованием технологии распараллеливания CUDA от Nvidia.

Таблица 3. Сравнение скорости реализаций NTRU, RSA и ЭК для ЦПУ и ГПУ

Алгоритм	Язык и платформа	Параметры алгоритма	Зашифр/с	Расшифр/с	Бит/опер.
NTRU	C , Intel Core2 Extreme @ 3.00GHz	(N, q, p) = (1171, 2048, 3) (k = 256)	95	95	1756
	CUDA , GTX280 (1 операция)		571	546	
	CUDA , GTX280 (20000 операций параллельно)		$24*10^3$	$24*10^3$	
RSA	CUDA, Nvidia 8800GTS	2048 bit (k = 112)	-	104	2048
	C++, Intel Core2 @ 1.83GHz		$(6,66*10^3)$	168	
ЭК	CUDA, Nvidia 8800GTS	ECC-NIST-224 (k = 112)	-	$1,41*10^3$	
	C, Intel Core2 @ 1.83 GHz (ECDSA)		-	$1,86*10^3$	

В таблице 3 приведено сравнение реализаций NTRU с использованием ЦПУ и ГПУ и некоторых реализаций RSA и EC. Следует заметить, что количество данных, шифруемых за одну операцию, различно. Для приложений, которым необходима высокая пропускная способность, реализация с помощью CUDA превосходит все остальные реализа-

ции (принимая параметры более высокого уровня безопасности и большее число данных). Данная реализация способна выполнять более 200 тыс. операций зашифрования в секунду или 41,8 Мбайт/с. Для приложений, которым требуется небольшое число шифрований с малой задержкой, распараллеливание с помощью CUDA работает не так быстро по сравнению с реализацией на ЦПУ.

Скорость работы NTRU гораздо выше, чем RSA и EC: он в 1300 раз быстрее 2048-битного RSA и в 117 раз быстрее ECC NIST-224 (если сравнивать количество операций в секунду), или в 1113 раз быстрее, чем 2048-битный RSA (если сравнивать пропускную способность).

Исходя из данных, имеющихся на текущий момент, можно сделать промежуточные выводы о высоком уровне стойкости NTRU, который не уступает стойкости алгоритмов на базе эллиптических кривых, а в некоторых аспектах и превосходит его (устойчивость NTRU к квантовому криптоанализу). Но в связи с относительной новизной и малой распространенностью асимметричных алгоритмов такого класса необходимо проводить дополнительные исследования на предмет возможных закладок и критических уязвимостей, которые могут быть использованы для разработки эффективных атак.

В результате анализа быстродействия NTRU было установлено, что его скорость работы гораздо выше, чем у RSA и ЭК. Наилучшие результаты производительности NTRU показал при его реализации на платформе CUDA, так как он очень хорошо поддается распараллеливанию, в отличие от RSA, попытки распараллелить который практически не дают прироста скорости. При сравнений скоростей NTRU, RSA и ECC с параметрами, соответствующими уровню стойкости k = 256 бит NTRU на 4 порядка быстрее RSA и на 3 порядка быстрее ECC. Также следует отметить меньший размер реализации NTRU (порядка 8 Кб), что очень важно для мобильных и встраиваемых систем, поэтому NTRU относят к алгоритмам «легковесной криптографии».

Класс асимметричных алгоритмов, основанных на проблемах в алгебраических решетках, по совокупности всех показателей значительно превосходит другие алгоритмы с открытым ключом. Поэтому именно NTRU во многих сферах должен прийти на смену RSA и ECC и стать таким же общепринятым стандартом асимметричной криптографии, каким стал AES в сфере блочного шифрования.

Литература:

1. American National Standard for Financial Services ANSI X9.98-2010 Lattice Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry .

2. C. Ludwig: A Faster Lattice Reduction Method Using Quantum Search, TU-Darmstadt Cryptography and Computeralgebra Technical Report No. TI-3/03, revised version published in Proc. of ISAAC 2003

3. Tsukiji Tatsuie, Kamiyama Hiroaki, "Efficient algorithm for the unique shortest lattice vector problem using quantum oracle?", IEIC Technical Report (Institute of Electronics, Information and Communication Engineers), VOL.101;NO.44(COMP2001 5-12);PAGE.9-16(2001).

4. Jens Hermans, Frederik Vercauteren, Bart Preneel. Speed records for NTRU. Department of Electrical Engineering, University of Leuven Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

МЕТОД ПОСТРОЕНИЯ МНОГОФАЗНЫХ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ

Горбенко И. Д., Киянчук Р. И., Замула А. А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14,
каф. Безопасности информационных технологий, тел. (057) 702-14-25
ruslan.kiyanchuk@gmail.com, alexz_@bk.ru

Spread spectrum signals are essential for building effective and widely used radio communication systems. The system quality heavily depends on chosen discrete signals set and their correlation properties. Therefore techniques for generating such high quality signals are needed. Our paper introduces efficient methods for binary and polyphase discrete signals generation. The signals are formed by computing n-th character of Galois field, where n is the number of signal phases. Binary signals generation may be optimized using decimation method which is also described in the paper.

В большинстве случаев среда, в которой работает приёмо-передающая система не способствует надёжному её функционированию. Принятый системой сигнал является результатом наложения шумов и многих копий исходного сигнала с искажёнными параметрами, что усложняет извлечение полученных данных. Для эффективного разрешения сигналов необходимо, чтобы их кодовые последовательности обладали достаточно низкой корреляцией [3]. Чем меньше подобие сигналов, тем проще системе безошибочно их принять даже со значительными искажениями. В условиях сильных шумов (фоновых или созданных намеренно) при ограничении на пиковую мощность передатчика разрешение сигналов становится практически невозможным. Решить данную проблему при частотно-временных измерениях позволяет технология распределённого спектра сигналов.

Одним из методов формирования кодовых последовательностей с соответствующими корреляционными характеристиками является алгоритм построения многопозиционных характеристических дискретных сигналов [2]. Метод основан на вычислении характера конечного поля Галуа --- отображения поля на некоторую абелеву группу. Как будет показано далее, частный случай этого алгоритма (порядок характера простого поля равен 2) позволяет также получить двоичные дискретные сигналы [1].

Функция вычисления k – значного характера поля имеет вид:

$$\psi(a_i) = \exp(j\frac{2\pi}{k})\cdot v_i, \quad (1)$$

где $\begin{cases} p^n - 1 \equiv 0 \bmod k, \\ 2 \le k \le p^n - 1; \end{cases}$

v_i -- индексы элементов поля $GF(p^n)$, упорядоченных в порядке возрастания;

n -- степень расширения поля;

k -- порядок характера конечного поля.

Длина кодовой последовательности равна $p^n - 1$. Метод формирования многопозиционных характеристических дискретных сигналов может быть представлен следующими шагами (операция индексации массива при описании алгоритма показана нижним индексом или квадратными скобками "[...]").

1. Формируется массив индексов $v_i = [0, p^n - 1)$ и массив элементов расширенного поля $GF(p^n)$ путём умножения мультипликативного генератора поля на самого себя до получения всех элементов:

$$a_i = \theta^i(x) \bmod(f(x), p), \quad (2)$$

где $f(x)$ -- неприводимый над полем полином.

Например, поле $GF(3^2)$ состоит из элементов $\{1,3,4,7,2,6,8,5\}$.

2. Формируется массив C инкрементированных элементов поля $GF(p^n)$ по правилу:

$$\begin{aligned} C_i &= 1 \qquad \text{при } \theta^i \equiv 0 \bmod(f(x), p), \\ C_i &= a_i + 1 \quad \text{иначе,} \end{aligned} \tag{3}$$

где $i = [0, p^n - 1)$.

Например, для поля $GF(3^2)$ массив C выглядит так: $\{2,4,5,8,1,7,6,3\}$.

3. Формируется массив K по правилу:

$$K[a_i - 1] = i + 1, \tag{4}$$

где $i = [0, p^n - 1)$.

Пример массива K для поля $GF(3^2)$ выглядит так: $\{1,5,2,3,8,6,4,7\}$.

4. Формируется массив U по правилу:

$$U_i = K[C_i - 1] (\bmod p). \tag{5}$$

Пример массива U над полем $GF(3^2)$: $\{5,0,4,6,1,3,2,7\}$

5. В соответствии с (1) для всех элементов массива U вычисляют $k-$значный характер поля

$$\psi(a_i) = \psi(U_i). \tag{6}$$

В частности,

$$\begin{aligned} &\psi(U_i) = 1 && \text{если } U_i \equiv 0 (\bmod k), \\ &\psi(U_i) = \exp(j\frac{2\pi}{k}) \cdot 1 && \text{если } U_i \equiv 1 (\bmod k), \\ &\vdots \\ &\psi(U_i) = \exp(j\frac{2\pi}{k}) \cdot (k-1) && \text{если } U_i \equiv k-1 (\bmod k). \end{aligned} \tag{7}$$

Формирование множества всех возможных кодов для данного поля возможно путем нахождения всех изоморфных полей.

Как уже сказано ранее, в случае 2-значного характера построение бинарных кодовых последовательностей можно оптимизировать. Нахождение всех неприводимых полиномов и их возведение в степень для построения полей --- ресурсоемкие с точки зрения вычислений операции. Но в случае двоичных последовательностей достаточно построить только базовое поле $GF(p)$, а все изоморфные сигналы возможно получить путем выбора элементов на позициях, номер которых является числом взаимнопростым с $p-1$ [1]. Для заданной кодовой последовательности C нахождение изоморфного сигнала E по децимации D представлено ниже:

$$E_i = C[D * i \bmod(p^n - 1)], \tag{8}$$

где $p^n - 1$ -- период сигнала. Вычислив изоморфные кодовые последовательнсти согласно (8) для всех децимаций, получим множество всех возможных двоичных кодов для данного расширения поля. Мощность этого множества равна функции Ейлера $\phi(p-1)$.

Множество характеристических кодов над простым полем $GF(13)$ для разных характеров представлено в таблице 1.

Таблица 1. Характеристические коды над полем $GF(13)$

Характер	Кодовые последовательности
2	[0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0]
	[0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0]
	[1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0]
	[0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0]
3	[2, 2, 1, 0, 0, 0, 1, 1, 2, 0, 2, 1]
	[0, 2, 0, 2, 2, 1, 1, 0, 0, 1, 1, 2]
	[1, 1, 0, 0, 1, 1, 2, 2, 0, 2, 0, 2]
	[1, 2, 0, 2, 1, 1, 0, 0, 0, 1, 2, 2]
6	[2, 5, 4, 3, 3, 0, 1, 1, 5, 0, 2, 4]
	[0, 2, 3, 5, 5, 1, 4, 3, 0, 4, 1, 2]
	[1, 4, 0, 3, 4, 1, 5, 5, 3, 2, 0, 2]
	[4, 2, 0, 5, 1, 1, 0, 3, 3, 4, 5, 2]
11	[2, 5, 10, 9, 3, 1, 1, 7, 0, 6, 8, 4]
	[1, 8, 9, 0, 5, 1, 4, 3, 6, 10, 7, 2]
	[7, 10, 6, 3, 4, 1, 5, 0, 9, 8, 1, 2]
	[4, 8, 6, 0, 7, 1, 1, 3, 9, 10, 5, 2]

В работе представлены эффективные методы построения многопозиционных и двоичных дискретных характеристических кодов, применимых в технологиях распределенного спектра. Сложность синтезирования данных кодов меньше известных алгоритмов построения дискретных последовательностей [4], что позволяет использовать их в системах с ограниченными вычислительными ресурсами и при этом сохранять высокую производительность.

Литература:

1. Горбенко, И. Д., Замула, А. А. и Бессарабенко, К. В. Ускоренные алгоритмы формирования систем характеристических дискретных сигналов. *Радиотехника*, 84:69-72, 1988.

2. Горбенко, И. Д., Штанько, И. А. и Пестерев, А. К. Ускоренный алгоритм построения многопозиционных характеристических дискретных сигналов. *Радиотехника*, 101, 1997.

3. Ипатов, Валерий П. *Широкополосные системы и кодовое разделение сигналов. Принципы и приложения*. Техносфера, 2007.

4. Свердлик, М. Б. *Оптимальные дискретные сигналы*. «Советское радио», Москва, 1975.

ЗАЩИТА РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СЛОЖНЫХ СИГНАЛОВ

Горбенко И.Д., Замула А.А.
Харьковский национальний университет радиоэлектроники
61166, Харьков, проспект Ленина 14, кафедра безопасности информационных технологий, тел. (057)7021425, E – mail: alexz_@bk.ru

The report suggests methods for the synthesis of a class of complex signals based on the properties of Galois fields. In addition, a theorem on which the characters are established connection elements of the multiplicative group of the Galois field and the dependence of the characters of discrete codes, which use the characters of the multiplicative group. The proposed work describes the ensemble, correlation, statistical and structural properties of one type of complex signals. The possibility of improving immunity, secrecy of the system transfer information using this class of signals.

Введение

Системы передачи информации являются одним из основных видов радиотехнических систем и быстро развиваются во многих отношениях. К таким системам предъявляются все более жесткие требования по обеспечению их работы в условиях сложных внешних воздействий, а так же естественных и преднамеренных помех и помех от других радиотехнических систем, работающих на близких частотах или в общем участке диапазона частот.

Важными характеристиками некоторых систем передачи информации являются помехоустойчивость и скрытность функционирования. Под помехоустойчивостью понимают способность системы противостоять воздействию мощных помех. Скрытность функционирования системы предполагает способность системы функционировать в режиме, затрудняющим обнаружение передаваемых сообщений и оценку их параметров специальной разведывательной аппаратурой злоумышленника. Одним из видов скрытности является информационная скрытность. Такой вид скрытности предполагает целый комплекс мер, методов и средств для затруднения определения злоумышленником: самого факта передачи сообщений по каналам связи, содержания передаваемых сообщений и другое. Комплексное решение проблемы обеспечения помехоустойчивости, скрытности функционирования системы передачи информации может быть достигнуто, в том числе, на основе реализации динамического режима передачи информации, при котором соответствие: бит сообщения – сигнал меняется с течением времени по закону, предсказание которого возможно с вероятностью, не превышающей допустимую. Одним из путей достижения заданной помехоустойчивости, является реализация частотной избыточности в канале связи.

Большое значение при решении задач обеспечения требуемой помехоустойчивости и скрытности функционирования (в том числе, информационной скрытности) имеют исследования, связанные с использованием новых видов сигналов, получивших название: сложных, широкополосных, многомерных и шумоподобных. Разработка методов синтеза сложных сигналов с хорошими корреляционными, ансамблевыми, статистическими, структурными и другими свойствами является актуальной задачей.

При радиоэлектронном противодействии эффективная помеха может быть организована только после обнаружения присутствия противостоящей системы в эфире и оценки таких ее параметров как частотный диапазон и занимаемая полоса. Если скрытная система использует сигнал с некоторым законом модуляции, параметры которого неизвестны перехватчику, то последний лишен возможности применения согласованного фильтра или коррелятора для обнаружения сигнала. В этих условиях у противостоящей системы нет иного выбора, как рассматривать перехватываемый сигнал в виде случайного и основывать его обнаружение только на факте появления или отсутствия некоторого избытка энергии в некотором участке частотного диапазона. Перехватчик применяет энергетический детектор, называемый также радиометром, который является оптимальным с точки

зрения обнаружения ограниченного по полосе шумового сигнала на фоне аддитивного белого гауссовского шума [1].

Перехватчику могут быть неизвестны заранее сведения о частотном диапазоне и интервале времени, занимаемом сигналом. Учитывая эти обстоятельства, его стратегия будет заключаться в комбинировании указанных параметров, осуществляя процедуру обнаружения либо путем сканирования частотно-временной области, либо используя набор параллельных каналов, каждый из которых ответственен за анализ ограниченного участка частотно-временной области. В любом случае качество работы приемника системы-перехватчика будет полностью определяться характеристикой энергетического детектора, настроенного на истинную для перехватываемого сигнала частотно-временную зону. В свою очередь, у скрытной системы имеется только единственная возможность предотвратить обнаружение своего сигнала потенциальным перехватчиком: использовать сигналы с распределенным спектром, обладающие максимально возможным значением выигрыша от обработки (произведение полосы частот, занимаемой сигналом на его длительность). Единственной причиной, вынуждающей перехватчик прибегнуть к такому неэффективному инструменту как энергетический приемник, является отсутствие информации о структуре обнаруживаемого сигнала, т.е. его закона модуляции. По этой причине перехватчик не может обрабатывать сигнал аналогично приемнику скрытной системы (т.е. осуществлять согласованную фильтрацию). Очевидно, что в случае недостаточной структурной сложности сигнала и осведомленности перехватчика о его возможных альтернативных вариантах, последний может попытаться их все реализовать. Соответствующим оборудованием для этого может служить набор параллельных согласованных фильтров либо единый перестраиваемый фильтр (несколько фильтров), пригодный для обработки сигналов различных по структуре последовательно во времени, если сигнал, который необходимо обнаружить, принимается достаточно долго. Поэтому другая сторона стратегии скрытной системы в борьбе с перехватчиком состоит в применении сигналов с практически не раскрываемой структурой.

Основное содержание исследований

В приложениях, имеющих дело с безопасностью информации, степень защиты данных определяется числом равновероятных ключей, с помощью которых криптоаналитик старается взломать шифротекст, т.е. зашифрованные данные. Применительно к структуре сигнала каждый из таких ключей есть ничто иное, как закон модуляции, который, как правило, повторяется с периодом T. Предположим, что сигнал построен на основе M - ичного алфавита, т.е. возможны M реализаций индивидуального сигнального элемента (чипа). Если полоса, отводимая системе, равна W, то общее сигнальное пространство имеет размерность, определяемое как WT, т.е. закон модуляции может быть сконструирован посредством WT чипов. Очевидно, что величина M^{WT} определяет общее число различных законов модуляции, т.е. число ключей, и, значит, разработчик, отвечающий за секретность модуляционного формата разрабатываемой системы, должен использовать сигналы с достаточно большим выигрышем от обработки. Таким образом технология широкополосности в значительной степени способствует криптографической защите структуры сигнала.

Усилия исследователей направлены на поиски ансамблей сложных сигналов, характеристики которых с ростом длины приближаются к характеристикам гипотетического ансамбля, т.е. ансамбля, все представители которого обладают нулевой постоянной составляющей, идеальной периодической автокорреляционной функцией (ПФАК) и нулевой периодической функцией взаимной корреляции (ПФВК). Широко распространенным критерием подобного приближения является минимаксный критерий, ориентирующий синтез ансамбля на минимизацию максимального значения на множестве всех нежелательных корреляций. Для идеального гипотетического ансамбля корреляционный пик как наибольшее из двух величин: максимума среди всех боковых лепестков автокорреляций последовательностей и максимума среди значений взаимных корреляций всех пар

последовательностей равны нулю, а для любого реального ансамбля корреляционный пик может служить адекватной мерой его близости к идеальному.

Ансамбли со значением корреляционного пика достигающие предела, предсказываемого нижними границами Велча и Сидельникова [1], являются оптимальными по критерию корреляционного пика, и иногда называются минимаксными.

Синтез семейств сигналов с необходимыми авто и взаимно корреляционными свойствами заключается в отыскании семейства дискретных последовательностей, обладающего соответствующими авто и взаимно корреляционными функциями. Искусство проектирования широкополосных систем во многих аспектах базируется на нахождении сигналов с соответствующими корреляционными свойствами.

Минимизация уровня боковых лепестков автокорреляционной функции (АКФ) имеет наибольшее значение при конструировании сигнала для таких приложений как измерение времени запаздывания, временное разрешение и др. Следует иметь в виду, что равенство нулю всех боковых лепестков невозможно для финитных или апериодических фозоманипулированных сигналов.

При синтезе сигналов применяют минимаксный критерий, который требует достижения минимально возможной величины максимального бокового лепестка АКФ апериодического кода. Очевидно, что предпочтительными являются кодовые последовательности с наименьшим значением максимального бокового лепестка. Таким образом требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка АФАК.

Сформулированная выше оптимизационная задача, как и многие другие задачи дискретной оптимизации, не имеют общего аналитического решения.

Обсуждаются методы синтеза оптимальных бинарных последовательностей большой длины с заданными авто - и взаимнокорреляционными свойствами.

Рассмотрены так называемые характеристические дискретные сигналы (ХДС) с числом позиций (символов) $L = 4x + 2$ и $L = 4x$, синтез которых базируется на использовании характера ψ мультипликативной группы поля $GF\,(P)$ [2].

Правило кодирования таких кодов, например, для $L = 4x + 2$ имеет вид [2]:

$$\mu = \{\mu_i : i = 0, 1, \ldots, P-2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\mathrm{mod}\, P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\, P), \qquad (1)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\mathrm{mod}\, P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\, P), \qquad (2)$$

где Θ - первообразный элемент поля $GF\,(P)$.

Мощность метода кодирования данного класса сигналов (М) равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \varphi(L)/2$.

Известно так же [2], что правила кодирования ХДС с числом позиций (символов) $L = 4x + 2$ приводят к коду с двухуровневой периодической функцией автокорреляции $R_\mu = \{-2, 2\}$.

Максимальные по модулю значения боковых лепестков функции автокорреляции импульсного бинарного фазоманипулированного сигнала, построенного на базе кода μ находятся в пределах $(0{,}47 \div 0{,}82)/\sqrt{L}$.

Способ формирования ХДС длительностью L, который приведен в работе [2], сводится к составлению таблицы соответствия i-й элемент поля ($a_i = \theta_j^i + 1$ (θ_j^i - первообразный элемент поля)) - i-й индекс. Для составления таблицы необходимо решить L сравнений вида:

$$a_i \equiv \Theta_j^{U_i} (\mathrm{mod}\ P),\ i = \overline{0, P-1}, \qquad (3)$$

где Ui – индекс элемента поля GF(P), определяемый из решения сравнения (1). Данный способ из-за отсутствия алгоритмизируемых процедур трудно осуществим.

В работах [3,4] предложены способ и устройство формирования ХДС. Способ основан на рекуррентной зависимости между элементами и индексами элементов поля Галуа, при этом становится возможным алгоритмизировать процедуры формирования символов ХДС. Однако вычислительная сложность, (время формирования ХДС) остается значительной.

Приводятся теоремы, на основании которых устанавливаются связи характеров элементов мультипликативной группы поля Галуа и зависимость символов дискретных кодов, построенных на использовании характеров мультипликативной группы поля. Выявленные и описанные в теоремах связи элементов и характеров элементов поля позволяют алгоритмизировать процедуры формирования символов ХДС, и, кроме того, повысить быстродействие устройств формирования ХДС что несомненно оказывает влияние на успешное решение ряда задач, в том числе, реализацию динамического режима передачи информации.

Формулируется и приводится доказательство теоремы, с использованием которой появляется возможность синтезировать все множество изоморфизмов характеристических дискретных сигналов. Показано, такой синтез может быть реализован посредством децимации сигнала, построенного по одному из первообразных элементов поля Галуа. Формулируются требования к выбору коэффициентов децимации.

Даются оценки помехоустойчивости и скрытности функционирования системы передачи информации при использовании характеристических дискретных сигналов.

Выводы

В докладе приводится анализ возможностей применения различных ансамблей минимаксных последовательностей для ряда приложений информационных систем, в частности, в качестве: манипулирующих или расширяющих спектр в системах передачи информации с шумоподобными сигналами, управляющих последовательностей в системах передачи информации с псевдослучайной перестройкой рабочей частоты, «исходного материала» для ключевых последовательностей символов в криптографии и др.

Литература:

1. Valery P. Ipatov Spread Spectrum and CDMA principles and Applications// Univesity of Turku.

2. Свердлик М.Б. Оптимальные дискретные сигналы. М., 1975. 200 с.

3. Горбенко И.Д., Замула А.А.. Ускоренные алгоритмы построения систем характеристических дискретных сигналов //Радиотехника. 1988. Вып. 84. с.69-72.

4. А.с. СССР Устройство для формирования псевдослучайных сигналов / В.И. Долгов, И.Д. Горбенко – 1983.- № 5. – с. 63.

ОБГРУНТУВАННЯ ВИМОГ ДО МЕТОДІВ ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Гріненко Т.О., Мордвінов Р.І.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Леніна, каф. Безпеки інформаційних технологій, тел. (057) 702-14-25,
E-mail: bit@kture.kharkov.ua, факс (057)7021425

It is grounded requirements to pseudorandom number generators. The research results concerning provided methods are based on hash functions, block cipher algorithms and number theoretic problems.

Генератори випадкових чисел, ймовірно, є одним із самих основних елементів криптографічних примітивів. Вони широко використовуються для генерування ключів, паролів, загальносистемних параметрів та ін. На практиці реалізацію отримали два основних методи генерування ключів – на основі використання випадкових чисел, що формуються з використанням фізичних випадкових процесів, та які не можуть бути відновлені в просторі та часі, та на основі використання псевдовипадкових чисел, що можуть бути відновленими в просторі і часі.

До детермінованих генераторів випадкових послідовностей (ДГВП) та методів, за якими формуються псевдовипадкові послідовності (ПВП) висунуто ряд вимог. Основними з них є: пряма та зворотна непередбачуваність чисел або структурна скритність, складність або швидкодія генерування, необоротність функції генерування ключа, під якою розуміється обчислювальна складність визначення ключа ДГВП, що застосовується, захищеність генератора від впливу на процес генерування ключа, а також забезпечення заданого періоду повторення ПВП. При цьому рівень гарантій в суттєвій мірі залежить від ентропії джерела ключів і на сьогодні вона повинна складати від 80 до 512 бітів. На наш погляд, цим вимогам значною мірою можуть задовольняти генератори ПВП, які розроблені з використанням переваг теоретико-числових задач (наприклад, задачі дискретного логарифма в групі точок еліптичних кривих) [1]. При забезпеченні вимог випадковості і/або непередбачуваності такого генератора рішення задачі криптоаналіза буде експоненційно складним. У загальному випадку для побудови генератора ПВП використовується однобічна функція. Для побудови таких однобічних функцій використовуються функції, складність яких ґрунтується на складності дискретного логарифму або на складності факторизації великого числа.

Зважаючи на актуальність та необхідність якісного забезпечення перелічених вимог на світовому та національному рівнях застосовується практика стандартизації вимог до методів, механізмів та засобів генерації та тестування ПВП [2-7].

Серед стандартів генерування випадкових послідовностей бітів уже визнаними на міжнародному рівні є ISO 19790 [2], ISO/IEC 18031 [3] та ANSI X9.98 [4]. В них з різною мірою деталізації визначені вимоги до ДГВП, методи та алгоритми їх реалізації на основі теоретико-числових задач, блокових симетричних шифрів та на основі перетворення з використанням необоротних колізійно стійких функцій.

Спираючись на описані в стандарті ДСТУ ISO/IEC 18031 схеми генераторів випадкових бітів були реалізовані генератори випадкових бітів на геш-функціях та в групі точок ЕК і перевірено їх статистичні характеристики за допомогою методики NIST STS. Результати тестування розглянутих ДГВП підтвердили високий рівень випадковості послідовностей, що були згенеровані в процесі досліджень.

Основними обмеженнями методів, що викладені в ISO 19790 та ISO/IEC 18031, є відсутність доведення стійкості генератора до компрометації ключа, що використовує цей генератор та непередбачуваності як до раніше, так і після генеруємих псевдовипадкових бітів. Необхідно також відмітити і недоліки конкретних методів генерування послідовностей ПВБ, що представлені в стандарті ISO/IEC 18031, тобто на основі блокових шифрів, вирішення теоретико-числових задач та гешування. При застосуванні методу, що

базується на використанні колізійно стійких функцій гешування залишаються проблемними питання визначення значення величини періоду повторення.

У табл. 1 наводяться дані по проходженню ПВП тестів за Правилом 1.

Таблиця 1.

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (71%)	189 (100%)
SHA1 (ISO/IEC 18031)	132 (69%)	188 (99%)
SHA2 256 (ISO/IEC 18031)	130 (68%)	187 (98%)
SHA2 384 (ISO/IEC 18031)	133 (70%)	189 (100%)
SHA2 512 (ISO/IEC 18031)	141 (74%)	189 (100%)
AES (ISO/IEC 18031)	138 (73%)	189 (100%)
DES (ISO/IEC 18031)	132 (69%)	188 (99%)
ГОСТ 28-147 (ISO/IEC 18031)	132 (69%)	188 (99%)
TDES (ISO/IEC 18031)	135 (71%)	189 (100%)
ДГВП на ЕК (ISO/IEC 18031)	129 (68,25%)	189 (100%)

У табл. 2 представлені зведені результати по проходженню генераторами тестів за Правилом 2.

Таблиця 2.

Генератор	Кількість тестів, у яких значення ймовірності $P \le 0{,}01$	Кількість тестів, у яких значення ймовірності $P \le 0{,}001$
BBS	0	0
SHA1 (ISO/IEC 18031)	0	0
SHA2 256 (ISO/IEC 18031)	0	0
SHA2 384 (ISO/IEC 18031)	3	0
SHA2 512 (ISO/IEC 18031)	0	0
AES (ISO/IEC 18031)	0	0
DES (ISO/IEC 18031)	4	1
ГОСТ 28-147 (ISO/IEC 18031)	1	0
TDES (ISO/IEC 18031)	3	0
ДГВП на ЕК (ISO/IEC 18031)	1	0

У [1] наведено удосконалений метод і алгоритми побудови ДГВП на основі використання криптографічних перетворень в групі точок ЕК над простими і розширеннями полів Галуа та застосування стійких до колізій функцій гешування, використання якого дозволить формувати ПВП з необхідними властивостями нерозрізнюваності та необоротності.

Задача оцінки необоротності запропонованого генератора у цілому по суті зводиться до послідовного вирішення двох задач – спочатку знаходження по відомому виходу генератора (геш-значення) його прообразу, а потім по відомому прообразу до вирішення задачі дискретного логарифмування в групі точок еліптичних кривих з визначенням секретного ключа генератора. Доказано, що складність обернення генератора ПВП на основі застосування гешування носить експоненційний характер. При цьому складність суттєво зменшується, якщо криптоаналіз здійснюється на основі створення колізій. Найбільш

складною є атака знаходження прообразу. Генератор ПВП, що ґрунтується на використанні як скалярного множення на еліптичній кривій так і гешування, має складність обернення більшу ніж атака «груба сила». Це означає, що для цього методу атака типу «груба сила» є найбільш ефективною з точки зору криптоаналітика.

Запропонований у [1] математичний апарат дозволяє також зробити оцінки ймовірностей виникнення колізій геш-значень точок еліптичних кривих, а також вибрати довжини геш-значень, наприклад, допустимі значення. При цьому необхідно враховувати, що на практиці довжини геш-значень є стандартизованими – 160, 256, 384 та 512 бітів, а також знайти обмеження на число символів випадкової послідовності бітів, які можуть генеруватись на одному і тому ж ключі.

Увага до генераторів псевдовипадкових послідовностей на ЕК з боку криптологів зростає. На наш погляд, для систем захисту інформації з доказовим рівнем стійкості та систем, які не потребують жорстких часових обмежень, найбільш придатним для застосування є генератор на еліптичній кривій, оскільки він має доказовий теоретичний рівень стійкості. Застосування математичного апарата груп точок ЕК дозволяє побудувати різні генератори ПВП. Основними методами формування ПВП є методи, що засновані на операціях додавання й множення в групах точок ЕК.

Література:

1. Гріненко Т.О., Горбенко Ю.І., Мордвінов Р.І. Властивості та перспективи застосування генераторів псевдовипадкових послідовностей на еліптичних кривих. – Системи обробки інформації. ХУПС. Вип. 2(92) – 2011. – С.76-80.

2. ISO/IEC 19790:2006. Information technology – Security techniques – Security requirements for cryptographic modules.

3. ISO/IEC 18031. Information technology — Security techniques — Random bit generation, 2005.

4. American National Standard for Financial Services ANSI X9.98 - 2010 Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry, 2010.

5. ANSI/X9 X9.82-3:2007. Random Number Generation, Part 3: Deterministic Random Bit Generators. Accredited Standards Committee X9 Incorporated, 11-Sep-2007 – 113 pages.

6. AIS 20. Functionality classes and evaluation methodology for Deterministic random number generators. BSI. 1999.

7. AIS 31. Functionality classes and evaluation methodology for true (physical) random number generators. BSI. 2001.

МЕТОД СТРУКТУРИРОВАННОЙ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Замула А.А., Черныш В. И., Иванов К.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25)
E-mail: vlad.chernish@gmail.com, тел. (063) 208-44-30

The method of analytical work in structuring risk of IS. A seven components described method steps.

Информационная безопасность (ИБ) в настоящее время становится необходимым условием успешного развития хозяйствующего субъекта. Риск компрометации информации влияет на материальные и нематериальные активы организации и, в конечном счёте, на результаты её производственно-экономической деятельности. В связи с широким спектром возможных информационных рисков, значительным разбросом значений ущерба при их реализации и ограниченностью бюджета на информационную безопасность возникает задача рационального финансирования затрат на защиту информации. Возможна и другая постановка задачи: при фиксированном объеме финансовых вложений необходимо снизить уровень риска компрометации информации до минимального значения.

Оценка информационных рисков (ИР) проводится с использованием методов, требующих статистических данных по инцидентам, либо использующих некоторые категории значимости ИР. Недостатком таких методов является тот факт, что величина ИР имеет (чаще всего) субъективные значения, что вносит существенную погрешность в результаты их оценки. С другой стороны, оценка рисков с помощью экспертных методов вносит помеху в виде неточности оценки.

Цель процесса оценивания рисков состоит в определении характеристик рисков в информационной системе (ИС) и ее ресурсах. На основе таких данных выбираются необходимые средства управления ИБ.

В докладе предлагается метод выполнения аналитических работ по структурированию рисков ИБ. Метод включает в себя 7 шагов. Приводится характеристика шагов предлагаемого метода.

Шаг 1: Описание системы. На этом шаге проводится сбор сведений для определения границ и описания системы на различных иерархических уровнях с целью выявления уязвимостей и оценки достаточности принятых мер защиты.

Шаг 2: Идентификация источников угроз. Целью данного шага является определение потенциальных источников угроз для оцениваемой ИТ-системы и составление списка актуальных источников угроз для данной информационной системы.

Шаг 3: Идентификация уязвимостей. Целью данного шага является создание списка уязвимостей (недостатков или упущений), которыми могут воспользоваться потенциальные источники угроз.

Шаг 4: Анализ контроля безопасности. Цель данного шага – анализ средств контроля, уже внедренных компанией или планируемых для внедрения для уменьшения или устранения вероятности использования уязвимости системы.

Шаг 5: Определение вероятности. На данном шаге вычисляется значение вероятности успешной атаки, которое зависит от потенциала угрозы, создаваемой активным источником угрозы в поле уязвимости (табл. 1).

Шаг 6: Определение риска. Цель данного этапа заключается в определении максимального уровня риска при успешной реализации атаки от i-го источника по j-й уязвимости.

Простой способ получения оценок ИР для каждой пары угроза/уязвимость, который можно заложить в механизм оценки ИР, заключается в перемножении вероятности реализации угрозы и ущерба от реализации угрозы с последующим ранжированием полученных значений.

Таблица 1. Показатели веса вероятности успешной атаки

Эффективность защиты *Z(i,j)*	Потенциал угрозы *U(i,j)*				
	1	2	3	4	5
0 (защита отсутствует)	1	2	3	4	5
1	0	1	2	3	4
2	0	0	1	2	3
3	0	0	0	1	2
4	0	0	0	0	1
5	0	0	0	0	0

Табличные данные отражают пороговый эффект, связанный с преодолением защиты и получены на основе операции алгебраической разности. Распределение числовых значений показателя уровня вероятности приведено в таблице 2.

Таблица 2. Шкала значений уровня вероятности реализации угрозы

Уровень вероятности		Описание уровня
1	Очень низкий	Используемые средства защиты и методы их применения гарантируют защиту по отношению к данному типу угроз в пределах заданной уязвимости (используются сертифицированные профили защиты).
2	Низкий	У источника угрозы недостаточно мотиваций или возможностей, либо существующие средства контроля способны предотвратить или, по крайней мере, значительно помешать использованию уязвимости.
3	Средний	Источник угрозы мотивирован и обладает возможностями, но существующие средства контроля могут препятствовать успешному использованию уязвимости.
4	Высокий	Источник угрозы имеет высокие мотивации и достаточные возможности, а методы контроля для предотвращения проявления уязвимости не гарантируют защиту.
5	Очень высокий	Уровень мотивации, технические и организационные возможности источника угроз превышают соответствующие параметры защиты.

Шаг 7: Рекомендации по контролю и оформление итоговых документов. Данный шаг обеспечивает средства контроля, которые могут снизить или устранить идентифицированные риски и которые являются подходящими для данной компании. Целью рекомендуемых методов контроля является снижение уровня рисков для ИТ-системы и ее данных до приемлемого уровня.

После завершения оценки ИР (идентифицированы угрозы и уязвимости, оценены риски, рекомендованы средства контроля) следует оформить документацию в виде официального отчета или кратких инструкций.

В предложенном методе структурирования появляется возможность получения качественных и количественных оценок величин риска с максимальной возможностью учета априорных данных и результатов предварительных исследований характеристик и свойств ИР. Полученные оценки ИР могут быть использованы при разработке концепции обеспечения ИБ на этапе создания ИС, и для поддержания установленного уровня риска на этапе эксплуатации ИС.

МЕТОД ФОРМИРОВАНИЯ МНОЖЕСТВА ДИСКРЕТНЫХ СИГНАЛОВ С ЗАДАННЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

Замула А.А., Ярыгина Т.Е.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. БИТ, тел. (057) 702-14-25,
E-mail: yarigina.tatyana@gmail.com

The advantages of noise-like signals in spread spectrum communication systems are noise immunity, secrecy, code division of subscribers, ability to evaluate coordinates of moving objects, electromagnetic compatibility, etc. They are based on large ensembles of weakly correlated signals. Currently there are no efficient methods for discrete sequences synthesis of optimal minimax criterion. It is also difficult to estimate how close are the known signals to optimal sequences. All known methods for discrete sequences synthesis are based on brute force computation, which exceedingly limits their applications. Our paper proposes method that significantly (in comparison with known exhaustion methods) reduces computation complexity of synthesizing discrete sequences with certain correlation sidelobe.

Помехозащищенность, скрытность, кодовое разделение абонентов, измерение координат подвижных объектов, электромагнитная совместимость – далеко не весь перечень преимуществ применения шумоподобных сигналов в широкополосных системах связи.

При установлении синхронизации и разрешении сложных сигналов важную роль играют корреляционные свойства дискретных последовательностей (ДП), с помощью которых расширяется спектр. Предположим, что приемник сложных сигналов вычисляет соответствующую корреляционную функцию принимаемого сигнала с эталонной копией, хранящейся в памяти. После осуществления синхронизации он переходит в режим приема информации и начинает операцию декодирования последней. Любые частичные корреляции могут привести к ложному срабатыванию и нарушению работы приемника. Очевидно, что не любая КП может быть использована для таких целей. Требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка корреляционной функции [1]. Назовем такой критерий минимаксным.

В настоящее время отсутствуют регулярные методы синтеза ДП оптимальных по минимаксному критерию. Более того, довольно сложно оценить, насколько известные сигналы большой длины близки к оптимальным. Все известные методы синтеза ДП включают в себя перебор, что существенно ограничивает область их применения. К методам синтеза ДП относят [2]:

1. Метод направленного перебора.

Синтез предусматривает два этапа. Первый ориентирован на сужение области перебора и состоит в формулировке необходимых условий существования и допустимых комбинаторных соотношений параметров. Второй заключается в разработке эффективных переборных алгоритмов. Этим методом были найдены все бинарные последовательности Баркера с $N < 13$.

2. Метод синтеза апериодических ДП на основе периодических.

Идея метода основана на взаимосвязи периодической и апериодической АКФ для одной и той же ДП. Метод также состоит из двух этапов. Первый заключается в поиске ДП с «хорошей» ПАКФ. Второй — в поиске оптимальных по минимаксному критерию начальных условий. С помощью этого метода найдены оптимальные по минимаксному критерию бинарные и троичные последовательности. Однако второй этап этого метода также переборный и, следовательно, является существенным ограничением возможностей по периоду (длине) синтезируемой ДП.

3. Синтез ДП путем гомоморфного отображения мультипликативных групп простого и расширенного поля Галуа с помощью *k*-значного характера.

Последний метод, как показано в [3], поглощает практически все известные правила кодирования линейных ДП. Однако, с ростом характеристики поля и числа классов объем вычислений при направленном переборе резко увеличивается.

Существует и ряд других методов. Проблемы их усовершенствования состоят в синтезе ДП с «хорошей» ПАКФ и сокращении времени на этапе перебора. Метод, предлагаемый в данной работе, позволяет на этапе перебора существенно снизить объем вычислений по нахождению ДП с заданными значениями боковых лепестков корреляционной функции. В качестве ДП будем рассматривать характеристические дискретные сигналы (ХДС).

Пусть W_μ и W_ν есть ХДС с числом символов L, построенные посредством децимации исходного сигнала W_1 (сигнал, построенный по наименьшему из значений первообразных элементов поля) соответственно по коэффициентам μ и ν, а μ' и ν' новые коэффициенты децимации, причём $\mu' = \mu \cdot x(\mathrm{mod}\, L)$; $\nu' = \nu \cdot x(\mathrm{mod}\, L)$, где x – целое число, такое, что наибольший общий делитель (НОД) чисел x и L равен 1. Тогда децимация исходного ХДС W_1 по коэффициентам μ' и ν' дает новые пары, реализация ПФВК которых есть результат децимации ПФВК пары ХДС W_μ и W_ν.

Значение кодов ХДС, полученных путём децимации исходной последовательности по коэффициентам μ и ν, могут быть описаны выражениями [3]:

$$\mu_i = \begin{cases} \psi\left(\Theta_a^{\mu_i} + 1\right), если \left(\Theta_a^{\mu_i} + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta_a^{\mu_i} + 1\right) \equiv 0 (\mathrm{mod}\, P); \end{cases} \quad (1)$$

$$\nu_i = \begin{cases} \psi\left(\Theta_m^{\nu_i} + 1\right), если \left(\Theta_m^{\nu_i} + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta_m^{\nu_i} + 1\right) \equiv 0 (\mathrm{mod}\, P), i = \overline{0, L-1}. \end{cases} \quad (2)$$

Поскольку всегда можно найти такое k, что $\Theta_1 = \Theta^k$, где $\Theta = \Theta_1^\mu$, $\Theta_1 = \Theta_1^\nu$, и НОД $(k, L) = 1$, то (1) и (2) можно записать в следующем виде:

$$\mu_i = \begin{cases} \psi\left(\Theta^i + 1\right), если \left(\Theta^i + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta^i + 1\right) \equiv 0 (\mathrm{mod}\, P); \end{cases} \qquad \nu_i = \begin{cases} \psi\left(\Theta_1^i + 1\right), если \left(\Theta_1^i + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta_1^i + 1\right) \equiv 0 (\mathrm{mod}\, P). \end{cases}$$

Для сигналов, полученных по μ' и ν', имеем

$$\mu_i' = \begin{cases} \psi\left(\Theta^{i_1 x} + 1\right), если \left(\Theta^{i_1 x} + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta^{i_1 x} + 1\right) \equiv 0 (\mathrm{mod}\, P); \end{cases} \qquad \nu_i = \begin{cases} \psi\left(\Theta_1^{i_1 x} + 1\right), если \left(\Theta_1^{i_1 x} + 1\right) / \equiv 0 (\mathrm{mod}\, P); \\ 1, если \left(\Theta_1^{i_1 x} + 1\right) \equiv 0 (\mathrm{mod}\, P). \end{cases}$$

Выражения для ПФВК пар ХДС, построенных соответственно по μ, ν и μ', ν' имеют вид:

$$R_{\mu,\nu}(m) = \sum_{i=0}^{L-1} \psi\left(\Theta^i + 1\right) \psi\left(\Theta_1^{i+m} + 1\right); \qquad R_{\mu',\nu'}(m) = \sum_{i=0}^{L-1} \psi\left(\Theta^{i_1 x} + 1\right) \psi\left(\Theta_1^{(i+m_1)x} + 1\right).$$

И с учётом (1)

$$R_{\mu,\nu}(m) = \sum_{i=0}^{L-1} \psi\left(\Theta^i + 1\right) \psi\left(\Theta^{k(i+m)} + 1\right); \qquad R_{\mu',\nu'}(m) = \sum_{i=0}^{L-1} \psi\left(\Theta^{i_1 x} + 1\right) \psi\left(\Theta^{kx(i_1+m_1)} + 1\right)$$

Введём произвольные переменные $\{a,b,b^{'}\}\in GF(P^n)$. Пусть для сигналов, построенных путём децимации исходного сигнала, выполняются условия $a=\Theta^{k(i+m)}$, $b=\Theta^{i}$. Тогда $a/b=\Theta^{ki+km-i}$. Для пары сигналов, полученных путём децимации исходного сигнала по коэффициентам $\mu^{'}$ и $\nu^{'}$, найдём некоторое значение $\Theta^{kx(i_1+m_1)}$ равное a, т.е.

$$\Theta^{kx(i_1+m_1)}=\Theta^{k(i+m)}=a. \tag{3}$$

Для выполнения равенства (3) необходимо, чтобы

$$kx(i_1+m_1)\equiv k(i+m)(\mathrm{mod}\,L). \tag{4}$$

Поскольку НОД $(k,L)=1$, выражение (4) можно переписать в виде

$$x(i_1+m_1)\equiv i+m(\mathrm{mod}\,L);\; xi_1+xm_1\equiv i+m(\mathrm{mod}\,L);$$
$$xi_1\equiv i(\mathrm{mod}\,L);\; xm_1\equiv m(\mathrm{mod}\,L).$$

Найдём отношение $a/b^{'}$, где $b^{'}=Q^{i_1x}$ для пары ХДС, построенной в соответствии с $\mu^{'}$ и $\nu^{'}$.

$$a/b^{'}=\frac{\Theta^{kx(i_1+m_1)}}{\Theta^{i_1x}}=\Theta^{kxi_1+kxm_1-i_1x}. \tag{5}$$

С учётом (5) можно заключить, что $a/b^{'}=a/b$, и следовательно, $b^{'}=b$. А это означает, что в выражении для ПФВК $R_{\mu^{'},\nu^{'}}(m_1)$ изменится лишь порядок набора суммы для некоторого фиксированного отсчёта ПФВК пары ХДС, построенной по $\mu^{'}$ и $\nu^{'}$. Другими словами, значения функции ПФВК для пары ХДС, построенной путём децимации исходного сигнала по коэффициентам $\mu^{'}$ и $\nu^{'}$ будут такими же, как для ПФВК последовательностей, полученных по μ и ν. Но с учётом того, что $m=xm_1$, $R_{\mu^{'},\nu^{'}}(m_1)$ - есть результат децимации $R_{\mu,\nu}(m)$ по коэффициенту x, т.е. реализация ПФВК $R_{\mu^{'},\nu^{'}}(m_1)$ будет результатом децимации ПФВК $R_{\mu^{'},\nu^{'}}(m)$.

Пусть $\|R\|$ есть матрица максимальных значений боковых лепестков ПФВК пар ХДС w_i и w_j, $i,j=\overline{1,M}$ размерности $M\times M$, причём M – число изоморфизмов ХДС, а строки и столбцы матрицы обозначены значениями упорядоченных по возрастанию коэффициентов децимации. Тогда строка матрицы (первая строка), содержащая значения боковых лепестков ПФВК исходного изоморфизма со всеми оставшимися $(M-1)$ изоморфизмами, содержит все возможные значения боковых лепестков ПФВК, которые дают пары w_i и w_j, $i,j=\overline{1,M}$.

Очевидно, что для определения значений максимальных боковых выбросов ПФВК сочетаний всех пар ХДС достаточно рассчитать реализации ПФВК исходного сигнала w_1 со всеми оставшимися w_2, w_3, …, w_{M-1} изоморфизмами, т.е. реализации ПФВК для первой строки матрицы $\|R\|$.

В таблице приведена взаимокорреляционная матрица боковых лепестков ПФВК для ХК с числом элементов $L=$ 60 для пар ХК. Первая строка матрицы включает в себя значения боковых лепестков ПФВК исходного кода (коэффициент децимации $k_1=1$) со всеми другими ХК, полученными путём децимации исходного ХДС по множеству коэффициентов децимации $k_i\in\varphi$ (L). Исходя из данных таблицы, минимальное значение максимальных боковых лепестков ПФВК имеет место для пар ХК, полученных по коэффициентам децимации 1 и 7.

Таблица 1. Взаимокорреляционная матрица для ХДС с числом элементов $L = 60$

Коэф. децимации / Коэф. децимации	1	7	11	13	17	19	23	29	31	37	41	43	47	53	59	49
1	60	16	24	20	20	16	20	36	32	20	36	16	20	20	16	28
7	16	60	20	16	24	20	36	20	20	32	20	28	36	16	20	16
11	24	20	60	20	16	36	20	16	36	20	32	20	20	16	28	16
13	20	16	20	60	36	16	24	20	16	28	20	32	16	36	20	20
17	20	24	16	36	60	20	16	20	20	36	20	16	32	28	16	20
19	16	20	36	16	20	60	20	24	28	16	16	20	20	20	36	32
23	20	36	20	24	16	20	60	16	20	16	16	36	28	32	20	20
29	36	20	16	20	20	24	16	60	16	20	28	20	16	20	32	36
31	32	20	36	16	20	28	20	16	60	16	24	20	20	20	36	16
37	20	32	20	28	36	16	16	20	16	60	20	16	24	36	20	20
41	36	20	32	20	20	16	16	28	24	20	60	20	16	20	16	36
43	16	28	20	32	16	20	36	20	20	16	20	60	36	24	20	16
47	20	36	20	16	32	20	28	16	20	24	16	36	60	16	20	20
53	20	16	16	36	28	20	32	20	20	36	20	24	16	60	16	20
59	16	20	28	20	16	36	20	32	36	20	16	20	20	16	60	24
49	28	16	16	20	20	32	20	36	16	20	36	16	20	20	24	60

Соответствующим образом могут быть установлены все пары ХДС, приводящие к таким же значениям боковых лепестков. Например, умножая коэффициенты децимации $k = 1$ и $k = 7$ на $x = 7$, мы получим новую пару изоморфизмов ХДС, для которой $k = 49$ и $k = 49$. Как следует из таблицы, данная пара ХДС имеет такое же значение максимальных боковых лепестков ПФВК как и для исходной пары, т. е. 16. Нетрудно убедиться в том, что знание значений первой строки взаимокорреляционной матрицы является исчерпывающим для расчёта статистических характеристик ПФВК системы ХДС.

Оценим вычислительную сложность предложенного метода исследования корреляционных свойств ДП. Полный перебор всех возможных пар ДП характеристического кода для получения значений максимальных боковых лепестков функции корреляции требует выполнения N_1 операций. Очевидно, что $N_1 = C^2_{\varphi(L)}$. Для реализации предлагаемого метода число операций N_2 определяется из соотношения $N_2 = \varphi(L)$.

Выигрыш в вычислительной сложности (C) предлагаемого метода перебора по сравнению с известным оценивается соотношением:

$$C = N_1 / N_2 = \frac{1}{2}(\varphi(L) - 1) \qquad (6)$$

Анализ выражения (6) показывает, что выигрыш в вычислительной сложности представленного метода с увеличением числа элементов L ДП возрастает. Приведенные в таблице данные позволяют выбрать ДП, минимизиирующие вероятность ошибок при синхронизации и различении сигналов.

Литература:

1. Spread Spectrum and CDMA. Principles and Applications. Valery P. Ipatov, Univesity of Turku

2. Гантмахер В.Е., Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. Анализ, синтез, обработка – СПб.: Наука и Техника, 2005. – 400 с.

3. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Советское радио, 1975. - 200 с.

СЖАТИЕ ИЗОБРАЖЕНИЙ С ПОТЕРЯМИ БЕЗ ВИЗУАЛЬНО ЗАМЕТНЫХ ИСКАЖЕНИЙ: ПРИМЕНЕНИЯ, ПРОГРЕСС, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ

Зеленский А.А., Земляченко А.Н., Кривенко С.С., Лукин В.В., Пономаренко Н.Н.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»
Кафедра приема, передачи и обработки сигналов, ул. Чкалова, 17, ХАИ, 31070, Харьков,
Тел. +380577884504, e-mail lukin@ai.kharkov.com

Lossy compression of images without visible distortions can be applied in medical diagnostics, consumer digital cameras, remote sensing, etc. A problem is how to carry out such lossy compression automatically. The paper deals with considering visual quality metrics that can be used for this purpose and the corresponding thresholds for these metrics to be set. Then, automatic procedure and software to be applied are described. They are applied to a wide set of test images and it is demonstrated that a provided compression ratio varies in the limits from 3 to 20 depending upon image characteristics. Novel coders that can improve either compression ratio of visual quality are described. The problems and perspectives of further design and analysis are considered. Some results for images of different types are presented.

Разнообразные изображения являются одним из основных типов данных, передаваемых по сетям связи и используемых в повседневной жизни, медицине, неразрушающем контроле, дистанционном зондировании (ДЗ). Рост числа изображений и занимаемой ими памяти опережает увеличение пропускной способности каналов связи и памяти средств хранения данных. В связи с этим значительное внимание уделяется совершенствованию методов и алгоритмов сжатия изображений. Коэффициенты сжатия (КС), достигаемые при применении сжатия без потерь, часто не удовлетворяют пользователей. Поэтому все чаще используются методы сжатия с потерями.

Несмотря на наличие таких стандартов сжатия с потерями как JPEG и JPEG2000, продолжаются исследования в области разработки новых методов сжатия без потерь. Их актуальность обусловлена желательностью улучшить характеристики кодеров – повысить КС, автоматизировать сжатие с обеспечением желаемого качества. При этом под качеством для изображений часто понимают визуальное качество, поскольку оно имеет важное значение для медицинских приложений [1], обычных цифровых фотографий, данных ДЗ [2], и т.д. Для многих приложений сжатия с потерями первоочередной задачей является обеспечение приемлемого визуального качества или внесение таких искажений, которые были бы визуально незаметны.

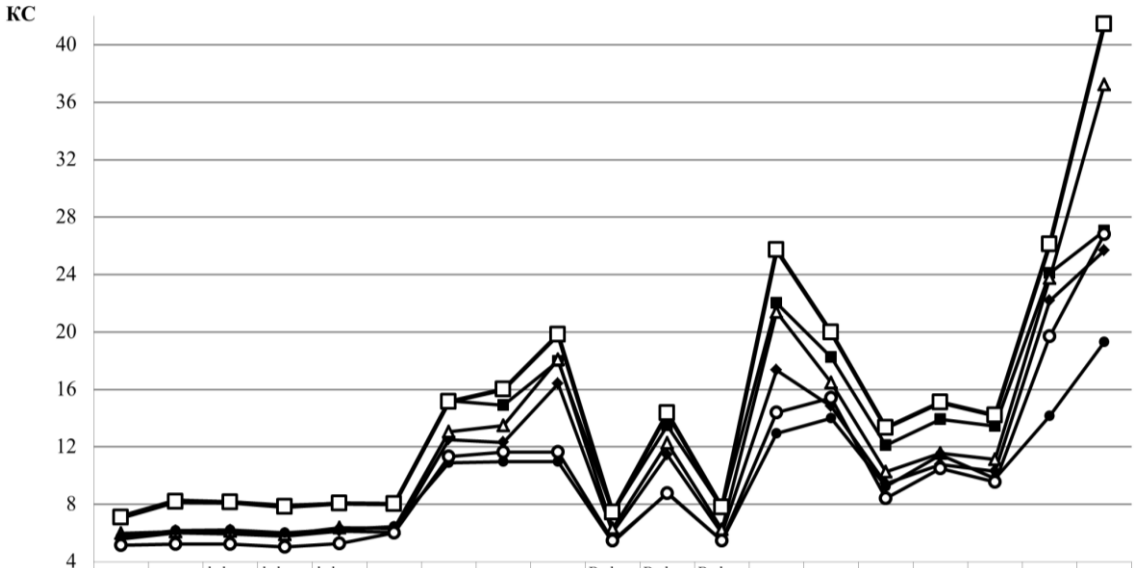
Решение этой задачи осложнено рядом факторов. Во-первых, традиционные метрики (среднеквадратическая ошибка, пиковое отношение сигнал-шум) неадекватно характеризуют визуальное качество сжатых изображений [3]. Во-вторых, даже для недавно разработанных метрик визуального качества до последнего времени отсутствовали практические рекомендации по значениям их параметров, при которых внесенные сжатием с потерями искажения визуально незаметны. Недавно проведенные исследования [4] позволили установить, что метрики PSNR-HVS-M и MSSIM достаточно адекватно характеризуют визуальное качество сжатых изображений. Более того, если при сжатии достигается PSNR-HVS-M>40 дБ или MSSIM>0,985, то с большой вероятностью (выше 0,8) вносимые искажения визуально незаметны. Поскольку при наличии исходного (сжимаемого) и сжатого изображений возможно определить значение контролируемой метрики, то имеются предпосылки для сжатия изображений с потерями с обеспечением визуально незаметных искажений.

Однако для достижения такого сжатия необходимо иметь соответствующие процедуры, позволяющие обеспечить значение используемой метрики не хуже заданного. В настоящее время эти процедуры предусматривают неоднократное сжатие и декомпрессию сжимаемого изображения, расчет значения метрики после каждой итерации и изменение параметров кодера с целью обеспечить значение метрики с требуемой точностью. Итеративность процедуры является одним из ее недостатков. Число итераций зависит от многих факторов: используемого метода сжатия; стартовых значений параметров, управ-

ляющих степенью сжатия, и пределов их изменения; организации итеративной процедуры; требуемой точности обеспечения значения метрики; свойств сжимаемого изображения. При отсутствии априорной информации о пределах варьирования параметра, управляющего сжатием (шага квантования или bpp), число итераций может быть порядка 10.

Прежде, чем рассматривать частные вопросы повышения быстродействия сжатия, покажем, что применение сжатия с потерями без визуально заметных искажений целесообразно на практике. На рис. 1 приведены значения КС для шести методов сжатия с потерями для достаточно большого числа тестовых изображений с различной степенью сложности (текстурности). Данные приведены для метрики MSSIM=0,985, обеспечиваемой с точностью 0,002.

Рассмотрены следующие методы сжатия: JPEG с неравномерной таблицей квантования коэффициентов дискретного косинусного преобразования (ДКП); SPIHT, которые по принципу функционирования и обеспечиваемым результатам аналогичен JPEG2000; не адаптированные под визуальное качество кодеры AGU и ADCT, в основу которых также положено ДКП в блоках (версии доступны для скачивания на http://ponomarenko.info/#dow); адаптированные под визуальное качество кодеры AGU-M и ADCT-M, также на основе ДКП. Четыре последних кодера были разработаны с участием сотрудников каф. 504 ХАИ. В качестве тестовых использовались стандартные тестовые изображения Baboon, Barbara, Peppers, Cameraman, Airfield в градациях серого, а также цветовые компоненты цветных вариантов некоторых из этих изображений и ряд других. В нижней части рис. 1 для удобства приведена таблица значений КС, позволяющая более точно провести сравнение эффективности кодеров.



	grass	baboon	baboon red	baboon green	baboon blue	airfield	goldhill	boat	Barbara	Barbara red	Barbara green	Barbara blue	camera man	peppers	peppers red	peppers green	peppers blue	Lenna	pole
AGU	5,58	6,04	5,96	5,79	6,13	6,07	12,49	12,31	16,4	6,08	11,44	6	17,36	14,84	9,43	10,77	10,3	22,17	25,69
AGU-M	7,2	8,32	8,2	7,96	8,05	7,97	15,22	14,89	17,98	7,43	13,49	7,75	22,04	18,23	12,1	13,91	13,44	24,12	27,05
ADCT	6	6,12	6,15	5,91	6,37	6,33	13,05	13,5	18,1	6,33	12,28	6,27	21,38	16,47	10,25	11,58	11,15	23,76	37,25
ADCT-M	7,08	8,19	8,16	7,85	8,06	8,02	15,13	16	19,82	7,43	14,37	7,8	25,72	19,97	13,32	15,11	14,21	26,1	41,45
JPEG	5,76	6,19	6,24	6,03	6,26	6,44	10,89	10,97	10,96	5,35	8,83	5,47	12,96	14,02	9,26	11,43	9,8	14,16	19,31
SPIHT	5,16	5,22	5,22	5,03	5,28	6,03	11,32	11,63	11,63	5,49	8,76	5,49	14,38	15,42	8,42	10,49	9,55	19,69	26,8

Рис. 1. Значения КС для разных тестовых изображений и кодеров при MSSIM=0,985

Анализ приведенных зависимостей позволяет сделать ряд важных выводов. Во-первых, примерно одно и то же визуальное качество изображений наблюдается при существенно разных КС. Для текстурных изображений (Grass, Baboon) значения КС лежат в пределах от 5,2 до 8,2 (в зависимости от кодера), а для изображений с простой структурой, имеющих большие однородные участки (Lenna, Pole), значения КС достигают 41,5 для наилучшего из кодеров. Во-вторых, для изображений со сложной структурой JPEG

обеспечивает более высокие значения КС по сравнению с кодером SPIHT, а для изображений с простой структурой имеет место обратная ситуация.

Кодеры AGU и ADCT имеют преимущества в степени сжатия по сравнению с JPEG и SPIHT лишь для изображений со сравнительно простой структурой. Модификации AGU-M и ADCT-M обеспечивают, как правило, наибольшую степень сжатия. AGU-M характеризуется более высоким быстродействием, поскольку для ADCT-M выполняется оптимизация схемы разбиения изображения на блоки неодинакового размера.

Основной вывод состоит в том, что для всех рассмотренных методов сжатия с потерями (но без визуально заметных искажений) обеспечиваемые значения КС в разы, а для простых изображений и в десятки раз превосходят значения КС для методов сжатия без потерь, для которых значения КС редко превосходят 2 при обработке изображений в градациях серого. Аналогичные закономерности и результаты получены при использовании метрики PSNR-HVS-M=40 дБ. Если установить большие значения метрик, например, MSSIM=0,99 или PSNR-HVS-M=42 дБ, то закономерности не изменятся, лишь значения КС уменьшатся примерно на 20%.

Нами были проведены исследования для других типов изображений: полученных путем сканирования страниц книг и буклетов (яркостная компонента), рентгеновские изображения, данные многозонального дистанционного зондирования систем AVIRIS и HYPERION (раздельно для каждого канала). Полученные значения КС лежат в том же диапазоне (обычно от 7…8 до 25…35), а сравнительная эффективность кодеров та же, то есть наилучшие значения КС достигаются для кодеров ADCT-M и AGU-M. Более того, если исходные изображения представлены не в виде 8-битных данных, а с использованием большего числа бит (например 16), то целесообразно привести их к диапазону 0…255 путем простых линейных преобразований (масштабирования), а затем применить сжатие с потерями. При этом КС существенно возрастает. Кроме того, при расчете метрики $PSNR\text{-}HVS\text{-}M=10\lg(D^2/MSE_{HVS\text{-}M})$ динамический диапазон представления изображения D может быть легко учтен ($MSE_{HVS\text{-}M}$ – среднеквадратическая ошибка, рассчитываемая с учетом разной чувствительности зрения к искажениям в разных пространственных частотах и эффектов маскирования).

Применимость предлагаемого подхода к сжатию была оценена и с других точек зрения. В частности, к декомпрессированным изображениям текстов на страницах отсканированной книги были применены автоматизированные распознаватели текста. Оказалось, что при сжатии таких изображений с обеспечением PSNR-HVS-M=40 дБ и даже немного меньше сжатие не оказывает влияния на вероятность правильного распознавания текста.

При PSNR-HVS-M>42 дБ сжатие практически не оказывает влияния на вероятность правильной классификации данных многозонального дистанционного зондирования. Более того, для изображений, на которых визуально заметен шум, имеет место его небольшое подавление (эффект фильтрации).

Возвращаясь к рассмотренной выше проблеме итеративности процедур обеспечения заданного значения метрики, отметим следующее. Для кодеров с варьированием КС путем изменения шага квантования (ШК) (что справедливо для всех кодеров на основе ДКП), проведены предварительные исследования значений ШК при обеспечении заданных значений метрик.

В этом плане интересна зависимость, приведенная на рис. 2, где представлены значения ШК при обеспечении PSNR-HVS-M=40 дБ для кодера AGU-M при сжатии ряда тестовых изображений. Очевидно, что значения ШК для рассмотренных изображений мало отличаются. В данном случае в среднем они чуть меньше 12, изменясь в пределах от 10,2 до 13,5. Следовательно, возможны различные практические решения. Например, можно для сжатия всех изображений использовать ШК=10, пожертвовав при этом достижением более высокого значения КС, но обеспечив сжатие без использования итерационной процедуры. Хотя для выработки окончательных рекомендаций необходимо прове-

дение более тщательных исследований, использование такого подхода представляется перспективным.

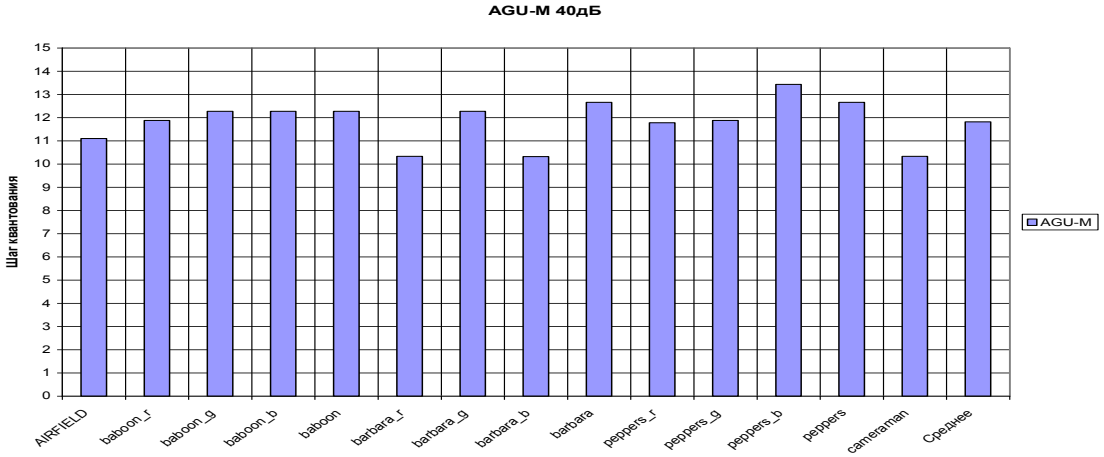


Рис. 2. Значения ШК для разных изображений

Дополнительные перспективы открываются при сжатии многоканальных изображений, начиная с обычных цветных изображений и заканчивая многозональными (гиперспектральными). Для таких изображений характерна спектральная избыточность (высокая коррелированность сигнальной составляющей в компонентных изображениях), что делает целесообразным применение трехмерных кодеров [5]. Как показывают результаты [5], при этом могут быть достигнуты значения КС в 2...3 раза больше, чем при поканальном сжатии.

Однако для реализации трехмерного сжатия необходимо, чтобы используемый шаг квантования был приемлемым для изображений во всех каналах. В связи с этим примерное постоянство ШК независимо от особенностей сжимаемого изображения, продемонстрированное выше, может быть полезно и при разработке методов сжатия в рамках рассматриваемого подхода с использованием трехмерных кодеров, что является еще одним перспективным направлением дальнейших исследований.

Литература:

1. A. Fidler, U. Skaleric, B. Likar, The impact of image information on compressability and degradation in medical image compression, Med. Phys. 33(8), pp. 2832-2838, August 2006.

2. Лукин В.В., Зряхов М.С., Кривенко С.С., Станкевич С.А., Попов М.А., Лищенко Л.П. Сжатие гиперспектральных изображений с потерями и их классификация, Авиационно-космическая техника и технология, ХАИ, Харьков, № 1/79, 2011. – С. 86-95.

3. Wang Z., Simoncelli E.P., Bovik A.C., Multi-scale Structural Similarity for Visual Quality Assessment, Proceedings of the 37th IEEE Asilomar Conference on Signals, Systems and Computers, Vol. 2, pp. 1398-1402, 2003.

4. V. Lukin, M. Zriakhov, S. Krivenko, N. Ponomarenko, Z. Miao, Lossy compression of images without visible distortions and its applications, Proceedings of ICSP 2010, Beijing, October, 2010, pp. 694-697.

5. N. Ponomarenko, M. Zriakhov, V. Lukin, A. Kaarna, Improved Grouping and Noise Cancellation for Automatic Lossy Compression of AVIRIS Images, Proceedings of ACIVS, Springer, Heidelberg, LNCS-6475, Part II, Australia, 2010, pp. 261-271.

ВПЛИВ ВЛАСТИВОСТЕЙ ТРАФІКУ НА ПАРАМЕТРИ ЯКОСТІ ОБСЛУГОВУВАННЯ ВУЗЛА МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ

М.М. Климаш, О.А. Лаврів, Б.А. Бугиль
Національний університет «Львівська політехніка»
73013, Україна, м. Львів, вул. Професорська, 2, Інститут телекомунікацій, радіоелектроніки та електронної техніки,
кафедра «Телекомунікації», тел. +38(032) 258-24-44
E-mail: o.lavriv@gmail.com

This work has proposed a model of quality of service provision for a multiservice network's node on the basis of its structural and functional parameters optimizing. The investigation of QoS dependence from structural and functional parameters of network node and input traffic parameters had been considered.

Вступ

При передаванні значних обсягів мультимедійної інформації виникають негативні чинники, які призводять до перевантаження мережевих вузлів, зростання затримок та збільшення їх варіації. Найбільш значний вплив на процес передавання даних здійснюють розподільчі вузли, в яких виникають черги на обслуговування, тому важливим завданням є визначення їх структурно-функціональних параметрів, які гарантують забезпечення необхідної якості обслуговування. В роботі [1] проаналізовано проблему забезпечення якості обслуговування в IP мережі і показано основні механізми QoS, що застосовуються в мережах з пакетною комутацією. Встановлено, що існує і до кінця не вирішена проблема оптимального вибору ресурсів мережі для гарантування замовленої абонентом якості надання послуг. В роботах [2,3] описано способи дослідження параметрів якості обслуговування мережевих вузлів шляхом їх аналітичного моделювання з використанням методів удосконаленої теорії масового обслуговування. Показано, що дана задача є актуальною у зв'язку зі зміною структури та властивостей трафіку мультисервісних мереж. Однак, згадані методи дозволяють лише наближено оцінити параметри системи обслуговування мультимедійного трафіку, адже в них допускається наближення реального розподілу трафіку до відомих аналітичних розподілів на основі зближення їх ентропії. В даній статті запропоновано оцінювати необхідні структурно-функціональні параметри системи обслуговування на основі імітаційного статистичного моделювання вхідного трафіку та аналітичного моделювання механізму обслуговування. Проведено моделювання обслуговування за порядком черги із врахуванням затримок, які виникають в обслуговуючому пристрої.

Моделювання та дослідження параметрів якості обслуговування системи розподілу мультисервісного трафіку з обслуговуванням за порядком черги і вхідним самоподібним трафіком

Спосіб моделювання вхідного потоку та визначення необхідного розміру буфера для його обслуговування запропоновано в [4]. На основі даних досліджень і розробленої моделі обслуговування за порядком черги проведено моделювання залежності параметрів якості обслуговування (затримки, джитеру, розміру буфера) від структурно-функціональних параметрів вузла обслуговування та параметрів вхідного трафіку.

Вхідні умови моделювання: кількість пакетів – 50 тисяч; діапазон зміни пропускної здатності вхідного та вихідного інтерфейсу від 10 Мбіт/с до 100 Мбіт/с; діапазон зміни тривалості обробки пакету обслуговуючим пристроєм рівний 0,1 нс до 1 нс та швидкості внутрішньої шини мережевого вузла від 1 Гбіт/с до 2 Гбіт/с.

Обслуговуючий пристрій здійснює опрацювання пакету за формулою:

$$\Delta T_{обслуговування} = \Delta T_{буфер} + 2 * \frac{\Delta R_{пак.}}{V_{шини}} + T_{обробки} \qquad (1)$$

де $V_{шини}$ – швидкість внутрішньої шини обслуговуючого пристрою (прийнято, що швидкості вхідної і вихідної шин рівні);

$\Delta T_{буфер}$ – тривалість очікування пакетом у буфері;

$\Delta R_{пак.}$ – довжина пакету;

$T_{обробки}$ – тривалість опрацювання пакету у процесорі обслуговуючого пристрою;

$\Delta T_{обслуговування}$ – тривалість обслуговування пакету.

Отриманий за методом, описаним у (4), трафік надходить на обслуговуючий пристрій, що представляє собою послідовність чотирьох елементів: буфера, внутрішньої вхідної шини, власне обслуговуючого пристрою та внутрішньої вихідної шини. Інтенсивність обслуговування визначається на проміжках 1 мс. Швидкість внутрішньої вхідної і вихідної шини $V_{шини}$ становить 1 Гбіт/с. Тривалість обслуговування пакету залежить від його довжини $\Delta R_{пак.}$, тривалості обробки обслуговуючим пристроєм $T_{обробки}$ і очікування у буфері $\Delta T_{буфер}$. Алгоритм обслуговування пакету наведено на рис. 1.

Зупинка роботи алгоритму може бути здійснена двома способами: або за досягненням заданої точності результату (значення коефіцієнту варіації другого порядку), або за вичерпанням всіх пакетів, які входять до вхідного потоку.

Визначення параметрів системи обслуговування проводиться на основі результатів імітаційного моделювання.

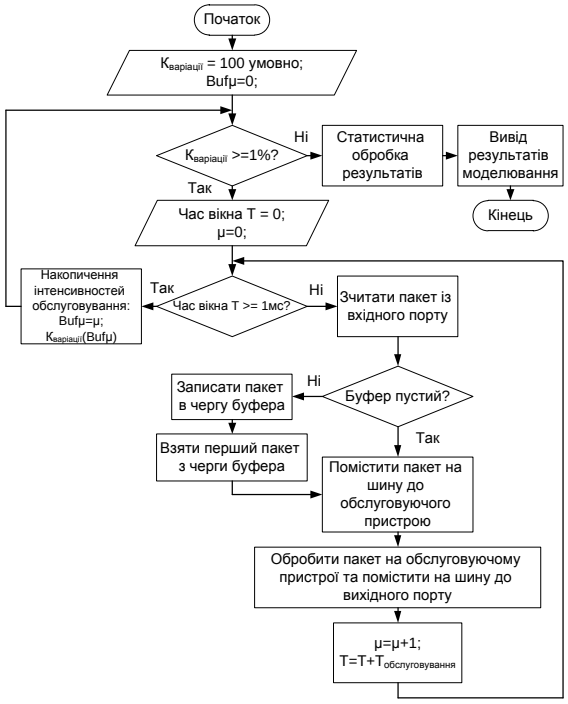


Рис. 1. Алгоритм обслуговування за чергою вхідного мультисервісного потоку одноканальною системою

Результатом роботи імітаційної моделі є вихідний потік дискретних інтенсивностей обслуговування μ з кроком 1 мс. Використовуючи згенерований вхідний потік [4], було розраховано коефіцієнт використання системи для різних значень пропускної здатності вхідного інтерфейсу. На рис. 2 показано графік залежності розміру буфера від коефіцієнту використання системи обслуговування. Значення розміру буфера були розраховані за методом, описаним у [3]. Даний метод виражає розмір буфера через параметр Херста і коефіцієнт використання системи. На кожному кроці моделювання змінювалась пропускна здатність вхідного/вихідного інтерфейсу, що зумовлювало зростання коефіцієнту використання системи, а також кількості пакетів, що надійшли у буфер (рис 3).

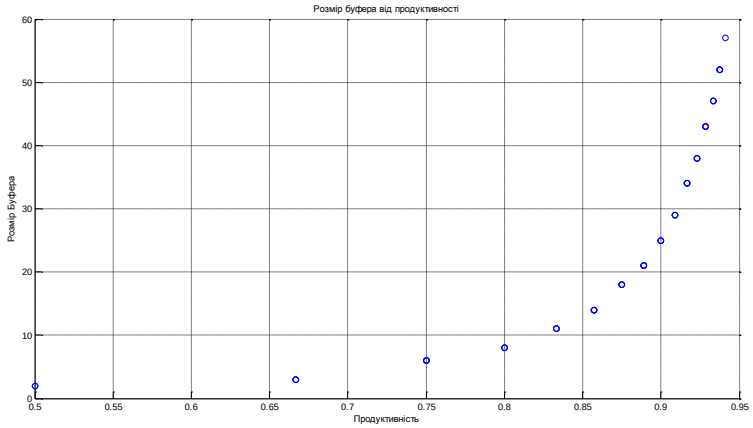


Рис. 2. Залежність розміру буфера від коефіцієнту завантаженості системи обслуговування

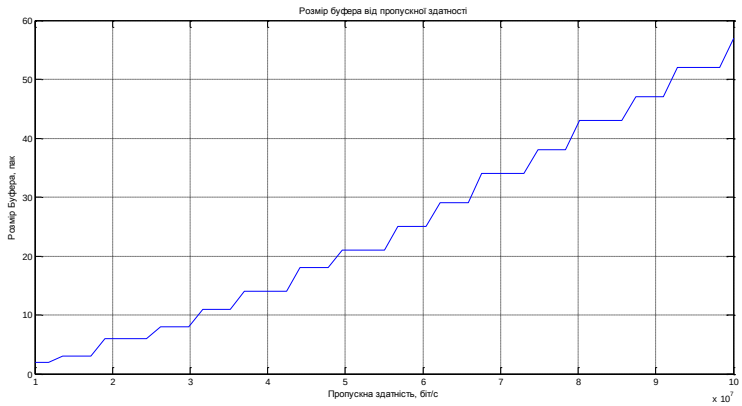


Рис. 3. Залежність розміру буфера від пропускної здатності вхідного інтерфейсу

В імітаційній моделі реалізовані головні структурно-функціональні вузли обслуговуючого пристрою. Одним із них є буфер. На рис. 4 показано вміст буфера на кожному кроці моделювання. Зафіксований пік завантаженості буфера становить 75 пакетів, що є дещо більшим показником за розрахований вище по методу [3]. Середнє значення розміру буфера становить 42,24 пакети. Враховуючи дану залежність, для передбачення безвтратної роботи обслуговуючого пристрою, потрібно збільшити розмір буфера до 75 пакетів * 750 байт = 56,25 Кбайт для інтервалу 1 мс. Враховуючи статистичний характер моделювання і похибку моделювання 15%, оптимальний розмір буфера повинен бути додатково збільшеним на 15%.

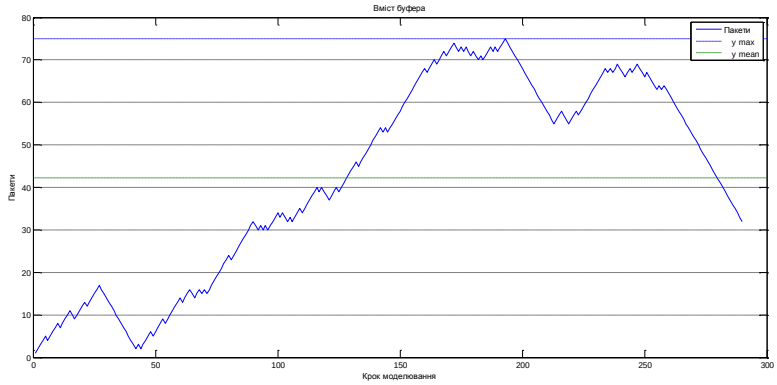
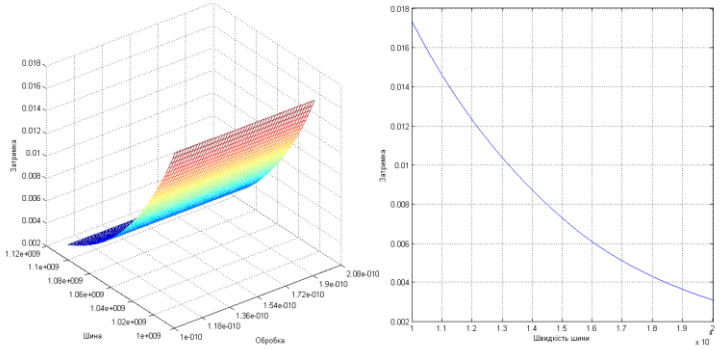


Рис. 4. Профіль завантаженості буфера в процесі моделювання

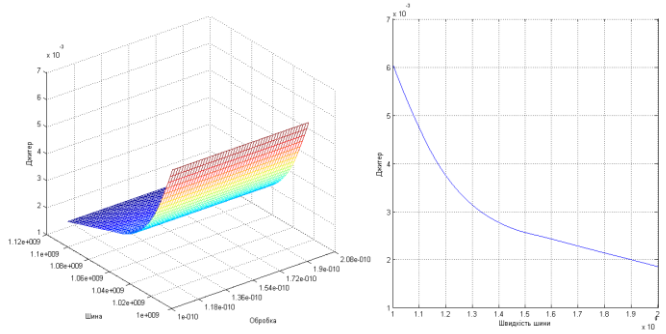
Оскільки, вміст буфера відстежувався під час моделювання, було визначено усереднені значення затримки пакетів відносно параметрів системи обслуговування, залежність представлена на рис. 5 (а,б).



а) *б)*

Рис. 5. Залежність затримки пакетів від параметрів системи обслуговування

Аналізуючи масив затримок, визначено середній джитер пакетів та його залежність від параметрів системи обслуговування (рис. 6 (а,б)).



а) *б)*

Рис. 6. Залежність джитера від параметрів системи обслуговування

Висновок

У роботі проведено імітаційне моделювання та дослідження параметрів якості обслуговування системи розподілу мультисервісного трафіку. За отриманими результатами сформовано рекомендації щодо вибору необхідних структурно-функціональних параметрів такої системи, а також проведено дослідження залежності параметрів якості сервісу від зміни параметрів системи обслуговування і властивостей вхідного потоку. Встановлено, що зі зростанням коефіцієнту використання мережевого вузла розмір буфера зростає за експонентою і при високих значеннях даного коефіцієнта зростає по прямій. Зі зростанням параметру Херста розмір буфера також зростає. Розроблена модель дозволяє по заданих затримці та джитеру вибрати оптимальні параметри системи обслуговування. Даний підхід може бути використаний на етапі проектування мультисервісної мережі.

Література:

1. Evans J., Filsfils C. Deploying IP and MPLS QoS for Multiservice Networks. Theory and Practice. – London: Elsevier Science, 2007. – 456 p.

2. Ложковский А.Г. Исследование системы обслуживания с ожиданием и рекуррентным потоком вызовов // Наукові праці ОНАЗ ім. О.С. Попова. – 2004. – № 2. – С. 56–59.

3. Ложковский А.Г., Ганифаев Р.А. Оценка параметров качества обслуживания самоподобного трафика энтропийным методом // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1 – С. 57–62.

4. Лаврів О.А. Моделювання та дослідження параметрів QoS в системі розподілу інформації з самоподібним вхідним потоком і обслуговуванням за порядком черги. Матеріали науково-практичної конференції «Проблеми телекомунікацій – 2011». – 2011 р.

ОЦЕНИВАНИЕ ВЗАИМНОЙ ЗАДЕРЖКИ ШИРОКОПОЛОСНЫХ СИГНАЛОВ ПРИ НЕГАУССОВЫХ ПОМЕХАХ

Куркин Д.А., Зеленский А.А., Лукин В.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»
Кафедра приема, передачи и обработки сигналов, ул. Чкалова, 17, ХАИ, 31070, Харьков,
Тел. +380577884504, e-mail lukin@ai.kharkov.com

Time delay estimation is used in tele- and video-conferencing, hydro-acoustics, etc. Most methods are designed under assumption of Gaussian noise in channels of interferometric antenna system. However, recent studies show that noise cannot be considered Gaussian quite often and it can be intensive. The studies show that in such situations it is possible to apply alternative methods of signal processing and time delay estimation. They can be based on robust estimates. Noise in the paper is modeled as symmetric α-stable process. It is shown that for α of about 1.5 the proposed methods outperform the classical ones.

Для ряда практических приложений целью обработки сигналов, принятых пространственно-разнесенными сенсорами, является оценивание взаимной задержки информационных широкополосных (часто шумоподобных) сигналов. Такая ситуация характерна для акустических систем определения направления на говорящего для современных комплексов, используемых при проведения теле- и видеоконференций, а также для пассивных гидроакустических систем определения пеленга источника случайного широкополосного сигнала [1, 2].

Классический метод оценивания временной задержки (при известном расстоянии между сенсорами) состоит в получении взаимной корреляционной функции (ВКФ) принятой смеси информационного широкополосного сигнала и шума и определении координаты наибольшего максимума ВКФ, которая затем пересчитывается в угловую координату (пеленг). Этот метод дает удовлетворительные результаты (является оптимальным) в предположении высокого отношения сигнал-шум, аддитивных независимых гауссовых помех в каналах приема и достаточного времени накопления (регистрации) сигналов при практической неподвижности источника излучения. Если же эти предположения вследствие тех или иных причин не соблюдаются в реальной ситуации, то эффективность классического метода резко снижается [2].

Исследования показывают, что акустический шум в помещении или с шум водной поверхности часть нельзя считать гауссовыми и они лучше апроксимируются симметричным α-стабильным (СаС) распределением с $\alpha = 1{,}6$ и $\alpha = 1{,}5$ соответственно [1]. Напомним, что гауссово распределение является частным случаем СаС распределения при $\alpha = 2$, а при $\alpha < 2$ по мере уменьшения α наблюдается резкий рост тяжести хвостов распределения (возрастание импульсивности шума). Как следствие, применение традиционных методов обработки перестает быть оптимальной процедурой.

На практике есть еще два фактора, которые определяют методику обработки. Во-первых, желательно выполнять расчет ВКФ достаточно быстро (практически в реальном времени), что, как правило, обеспечивает благодаря применению алгоритмов быстрого преобразования Фурье с получением взаимного спектра принятых колебаний. Во-вторых, желательно иметь возможность накапливать несколько элементарных реализаций с целью варьирования эффективного времени накопления и минимизации вероятности появления аномальных оценок взаимной задержки, которые могут привести к срыву слежения и другим негативным последствиям [3, 4]. Накопление обычно реализуют путем совместной обработки нескольких последовательно полученных оценок взаимного спектра, после чего рассчитывают ВКФ и оценивают взаимную задержку.

Суть предлагаемых модификаций состоит в том, что при получении оценки взаимного спектра для нескольких последовательных фрагментов принятых колебаний используются робастные оценки сдвига вместо обычного усреднения. Целью проведенных ис-

следований является сравнение точности определения взаимной задержки между сигналами, при применении различных методов расчета взаимного спектра.

Предположим, что имеется только два пространственно-разнесенных приемника, регистрирующие набор элементарных реализаций (фрагментов) вида

$$U_1^m(t) = S^m(t) + n_1^m(t),$$

$$U_2^m(t) = S^m(t - \tau_m) + n_2^m(t),$$

где $S^m(t), t = \left[T_{in}^m ; T_{fin}^m \right]$ – m-й фрагмент информационного широкополосного шума, $n_1^m(t)$ и $n_2^m(t)$ – m-е фрагменты некоррелированных помех соответственно в первом и втором каналах приема, τ_m – взаимная задержка для m-го фрагмента, полагаемая при моделировании одинаковой для всех фрагментов.

Предположим также, что имеется N фрагментов и выполняются следующие операции. На первом этапе для каждого фрагмента получают m-ю оценку взаимного спектра

$$\dot{S}_{12}^m(\omega) = \dot{S}_1^m(\omega) S_2^{*m}(\omega),$$

где $\dot{S}_1^m(\omega) = FFT(S_1^m(t))$ - оценка текущего спектра, полученная с помощью БПФ, $S_2^{*m}(\omega)$ - взаимно сопряженный БПФ-спектр во втором канале.

На втором этапе совместная (полученная для N фрагментов) оценка взаимного спектра может формироваться различными способами. Традиционным является использование усреднения $\hat{\dot{S}}_{12}^{\Sigma}(\omega) = \sum_{m=1}^{N} \dot{S}_{12}^m(\omega)$, однако возможны и другие варианты. В частности, нами рассматривались две процедуры:

$$\hat{\dot{S}}_{12}^{\Sigma}(\omega) = \underset{N}{med}(Re(\hat{\dot{S}}_{12}^m(\omega))) + j \underset{N}{med}(Im(\hat{\dot{S}}_{12}^m(\omega))),$$

где med() означает расчет медианы выборки данных, а также

$$\hat{\dot{S}}_{12}^{\Sigma}(\omega) = \underset{N}{\alpha tr}(Re(\hat{\dot{S}}_{12}^m(\omega))) + j \underset{N}{\alpha tr}(Im(\hat{\dot{S}}_{12}^m(\omega))),$$

где αtr () означает расчет α-урезанного среднего (используемое значение параметра усечения было выбрано примерно равным 0,2, то есть отбрасывались примерно 20% наименьших и наибольших значений в отсортированной выборке данных).

Наконец, после получения $\hat{\dot{S}}_{12}^{\Sigma}(\omega)$ одним из рассмотренных выше способов, формируется итоговая оценка ВКФ $Y(\tau) = IFFT(\hat{\dot{S}}_{12}^{\Sigma}(\omega))$, где IFFT - обратное БПФ, и находится значение $\hat{\tau}$, соответствующее наибольшему значению $Y(\tau)$.

Предварительный анализ распределений значений $Re(\hat{\dot{S}}_{12}^m(\omega))$ и $Im(\hat{\dot{S}}_{12}^m(\omega))$ показал, что даже при гауссовых помехах в каналах приема, но малых отношениях сигнал-помеха эти случайные величины являются негауссовыми и характеризуются симметричностью относительно параметра сдвига и большей тяжестью хвостов, чем для гауссова распределения. Еще большая тяжесть хвостов имеет место, если помехи в каналах приема обладают большей импульсивностью, что имеет место для СаС процессов. Именно это свойство позволило предположить, что предложенные процедуры совместной робастной обработки элементарных оценок взаимного спектра могут быть более эффективными, чем обычное усреднение.

Сравнительный анализ проводился с использованием двух количественных критериев точности. В качестве первого критерия использовалось среднеквадратическое отклонение оценки взаимной задержки

$$\sigma_\tau = \sqrt{\frac{1}{N_{exp\,n} - 1} \sum_{k=1}^{N_{exp\,n}} \left(\hat{\tau}_k - \bar{\tau} \right)^2}, \qquad (1)$$

где N_{expn} – количество независимых статистических экспериментов, для которых наблюдались нормальные оценки (отличающиеся не более, чем на ширину главного лепестка автокорреляционной функции информационного шума, от истинного значения взаимной задержки); $\hat{\tau}_k$ - оценка взаимной задержки, полученная в k-м «нормальном» эксперименте; $\bar{\tau}$ – средняя оценка взаимной задержки по всем «нормальным» экспериментам.

Кроме того, вторым количественным критерием анализируемых методов обработки была вероятность появления аномальных оценок (аномальной оценка считается в том случае, если она существенно отличается от истинного значения)

$$P_{anom} = \frac{N_{anom}}{N_{exp}} \tag{2}$$

где N_{anom} – количество аномальных оценок, полученных во всех статистических экспериментах (их общее количество равно N_{exp}).

В результате исследований были получены зависимости $\sigma_\tau(\gamma)$ и $P_{anom}(\gamma)$, полученные при различных значениях α и N, представленные в виде графиков (напомним, что α и γ – это параметры СаС распределения, используемого в качестве модели шума). Параметр γ характеризует для СаС распределений интенсивность помех. Поскольку теоретически дисперсия для СаС распределений при $\alpha < 2$ бесконечна, то зависимости выбранных критериев являются функциями не от отношения сигнал-шум, а от значений γ (чем больше γ, тем выше интенсивность помех). При проведении исследований использовалось $N_{exp} = 300$, а значения N выбирались равными 5, 9, 15 и 25. Рассматривались значения γ в таких диапазонах их изменения, чтобы вероятность появления аномальных ошибок заметно отличалась от нуля. Естественно, что для метода обработки желательно, чтобы он обеспечивал как можно меньшие значения как среднеквадратического отклонения оценок взаимной задержки, так и вероятность появления аномальных оценок.

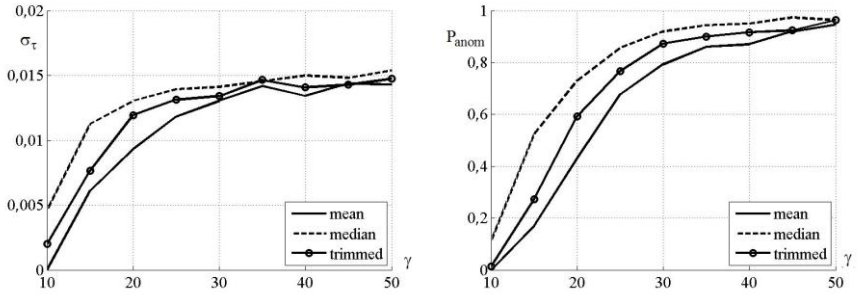


Рис. 1. Зависимости $\sigma_\tau(\gamma)$ и $P_{anom}(\gamma)$ для случая $\alpha = 2$, N=15

Информационный шумовой процесс моделировался с использованием НЧ-фильтрации гауссова белого шума таким образом, что его верхняя частота примерно в 5 раз меньше частоты дискретизации (которая в проводимых экспериментах была принята равной 20 кГц). Ввиду ограниченности объема публикации ниже приведены лишь некоторые из полученных зависимостей. Сразу же отметим, что при гауссовых помехах в каналах приема обычное усреднение (mean) оценок взаимных спектров является наиболее точным из рассматриваемых методов обработки. Об этом свидетельствуют графики, приведенные на рис. 1. Очевидно, что начиная с некоторого значения γ вероятность $P_{anom}(\gamma)$ приближается к единице, но для γ порядка 10…20 обычное усреднение взаимных спектров обеспечивает заметно более высокую точность, чем методы, основанные на устойчивых (робастных) оценках сдвига. При использовании медианной оценки имеет место наихудшая точность.

Однако по мере уменьшения значения α и увеличения γ ситуация изменяется. На рис. 2 представлены графики зависимостей $\sigma_{dt}(\gamma)$ и $P_{anom}(\gamma)$ для $\alpha = 1{,}8$. В этом случае

робастные оценки обеспечивают приблизительно одинаковую точность, которая существенно лучше, чем для обычного усреднения.

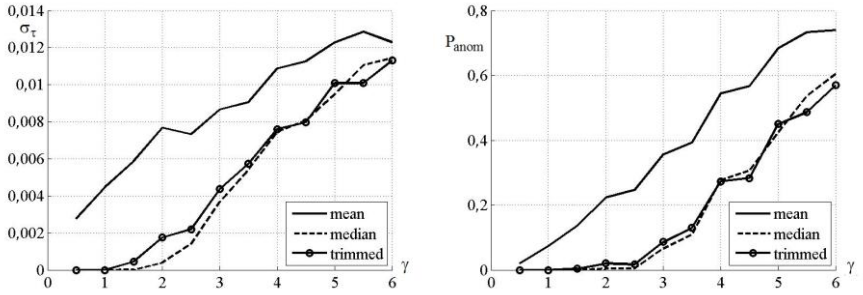


Рис. 2. Зависимости $\sigma_\tau(\gamma)$ и $P_{anom}(\gamma)$ для случая $\alpha = 1{,}8$, N=15

Наконец, на рисунке 3 представлены аналогичные зависимости для случая $\alpha = 1{,}6$, что хорошо аппроксимирует свойства акустических шумов в помещениях. В этом случае уже наиболее высокой точностью характеризуется метод совместной обработки взаимных спектров на основе медианной оценки.

Аналогичные зависимости и закономерности были получены и для других исследованных значений N. Это свидетельствует о целесообразности применения робастных оценок при взаимно-корреляционной обработке широкополосных сигналов при воздействии негауссовых помех в каналах приема. В дальнейшем планируется разработать методы адаптации робастных оценок к характеристикам таких помех для рассматриваемого приложения.

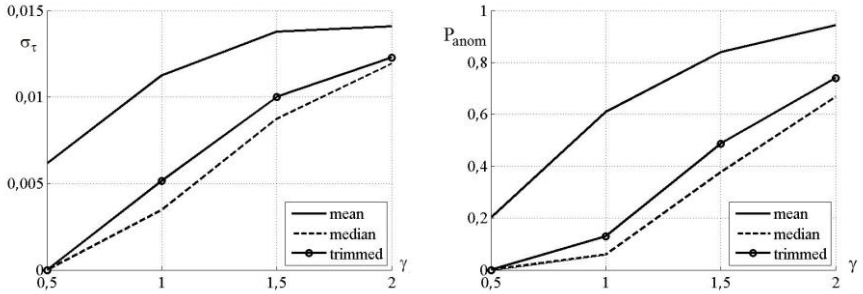


Рис. 3. Зависимости $\sigma_\tau(\gamma)$ и $P_{anom}(\gamma)$ для случая $\alpha = 1{,}6$, N=15

Литература:

1. M. Shao and C. L. Nikias, Signal processing with fractional lower order moments: stable processes and their applications," Proceedings of IEEE, vol. 81, No 7, pp. 986–1010, Jul. 1993.

2. Benesty J. / Time Delay Estimation via Minimum Entropy, IEEE Signal Processing Letters // Jacob Benesty, Yiteng Huang, Jingdong Chen. – March 2007. – Vol. 14, No 3. – pp. 157-160.

3. Champagne B. / Exact Maximum Likelihood Time Delay Estimation for Short Observation Intervals, IEEE Transactions on Signal Processing // B. Champagne, M. Eizenman, S. Pasupathy. – June 1991. – Vol. 39, No 6. – pp. 1245-1257.

4. J. P. Ianniello, Time delay estimation via cross-correlation in the presence of large estimation errors, IEEE Transactions on Acoustics., Speech, Signal Processing, Vol. ASSP-30, No 6, pp. 998–1003, Dec. 1982.

АНАЛИЗ УЯЗВИМОСТИ КРИПТОАЛГОРИТМОВ В ГРУППАХ КОС

Митяева И.А., Горбенко И.Д
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. Безопасности информационных технологий,
тел. (057) 702-14-25, E-mail: miaskad@gmail.com

In the last decade, a number of public key cryptosystems based on combinatorial group theoretic problems in braid groups have been proposed. These cryptosystems and some known attacks on them are represented in the given work.

Алгоритмы, основанные на преобразованиях в группах кос, являются одной из альтернативных ветвей криптографии. Криптосистема, основанная на косах – частный случай более общего подхода, впервые предложенного Аншелем, Аншелем и Гольфельдом. Позднее, на конференции CRYPTO'2000 была полностью описана идея создания данной криптосистемы. Ее ключевым моментом является задача эквивалентности. Существует алгоритм решения этой задачи за полиномиальное
время. Результатом его является каноническая форма n -косы, которая соответствует уникальной группе косы. Если мы преобразуем имеющееся произведение кос sps^{-1} в его каноническую форму, то нахождение исходных кос (множителей) будет иметь достаточно высокую сложность. Именно нахождение исходных кос является основной задачей криптоанализа рассматриваемых криптосистем.

Стойкость криптосистем с использованием кос-групп основывается на следующих проблемах:

1. Задача поиска сопряжений (CSP):

Пусть $(x,y) \in B_n \times B_n$ такие, что $y = a^{-1}xa$, где $a \in B_n$ или одной из подгрупп B_n. Задача – найти такое b, что $y = b^{-1}xb$.

2. Задача одновременного поиска множества сопряжений (MSCSP):

Пусть $(x_1,a^{-1}x_1a)\ldots(x_r,a^{-1}x_ra) \in B_n \times B_n$ такие, что $y = a^{-1}xa$, где $a \in B_n$ или одной из подгрупп B_n. Задача – найти такое b, что $y = b^{-1}x_1b = a^{-1}x_1a,\ldots, b^{-1}x_rb = a^{-1}x_ra$.

3. Задача декомпозиции (BDP):

Пусть $(x,y) \in B_n \times B_n$ такие, что $y = a_1xa_2$ для $(a_1,a_2) \in LB_n \times LB_n$. Задача – найти пару $(b_1,b_2) \in LB_n \times LB_n$ такую, что $y = b_1xb_2$.

4. Задача одновременной множественной декомпозиции (MSBDP):

Пусть $(x_1,a_1x_1a_2)\ldots(x_r,a_1x_ra_2) \in B_n \times B_n$ для $(a_1,a_2) \in LB_n \times LB_n$. Задача – найти пару $(b_1,b_2) \in LB_n \times LB_n$ такую, что $y = b_1x_1b_2 = a_1x_1a_2,\ldots, b_1x_rb_2 = a_1x_ra_2$.

5. Задача поиска корня (RP):

Пусть $x = a^p$, где a, $x \in B_n$ и $p \in N$. Задача поиска для экспоненты p – найти такую косу $b \in B_n$, чтобы $b^p = x$.

6. Задача выбора сопряженных элементов (CDP):

Пусть $(x,y) \in B_n \times B_n$. Задача – установить, являются ли x и y сопряженными, т.е. установить, существует ли такое $a \in B_n$ или одной из подгрупп B_n, что $y = a^{-1}xa$.

Исходя из вышеприведенного, рассмотрим три основные разновидности атак на криптосистемы, основанные на преобразованиях в группах кос:

1) использование решения задачи поиска сопряжений;

2) использование вероятностного подхода в B_n;

3) использование вспомогательной группы, как правило, в представлении Бурау[1].

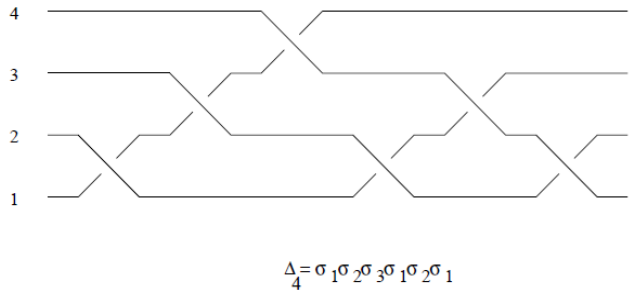
Решение задачи поиска сопряжений. Наиболее очевидный способ атаки на кос-криптосистемы – решение задачи поиска сопряжений в B_n, который стал известен благодаря основополагающей работе Гарсайда. Последующие уточнения метода значительно улучшили его алгоритмическую эффективность.

Метод Гарсайда для решения задачи поиска сопряжений в B_n состоит в привязке к каждой косе b характерного конечного набора сопряжений b, называемого высшим множеством. Эль-Рифай и Мортон предложили заменить высшее множество его подмножеством – супер высшим множеством(SSS). Супер высшее множество меньше, следовательно, его легче определить. Под SSS подразумевается множество всех сопряжений b минимально возможной запутанности. Для каждой косы b супер высшее множество конечно и алгоритмически вычислимо.

Две косы b и b’ сопряжены тогда и только тогда, когда их SSS. Таким образом, предполагаем разрешимость задачи поиска сопряжений в Bn. В действительности, известны и более точные результаты. Введем следующее определение: фундаментальная коса – $\Delta_n \in$ Bn, это коса, алгебраическая запись которой имеет вид:

$\Delta_n = (\sigma_1 \ldots \sigma_{n-1})\,(\sigma_1 \ldots \sigma_{n-2}) \ldots\ \sigma_1$

Геометрический пример приведен для косы Δ_4, где любые две нити пересекаются положительно, кроме одной (рис.1).



$\Delta_4 = \sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1$

Рис. 1. Фундаментальная коса для Δ_4

Предположим, что b – коса в B_n и (k; $b_1 \ldots, b_r$) – её нормальная форма. Если косы $\partial_+(b)$ и $\partial_-(b)$ определяются как

$$\partial_+(b) = \Delta_n^k b_2 \ldots b_r \varphi_n^k(b_1),\ \partial_-(b) = \Delta_n^k \varphi_n^k(b_r) b_1 \ldots b_{r-1}, \qquad (1)$$

где φ_n – флип-автоморфизм, отображающий σ_i в σ_{n-i} для каждого i; считается что $\partial_+(b)$(соответственно $\partial_-(b)$) получена циклированием (дециклированием) из b;

косы $\partial_+(b)$ и $\partial_-(b)$ – сопряжения b. Дело в том, что если b – коса в B_n, не принадлежащая супер высшему множеству b, т.е. не имеет минимальной запутанности в этом классе сопряжений, тогда циклированием или дециклированием максимум;

$n(n-1)/2$ раз можно найти сопряжение b точно меньшей запутанности. Таким образом, повторяя эти действия, после конечного числа шагов мы получим сопряжение b* для b, лежащее в супер высшем множестве b.

Приведем полную процедуру принятия решения о сопряженности кос b и b’, проиллюстрированную на рис.2:

1) Используя циклирование (cycling) и дециклирование (decycling), найти b* для b, лежащую в супер высшем множестве (SSS) b;
2) Используя циклирование и дециклирование, найти b’* для b’, лежащую в SSS(b’);
3) Определить SSS(b), насыщая {b*} простыми сопряжениями;
4) b и b’ будут сопряженными, если b’* принадлежит SSS(b).

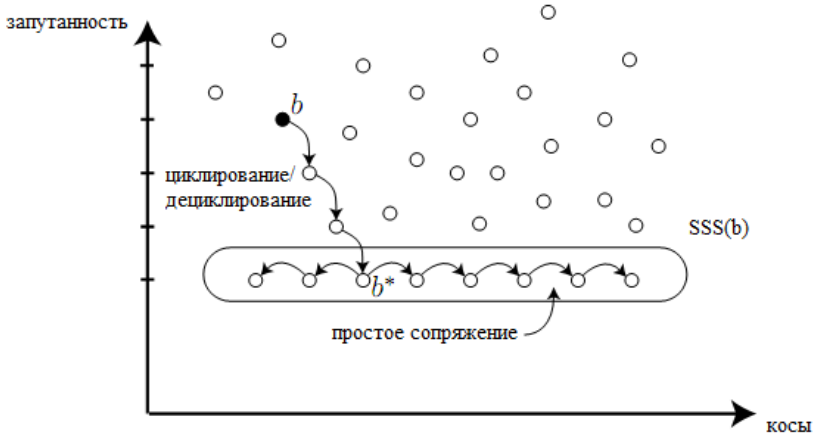


Рис. 3.Решение задачи сопряжения: определение SSS и его перечисление (точки показывают сопряжения b)

Отслеживая сопряжение кос на каждом шагу, можно не только определить, являются ли b и b’ сопряженными, но также получить сопряжение, если оно существует, т.е. если b и b’ сопряжены. Таким образом, решаются две задачи: задача сопряжения и задача поиска сопряжений в B_n[2].

Что касается сложности, так как циклирование и дециклирование постоянное количество раз гарантирует, что нормальная длина будет уменьшаться, если это возможно, нахождение сопряжения в SSS имеет линейную сложность по сравнению со сложностью для исходной косы. Потом остается только сложность перечисления SSS(b).

Совсем недавно В. Гебхардт предложил новое совершенствование. Это совершенствование состоит в замене SSS еще меньшим множеством, называемым ультра высшим множеством (USS). Рассмотрим действие циклирования на USS: начиная с косы b в ее SSS, не обязательно возвращаться к исходной b в циклировании SSS, но, безусловно, циклирование, в конечном счете, становится периодичным. Таким образом, можно разделить SSS на несколько орбит, состоящих из цикличных частей и остатков (рис.4).

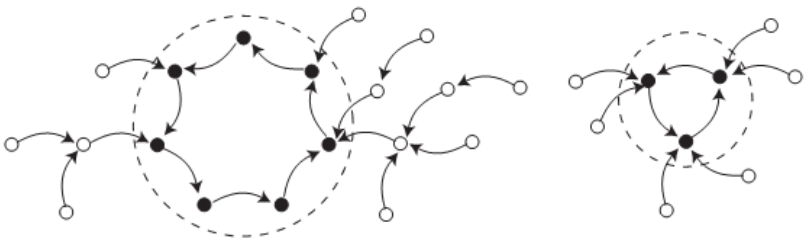


Рис. 4. Действие циклирования в SSS; черным показаны элементы USS

Гебхардт определяет ультра высшее множество как объединение цикличных частей орбиты. По определению USS является подмножеством SSS, и Гебхардт показывает, что USS может быть использовано вместо SSS: как и для SSS, элементы USS легко определить, а потом подсчитать и все USS, используя минимальные простые элементы. Дело в том, что размер USS обычно гораздо меньше SSS, типично его размер линеен относительно длины исходной косы, тогда как размер SSS экспоненциален. В таких случаях USS можно определить быстро и проблема сопряжения будет решена. На данный момент это не доказано, но сложность метода может быть сведена к полиномиальной.

Атаки, основанные на длине. Помимо использования конкретного решения задачи поиска сопряжений, также кос-криптосистемы можно атаковать, используя вероятностный эвристический подход: всякий раз, когда вероятность успеха более чем незначительна, этого может быть достаточно для того, чтоб поставить под угрозу кос-

криптосистему. Основанные на длине атаки относятся к этому семейству. Общий принцип таких атак состоит в попытке получить сопряжение для пары (p, p'), начиная с p', которая должна быть получена из p и многократно сопрягающаяся с p' в новую косу $tp't^{-1}$ так, что длина или запутанность $tp't^{-1}$ будет минимальной.

При осуществлении атаки проверяется, случается ли, что новое сопряжение $tp't^{-1}$ равно p. Атака особо применима к протоколам обмена ключами, основанным на задаче одновременного поиска множества сопряжений, потому что, в данном случае, злоумышленник знает несколько пар сопряженных кос, связанных с одной и той же сопряженной косой. Атака, описанная Хофхайнцем и Штайнвандтом, аналогична, но она включает в себя еще один шаг, и поэтому является более мощной. Вместо проверки, является ли $tp't^{-1}$ равным p, злоумышленник проверяет, чтобы «расстояние перестановки» между $tp't^{-1}$ и p не превышало 1, т.е. пытается найти такую перестановку *f*, что $tp't^{-1}$ равно простому сопряжению $\hat{f}p\hat{f}^{-1}$. Нахождение возможных перестановок является очень легким, так как оно сводится к решению задачи поиска сопряжений в симметричной группе S_n. При этом улучшении вероятность успешного осуществления атаки достигает 99% для протокола согласования ключей Аншеля-Аншеля-Гольдфельда в B_{80} при l = m = 20 и исходными косами p_i и q_j длины 5 или 10[3].

Атаки, основанные на линейных представлениях. Третий способ атаки кос-криптосистем – использование линейного представления кос-групп, т.е. отображение кос-групп в группы матриц. Так как задача сопряжения в линейной группе легка, так что можно думать о решении задачи сопряженности таким способом.

Наиболее известным представлением кос-групп B_n является представление Бурау, линейное представление со значениями $GL_n(Z[t,t^{-1}])$. Представление Бурау для B_n, как известно, неточно для $n \geq 5$, но ядро очень мало, потому вероятность того что различные косы примут один и тот же образ Бурау незначительна[3].

В заключение, можно сделать вывод, что важным фактором осуществления атаки является способ генерации ключей. Так, например, атака Гебхардта возможна лишь при достаточно малом USS, что не всегда соответствует действительности. Из вышеизложенного следует, что вычисление $p'= sps^{-1}$ с исходной косой p не является
лучшим способом генерации пары сопряженных кос. И это неудивительно, так как установление ряда ограничений на ключи – довольно распространенная ситуация, существует всего несколько криптосистем, где ключи могут быть выбраны в случайном порядке. Поэтому даже если некоторые авторы утверждают, что существующие атаки полностью нивелируют криптографию в группах кос, на данный момент, более разумным кажется заключить, что необходимо приложить больше усилий для построения доказуемо стойких крипоалгоритмов или же предоставлении доказательств того, что построение подобных криптоалгоритмов невозможно.

Литература:

1. D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, Length-based conjugacy search in the braid group, Contemp. Math. 418 (2006), 75–87.

2. J.S. Birman and T.E. Brendle, Braids: a survey, in: Handbook of knot theory, Elsevier, B.V., Amsterdam, 2005, pp. 19–103.

3. S.J. Lee & E.K. Lee, Potential weakness of the commutator key agreement protocol based on braid groups, Eurocrypt 2002, Springer Lect. Notes in Comput. Sci. 2332 (2002) 14–28.

ПЕРСПЕКТИВНЫЙ БЛОЧНЫЙ СИММЕТРИЧНЫЙ ШИФР, ОПТИМИЗИРОВАННЫЙ ДЛЯ АППАРАТНОЙ РЕАЛИЗАЦИИ

Олейников Р. В.[1], Киянчук Р. И.[2]
[1]ЗАО «Институт информационных технологий»
61166, г. Харьков, ул. Бакулина 12, E-mail: roliynykov@gmail.com
[2]Харьковский национальный университет радиоэлектроники
61166, г. Харьков, пр. Ленина 14,
каф. Безопасности информационных технологий, тел. (057) 702-14-25
E-mail: ruslan.kiyanchuk@gmail.com

Confidentiality of data transfer in modern information and telecommunication systems is usually provided by application of symmetric block ciphers. At the same time widely used block ciphers are generally designed for software implementation (AES) or special-purpose hardware modules (DES, TripleDES). Their system-on-a-chip implementations with strict constraints to the number of logic gates and energy consumption are quite ineffective. Consequently, such systems require a new generation cryptographic algorithms. Our paper examines requirements for symmetric block ciphers designed for lightweight hardware implementations, describes the perspective cipher specifications, its properties and comparison with already existing ciphers.

Массовая компьютеризация, активное использование электронных устройств в повседневной жизни и повсеместный доступ к Интернет открывают множество новых возможностей, но являются причиной возникновения значительных рисков, связанных с обработкой конфиденциальной информации. Финансовые приложения, беспроводные сенсорные сети, использование RFID-меток для учёта и в системах автоматического сбора пошлины требуют безопасной обработки и обмена данными с обеспечением целостности и конфиденциальности [3].

Большинство современных блочных симметричных шифров (БСШ) ориентированы на программную реализацию, а при аппаратной реализации требуют значительных ресурсов (количества вентилей, площади на кристалле, частоты процессора и энергопотребления) для получения приемлемого уровня производительности. Ограниченные ресурсы встраиваемых устройств не позволяют эффективно применять существующие надёжные шифры. По этой причине возникла потребность в разработке перспективных БСШ, ориентированных на эффективную аппаратную реализацию и гарантирующих приемлемый уровень безопасности данных [2]. Одной из последних разработок в данной области является шифр PRESENT, рассчитанный на аппаратную реализацию в устройствах с жёстко ограниченными ресурсами.

1 Описание шифра PRESENT

Основными требованиями к шифру PRESENT являются удовлетворительная безопасность, эффективность реализации и простота. Его возможно применять в условиях очень ограниченного аппаратного обеспечения, где использование существующих блочных симметричных шифров, таких как AES, невозможно.

1.1 Требования к перспективным блочным шифрам для аппаратной реализации

Разработчики PRESENT поставили перед шифром следующие требования [1]:

1. Шифр рассчитан на аппаратную реализацию.
2. Приложения требуют лишь удовлетворительный уровень безопасности.
3. Приложениям с малой степени вероятности понадобится шифрование больших объёмов данных. Реализация шифра может быть оптимизирована на компактность кода или производительность без ущерба стойкости и применимости.
4. В некоторых устройствах ключ шифрования фиксирован и встроен на этапе разработки. В таких устройствах нету необходимости в процедуре разворачивания ключа, следовательно, исключается множество атак на функцию выработки раундовых ключей.

5. Следом за безопасностью, основным ограничением служит размер аппаратной реализации шифра. Третьей важной метрикой является максимальное и среднее потребление энергии, а также требования к производительности.

6. В приложениях, требующих эффективного использования пространства на кристалле, блочный шифр часто необходим только в режиме шифрования, что сокращает накладные расходы на реализацию.

Криптоалгоритм PRESENT – блочный симметричный шифр с размером блока равным 64-м битам и размером ключа в 80 бит. Спецификация также описывает вариант с размером ключа в 128 бит. Аппаратная реализация PRESENT в режиме шифрования и расшифрования остаётся более компактной, чем AES только в режиме ифрования. Подключи могут вычисляться параллельно во время самой процедуры шифрования. PRESENT представляет собой SPN-структуру и состоит из 31 цикла. Последний, 32-й раундовый ключ используется для отбеливания после основной процедуры шифрования. Основной цикл состоит из линейного битового перемешивания и нелинейного слоя замены. Нелинейный слой использует 4-битовую подстановку, которая применяется 16 раз для всего блока в каждом цикле. Данные складываются с ключем по модулю 2.

1.2 Слой замен

В качестве нелинейного слоя используется одна 4-х битная подстановка $F_2^4 \to F_2^4$. Это прямое последствие жёстких требований к эффективности и компактности реализации. Симметричная 8-битная подстановка требует около 1000 вентильных эквивалентов (GE), столько же требует полная реализация шифра PRESENT [5]. Подстановка $F_2^6 \to F_2^4$ требует 128 GE, а подстановка $F_2^4 \to F_2^4$ – 21 - 39 GE. Для того, чтобы достигнуть лавинный эффект, на подстановку накладываются дополнительные ограничения. Обозначим коэффициент Фурье, как

$$S_b^W(a) = \sum_{x \in F_2^4} (-1)^{<b,S(x)>+<a,x>}. \quad (1)$$

Тогда подстановка PRESENT (табл. 1) удовлетворяет следующим условиям:

1. для любой фиксированной ненулевой входной разницы $\Delta_I \in F_2^4$ и любой фиксированной ненулевой выходной разницы $\Delta_O \in F_2^4$ требуется

$$\#\left\{x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\right\} \le 4; \quad (2)$$

2. для любой фиксированной ненулевой входной разницы $\Delta_I \in F_2^4$ и любой фиксированной выходной разности $\Delta_O \in F_2^4$ таких, что $wt(\Delta_I) = wt(\Delta_O) = 1$, имеем

$$x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta_O = 0; \quad (3)$$

3. для всех ненулевых $a \in F_2^4$ и всех ненулевых $b \in F_2^4$ выполняется $\left|S_b^W(a)\right| \le 8$;

4. для всех $a \in F_2^4$ и всех ненулевых $b \in F_2^4$ при $wt(a) = wt(b) = 1$ имеем $\left|S_b^W(a)\right| \le 4$.

Таблица 1: Подстановка PRESENT

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Из всего множества подстановок, удовлетворяющих условия, выбрана была та, аппаратная реализация которой требует наименьшее количество вентилей [1].

Максимальная вероятность выполнения дифференциальной характеристики для подстановки PRESENT равна 2^{-2}, следовательно для 25 циклов шифра данная вероятность будет составлять 2^{-100}. Максимальное отклонение линейной характеристики составляет $1/4$. Следовательно, вероятность выполнения линейного уравнения также равна $1/2 - 1/4 = 1/4$. При линейном криптоанализе для аппроксимирования 28 циклов

шифра, необходимо обладать 2^{84} парами сообщение/шифротекст, что превышает множество возможных входных блоков PRESENT.

1.3 Слой перемешивания

Главным аспектом при разработке слоя перемешивания было количество необходимых для реализации вентилей. Линейное битовое перемешивание не требует транзисторов в аппаратной реализации и хранения констант, поэтому может быть реализовано лишь разводкой контактов. К примеру, МДР-преобразование использующееся в AES-подобных шифрах при эффективной реализации требует хранение предварительно вычисленной таблицы степеней и таблицы логарифмов, а вычисление каждого элемента состоит из сложения и двух подстановок. Перемешивание PRESENT функционально можно описать с помощью формулы (4).

$$P(i) = \begin{cases} i \cdot 16 \bmod 63, & i \in 0, \ldots, 62 \\ 63, & i = 63. \end{cases} \quad (4)$$

1.4 Разворачивание ключей

Мастер-ключ хранится в регистре K и представлен последовательностью бит $k_{79}k_{78}\ldots k_0$. На каждом раунде подключём являются 64 старших (левых) бита регистра ключа. После выделения подключа, регистр обновляется по следующему закону:

1. $[k_{79}k_{78}k_1k_0] = [k_{18}k_{17}k_{20}k_{19}]$
2. $[K_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15} \oplus round\_counter]$

Стойкость шифра зависит от надёжности схемы разворачивания ключа. В алгоритме PRESENT счётчик циклов складывается по модулю 2 с битами регистра ключа для уменьшения зависимостей между раундовыми ключами. Для внесения нелинейности в формирование подключей при изменении состояния регистра ключа часть битов проходят замену по подстановке (табл. 1). К 21-му циклу все биты ключевого регистра являются нелинейной функцией от мастер-ключа, а после 21-го цикла каждый бит подключа зависит минимум от 4-х бит мастер-ключа.

1.5 Расшифрование

Для расшифрования криптограмм используются аналогичные преобразования, обратные оригинальным. Раундовые ключи подаются в шифр в том же порядке, что и при шифровании.

2 Характеристики аппаратной реализации шифра PRESENT

Авторы шифра рассматривали несколько целевых платформ для реализации: от интегральных схем ASIC и более гибких FPGA до чисто программных реализаций для 4-, 8-, 16- и 32-битных процессоров. Так как наиболее высокопроизводительной и миниатюрной является реализация ASIC, рассмотрим её подробнее. Результаты измерений статистики ASIC реализации шифра PRESENT по 180-нанометровому технологическому процессу с обработкой 4 бит за такт, представлена ниже.

Площадь: 1075 GE – требования к занимаемой площади измеряются в $нм^2$ и сильно зависят от технологического процесса и библиотеки стандартных ячеек. Для независимого сравнения требований принято указывать площадь в вентильных эквивалентах [GE]. Один вентильный эквивалент равен площади, занимаемой одним И-НЕ элементом с наименьшим номинальным током. Площадь в вентильных эквивалентах рассчитывается делением общей площади реализации на площадь И-НЕ элемента.

Производительность: 11.7 Kbps – скорость формирования нового результата относительно времени. Количество сформированных битов делится на затраченное время и представляется в битах за секунду [bps]. Эффективность: 10.89 $\frac{bps}{GE}$ – отношение площади реализации к производительности. Используется для измерения эффективности

аппаратного обеспечения. Измеряется в вентильных эквивалентах на бит в секунду $\left[\frac{GE}{bps}\right]$.

3 Сравнение PRESENT, ГОСТ 28147-89 и AES

Учитывая многолетний анализ и распространённость шифров AES и ГОСТ, актуально сравнение с ними нового шифра PRESENT. Сравнение шифров приведено в таблице 2. Следует отметить, что рассмотренная реализация PRESENT рассчитана на 4-битный процессор (обрабатывает 4 бита за такт), тогда как AES и ГОСТ не способны работать на 4-разрядных процессорах.

Таблица 2: Сравнение производительности PRESENT, AES и ГОСТ 28147-89

Шифр	Ключ, бит	Блок, бит	Производ., Кб/с	Площадь, GE	Эффектив., $\frac{bps}{GE}$
ГОСТ	256	64	14	800	17.5
AES	128	128	80	3100	25.81
PRESENT	64	80	11.7	1075	10.89

4 Выводы

Шифр PRESENT разрабатывался специально для аппаратной реализации и работы на устройствах с очень ограниченными ресурсами, таких как RFID-метки, где достаточно обеспечить удовлетворительный уровень безопасности для малых объёмов данных. Поэтому он неприменим для шифрования больших объёмов данных, требующих высокий уровень безопасности. Отсутствие сложных операций (умножение, модульное сложение) и таблиц предвычислений обеспечивают компактность аппаратной реализации, требование меньшей площади на кристалле, а следовательно – дешёвую себестоимость. Однако сравнение шифров PRESENT, AES и ГОСТ 28147-89 показало, что последний также хорошо показывает себя в сфере облегчённой криптографии и превосходит PRESENT по компактности реализации [4]. При модификации алгоритма ГОСТ, а именно замены восьми разных подстановок одной, аппаратная реализация будет занимать лишь 651 вентильных эквивалентов. К тому же в отличие от PRESENT, шифр ГОСТ 28147-89 испытан временем и хорошо проанализирован, существует множество его реализаций.

Учитывая подачу шифра ГОСТ на международный стандарт шифрования, актуальны дальнейшие исследования возможности применения шифра на устройствах с ограниченными ресурсами (энергопотребление, устойчивость к атакам по сторонним каналам). В свою очередь PRESENT может функционировать на 4-битных процессорах и является более гибким в реализации, что позволяет эффективно применять его на устройствах разной архитектуры.

Литература:

1. A. Bogdanov and C. Paar and A. Poschmann and others. PRESENT: An Ultra-Lightweight Block Cipher. *Proceedings of CHES 2007*. Springer-Verlag, 2007.

2. *A Survey of Lightweight-Cryptography Implementations*, 2007. Copublished by the IEEE CS and the IEEE CASS.

3. Axel Poschmann. Lightweight Cryptography From an Engineers Perspective. Technical report, Horst-Görtz Institut für IT Sicherheit, 2007.

4. Poschmann, Axel and Ling, San and Wang, Huaxiong. 256 bit standardized crypto for 650 GE: GOST revisited. *Proceedings of the 12th international conference on Cryptographic hardware and embedded systems* in CHES'10, pages 219--233, Berlin, Heidelberg, 2010. Springer-Verlag.

5. C. Rolfes and A. Poschmann and C. Paar. Security for 1000 Gate Equivalents. *ecrypt workshop SECSI - Secure Component and System Identification*. -, 2008.

КРИПТОАНАЛИЗ НА ОСНОВЕ АТАК ПО ПОБОЧНЫМ КАНАЛАМ

Олейников Р.В., Минаков А.Г.
АО "Институт информационных технологий"
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. безопасности информационных технологий
тел.(057) 702-14-25,
E-mail: ROliynykov@gmail.com, minakov13@gmail.com

This work describes the state situation in the area of side-channel attacks. It describes the various side channel known cryptanalysis methods available from the public literature. These attacks pose a serious threat to the security of cryptographic modules in the specific model with physical access o the attacking devic. In consequence, cryptographic implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered.

Информационно-телекоммуникационные системы активно применяются в современном мире, в том числе в критически важных системах. Информация, циркулирующая в них, нуждается в надёжной защите. При построении современных КСЗИ широко используются криптографические алгоритмы и протоколы, обладающие высоким уровнем стойкости к различным методам, основанным на математическом анализе свойств преобразований.

Тем не менее, для осуществления атак на криптографические примитивы было предложено использование так называемых побочных каналов, появляющихся в результате практической реализации математического алгоритма. Утечка данных через такие каналы чаще всего не предусматривается в классической модели безопасности протокола. Атаки по побочным каналам (Side Channel Attack) - это класс атак на криптосистему, которые, в отличие от теоретического криптоанализа, пытаются получить информацию о ключе или исходном тексте не на основании исследования описания криптографического алгоритма, а на основании данных, полученных в результате наблюдения за физическим процессом работы криптографического модуля, реализующего данный алгоритм.

Атаки по побочным каналам классифицируют по двум типам.

Инвазивные — неинвазивные. Инвазивные атаки требуют наличия прямого доступа к чипу или устройству. Типичным примером является подключение к шине данных для перехвата передаваемой информации. Неинвазивные атаки используют только информацию доступную извне: время работы устройства, потребляемая мощность, побочное электромагнитное излучение, звук работы системы. В некоторых источниках встречается термин полуинвазивные атаки. Эти атаки специфичны тем, что требуют наличия прямого доступа к поверхности чипа, но не требуют электрического контакта с металлической поверхностью.

Активные — пассивные. Активные атаки мешают должному функционированию оборудования (fault-injection attacks пытаются внести ошибки в вычисления). Пассивные атаки наблюдают за обработкой информации в устройстве, не нарушая его работу.

Перечень основных атак по побочным каналам и возможные методы защиты представлены ниже.

Probing attacks.

В данном типе атак для получения информации устройство вскрывается и исследуется каждый проводник, по которому передаются данные, или же с помощью электронного микроскопа исследуется состояние ячеек памяти. Эта задача может быть выполнена с использованием зондирующей станции, состоящей из микроскопа с микроманипуляторами.

Timing attacks.

Обычно, время работы программы рассматривается как параметр, который должен быть сокращён программистом. Однако известен факт, что время работы криптографического алгоритма также может являться информационным каналом для злоумышленника.

Время выполнения каждой логической операции может различаться в зависимости от входных данных (например, открытого текста или ключа). Это является следствием оптимизации производительности и других причин. При многократном измерении времени отклика системы на разные входные данные эта информация может оказаться исчерпывающей. Таким образом, атакующая сторона может произвести высокоточные измерения времени, за которое шифратор выполняет некоторые операции, и получить информацию о ключе (точнее, о его фрагментах).

В работе [1] приведена следующая классификация используемых в криптографических алгоритмах операций по степени их подверженности атакам по времени выполнения:

- не подвержены атакам по времени выполнения (т.е. выполняются за одинаковое число тактов на всех платформах): операции табличной замены, сдвига на фиксированное число битов, а также логические операции;
- в ряде случаев атаки по времени выполнения могут быть проведены против алгоритмов, в которых присутствуют операции модульного сложения или вычитания;
- наиболее проблемными с данной точки зрения являются операции умножения, деления, возведения в степень, а также сдвиги на переменное число битов.

Одним из наиболее показательных алгоритмов, против которых может быть проведена атака по времени выполнения, является алгоритм RC5. Среди других алгоритмов, подверженных данной атаке, в [2] упоминаются такие известные алгоритмы, как IDEA, Blowfish и DES.

В качестве противодействия атакам по времени выполнения предлагается следующее [2]:

1. обеспечить выполнение шифратором операций строго за одно и то же количество тактов процессора независимо от значений операндов, что сопряжено с техническими сложностями; кроме того, уменьшает быстродействие алгоритма, поскольку время выполнения операций в этом случае будет приведено к максимально возможному;
2. различным образом маскировать время выполнения операций: использовать случайные временные задержки, выполнять произвольные зашумляющие операции, внедрять в алгоритм различные случайные величины;
3. устранить условные переходы в реализации алгоритма.

Все это также приводит к уменьшению быстродействия алгоритма, поэтому наилучшим вариантом противодействия таким атакам является отсутствие в алгоритме шифрования операций, время выполнения которых зависит от обрабатываемых данных.

Power analysis attacks.

Как и время выполнения, энергопотребление криптографического устройства может предоставить дополнительную информацию о выполняемых операциях и входных параметрах. Суть данной атаки состоит в том, что в процессе работы шифратора злоумышленник с высокой точностью измеряет потребляемую мощность устройства. Современные лаборатории располагают оборудованием, способным производить измерения на исключительно высоких частотах (более 1 ГГц) и с высокой точностью (ошибка менее 1%).

Атаки по потребляемой мощности могут быть разделены на простые (Simple Power Analysis) и разностные (Differential Power Analysis). Простой анализ мощности представляет собой атаку по побочным каналам, которая включает в себя визуальный осмотр графиков текущего энергопотребления устройства. Изменение потребляемой мощности происходит в устройстве при выполнении различных математических операций. Цифровой осциллограф позволяет увидеть даже малые изменения в потребляемой мощности. Целью SPA является получение информации о конкретных выполняемых инструкциях в системе и о конкретных обрабатываемых данных. В общем случае SPA может дать как сведения о работе устройства, так и информацию о ключе. Для осуществления этой атаки криптоаналитик должен располагать точными данными о реализации устройства. Дифференциальный анализ мощности представляет собой атаку по побочным каналам, кото-

рая включает в себя статистический анализ потребляемой мощности. Эта атака применяется, если измерения содержат слишком много шума для простого анализа мощности. Более того, DPA зачастую не нуждается в данных о конкретной реализации и в качестве альтернативы использует статистические методы анализа. Дифференциальный анализ мощности – одно из самых мощных средств для проведения атак, использующих побочные каналы, причём эта атака требует сравнительно небольших затрат.

Основным методом борьбы с этим видом атак является балансировка потребляемой мощности. Следует добавить неиспользуемые (с точки зрения алгоритма) регистры и вентили, на которых выполняются бесполезные операции для того, чтобы сделать уровень потребляемой энергии постоянным значением. Такие методы, с помощью которых энергопотребление остаётся постоянным и не зависит от битов входа и ключа, предотвращают все виды атак по каналу энергопотребления.

Fault-injection attacks.

Суть рассматриваемой атаки заключается в осуществлении различного воздействия на криптографическое устройство с целью возникновения искажения информации на некоторых этапах шифрования. Это даёт возможность узнать входные параметры или некоторые части ключа. Наиболее распространённые методы воздействия:

- увеличение напряжения питания криптосистемы (выше максимально допустимого значения);
- изменение конструкции шифратора(нарушение электрических контактов);
- изменение тактовой частоты шифрующего устройства;
- помещение устройства в электромагнитное поле;
- повышение температуры некоторых частей криптографического устройства.

Подробный анализ может сравнивать данные на выходе до и после внесения изменений, таким образом, постепенно получая части ключа. Например, можно подобрать определённую интенсивность воздействия на алгоритм шифрования, чтобы происходила генерация одной ошибки за то время, которое тратится на шифрование одного блока. После каждого раунда шифрования находится секретный параметр, что в итоге приводит к полностью известному ключу.

Основные идеи этой методики были представлены в работе [3]. Предложенный подход был существенно развит в статье [4], где был описан дифференциальный анализ сбоев (differential fault analysis, DFA). Этот метод состоит в изучении результата работы алгоритма шифрования в нормальных условиях и при наличии сбоев при одном и том же входе (открытом тексте). Сбои обычно получаются созданием ошибки в процессе (кратковременная ошибка) или перед началом (постоянная ошибка) работы.

Противодействие атакам на основе сбоев. Не существует какой-либо универсальной защиты от воздействия на шифратор. Однако в [5] предлагается усложнение проведения атак на основе сбоев против аппаратного шифратора следующими способами:

- внедрение в шифратор детекторов различных воздействий (например, детекторов изменения напряжения, частоты питания и/или синхронизации, освещённости и т.д.), которые при обнаружении воздействия выполняли бы блокировку шифратора;
- различного рода пассивное экранирование шифратора, устранение которого приводило бы к выходу шифратора из строя;
- различные виды дублирования вычислений со сравнением результатов.

Для программных шифраторов также предлагаются методы защиты:

- использование контрольного суммирования фрагментов данных с периодической проверкой в процессе вычислений или различные контрольные вычисления;
- дублирование вычислений со сравнением результатов;
- внедрение в программу случайных избыточных вычислений.

Ясно, что подобные методы приводят к удорожанию шифратора и/или снижению его быстродействия, однако это необходимые методы при наличии у злоумышленника физического доступа к шифратору.

Electromagnetic analysis attacks.

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры. Катушка индуктивности помещается вблизи чипа, после чего измеряется электромагнитное поле. Возможно построение трёхмерных карт электромагнитного поля путём изменения положения катушки относительно чипа. Если добавить сюда изменение поля во времени, то получаем четырёхмерную модель. Анализ этих данных, как и в случае с изучением потребляемой мощности, может быть как простым, так и дифференциальным. Противодействием данному виду атак является надежное физическое экранирование или применение активных зашумляющих устройств.

Cache-based attacks.

В современных компьютерах для ускорения обработки информации при вычислениях используется кэш между процессором и оперативной памятью. Когда процессор обращается к информации, которая находится в оперативной памяти, то возникает задержка, так как необходимые данные должны быть загружены в кэш. Суть атаки заключается в анализе этих задержек и частоты появления кэша в вычислениях.

Таким образом, современные атаки по побочным каналам демонстрируют, что при наличии физического доступа к криптографическому устройству злоумышленник может значительно упростить криптоанализ. Известные методы защиты предполагают достаточно серьезное усложнение программной или аппаратной реализации, при этом не обеспечивая гарантий полной блокировки действий криптоаналитика. В дальнейших исследованиях целесообразно получить оценку верхней границы сложности и обоснование эффективности таких методов.

Литература:

1. Nechvatal J., Barker E., Dodson D., Dworkin M., Foti J., Roback E. Status report on the first round of the development of the advanced encryption standard // http://csrc.nist.gov — National Institute of Standards and Technology.
2. Kocher P. C. Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS, and Other Systems // http://citeseer.ist.psu.edu — 1999 — Cryptography Research, Inc., San Francisco, CA, USA.
3. Boneh D., DeMillo R. A., Lipton R. J. On the Importance of Checking Cryptografic Protocols for Faults // http://citeseer.ist.psu.edu — Bellcore, Morristown, NJ.
4. Biham E., Shamir A. Differential Fault Analysis of Secret Key Cryptosystems // http://citeseer.ist.psu.edu — Technion — Israel Institute of Technology, Haifa, Israel — 1997.
5. Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C. The Sorcer's Apprentice Guide to Fault // http://citeseer.ist.psu.edu.
6. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. - СПб.: БВХ-Петербург, 2009. - 576 с.: ил.
7. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ ПО ОТПЕЧАТКУ ПАЛЬЦА

Олешко И.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. БИТ, тел.(057) 702-16-25,
E-mail: InnaG88@gmail.com

These days fingerprint recognition is one of the most reliable and popular biometric recognition methods. In this paper we describe fingerprint recognition systems that consist of two main steps – fingerprint image preprocessing and feature matching by four different processes. The identification using co-occurrence matrix has reduced FAR and FRR than other processes. This method is simple, performs the comparison step quickly and has a good noise resistance.

На сегодняшний день биометрические технологии идентификации личности получили широкое распространение в различных областях обеспечения безопасности: от контроля и управления доступом в офисные помещения до гражданской идентификации правоохранительных приложений. С распространением таких технологий актуальной становится проблема выбора того или иного метода биометрической идентификации. Основным фактором, определяющим результаты выбора, является точность идентификации, которую можно оценить на основании ошибок первого (FRR – False Reject Rate, вероятность ложного отказа) и второго (FAR – False Acceptance Rate, вероятность ложной идентификации) рода. В настоящее время активно используются следующие биометрические признаки: отпечатки пальцев; геометрическая форма кисти руки; форма и размеры лица;

Особенности голоса; узор радужной оболочки и сетчатки глаз. Наибольшее распространение получила идентификация по отпечаткам пальцев. Основные достоинствами систем аутентификации по отпечатку пальца состоят в следующем: во-первых, отпечаток пальца уникален (за всю историю дактилоскопии не было обнаружено двух совпадающих отпечатков пальцев, принадлежащих разным лицам), а во-вторых, папиллярный узор не меняется на протяжении всей жизни человека.

Изображения отпечатков пальцев в электронно-цифровом виде формируются в результате сканирования дактилокарт с помощью планшетного сканера, ввода пальцев с «живого сканера», фотографирования цифровым фотоаппаратом следов пальцев с фотопленки и т.д. Изображения состоят из линий, обычно темного цвета, являющихся отображением папиллярных линий и имеющих разнообразную форму, между которыми на некотором расстоянии друг от друга расположены отверстия потовых канальцев.

Несмотря на многообразие строения папиллярных узоров, они поддаются четкой классификации, обеспечивающей процесс их индивидуализации и идентификации. Все папиллярные узоры делятся на три основных типа: дуговые, петлевые и завитковые, которые и составляют основу их классификации. Пример простого дугового, петлевого и завиткового узора приведены на рис. 1.

(a) (b) (c)

Рис. 1. Пример простого дугового (a), петлевого (b) и завиткового (c) папиллярного узора

В каждом отпечатке пальца можно определить два типа признаков: глобальные и локальные. Глобальные – это те признаки, которые можно увидеть невооруженным глазом: папиллярный узор, область изображения, ядро, пункт «дельта», тип линий, количество линий. Локальные признаки, или минуции, – уникальны для каждого отпечатка и определяют пункты изменения структуры папиллярных линии (окончание, раздвоение, разрыв и т.д.). Каждый отпечаток пальца содержит до 70 минуций. Практика показывает, что отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но совершенно невозможно наличие одинаковых множеств минуций. Идентификацию личности целесообразно осуществлять через локальные признаки. Основными локальными признаками являются окончание и разветвление линий.

Как правило, исходное изображение отпечатка (если оно не получено электронным способом), имеет плохое качество (повреждены линии, имеются разные искажения и т.д.). Для достоверного определения минуций необходимо обработать изображение и привести к особому виду (формату). Процесс обработки изображения осуществляется следующим образом: вычисление ориентации линий, улучшение качества линий, бинаризация изображения, утончение линий изображения.

Вычисление ориентации линий. Для вычисления ориентации линий выбираются точки (u,v)∈ I, рассматриваются окна $W(u,v,n)$, где n зависит от размерности матрицы, определяется вектор, перпендикулярный к прямой, которой принадлежит выбранная точка, и определяются суммы:

$$S_1 = \sum_{(i,j)\in W} g_1(u,v,i,j) \text{ и } S_2 = \sum_{(i,j)\in W} g_2(u,v,i,j),$$

где
$$g_1(u,v,i,j) = \begin{cases} 0, |I(u,v) - I(i,j)| < T \\ d(i,j)\cdot|I(u,v) - I(i,j)|, d_y(i,j) \ge 0 \\ -d(i,j)\cdot|I(u,v) - I(i,j)|, d_y(i,j) < 0 \end{cases},$$

$$g_2(u,v,i,j) = \begin{cases} 0, |I(u,v) - I(i,j)| < T \\ d(i,j)\cdot|I(u,v) - I(i,j)|, d_x(i,j) \ge 0 \\ -d(i,j)\cdot|I(u,v) - I(i,j)|, d_x(i,j) < 0 \end{cases}$$

где T – постоянная величина (на примере T=60), а вектор $d(i,j)$ был определен выше.

Используя эти формулы, для всех точек $(u,v)\in I$ определяется вектор $D(u,v)$:

$$D(u,v) = \begin{cases} \dfrac{S_1}{|S_1|}, |S_1| > |S_2|, \\ \dfrac{S_2}{|S_2|}, |S_2| > |S_1|. \end{cases}$$

Этот процесс повторяется 5 раз. После первого применения алгоритма некоторые векторы получаются нулевыми. При следующих применениях алгоритма качество изображения улучшается и, следовательно, количество нулевых векторов уменьшается.

Для уточнения направлений полученных векторов рассматриваются окна $W(u,v,n)$ для всех точек $(u,v)\in I$. Используя нулевой вектор $D(i,r)$, для всех векторов $D(i,j)$ определяется угол между векторами $D(i,r)$ и $D(i,j)$. Если этот угол тупой, то $D(i,r) = D(i,r) - D(i,j)$, в противном случае $D(i,r) = D(i,r) + D(i,j)$. Вычисляется

вектор $D(u,v) = D(i,r) / |D(i,r)|$ для всех точек окна $W(u,v,n)$. Этот процесс также повторяется 5 раз.

Улучшение качества линий. Используя векторы $D(u,v)$, и средний вес окон $W(u,v,n)$, можно улучшить качество линий, заменяя значения всех элементов матрицы на средний вес их окон. В качестве веса берется модуль sinα , где α – угол между векторами $D(u,v)$ и $d(i,j)$, $(i,j) \in W$. Средний вес окна считается по формуле:

$$I(u,v) = \frac{S(u,v)}{Q(u,v)},$$

где $$S(u,v) = \sum_{(i,j)\in W} I(i,j) \cdot |\sin\alpha|,\ Q(u,v) = \sum_{(i,j)\in W} |\sin\alpha|.$$

Этот процесс повторяется 5 раз (рис. 2-б).

Бинаризация изображения. Бинаризация изображения – это приведение изображения к черно-белому цвету. Процесс бинаризации начинается после вычисления направлений всех линий и улучшения качества изображений. Для всех элементов (u,v) матрицы I рассматриваются окна $W(u,v,n)$ и вычисляется средняя величина весов. Бинаризация изображения осуществляется по следующей формуле:

$$I(u,v) = \begin{cases} 255, \dfrac{S(u,v)}{Q(u,v)} \le 0 \\ 0, \dfrac{S(u,v)}{Q(u,v)} > 0 \end{cases}$$

где $$S(u,v) = \sum_{(i,j)\in W} (I(u,v) - I(i,j)) \cdot |\cos\alpha|,$$
$$Q(u,v) = \sum_{(i,j)\in W} |\cos\alpha|.$$

Здесь α – угол, образованный векторами $D(u,v)$ и $d(i,j)$, $(i,j) \in W$, $(u,v) \in$ I. Этот процесс повторяется 5 раз.

Утончение линий. Этап обработки изображений завершается утончением черных линий (шириной 1 или 2 пикселя). Для этого необходимо из черных линий убрать крайние точки. Рассматриваются окна $W(u,v,n)$ для всех точек (u,v) матрицы I, где n – такое число, при котором в окне не могут оказаться точки черного цвета из соседних линий. Далее считается сумма:

$$S(u,v) = \sum_{(i,j)\in W} I(i,j) \cdot \cos\alpha,$$

где α - угол, образованный векторами $D(u,v)$ и $d(i,j)$, $(i,j) \in W$, $(u,v) \in$ I. Элементы (u,v) матрицы I заменяются нулями (черный цвет заменяется на белый), если соответствующие суммы $S(u,v)$ больше заранее заданной величины T (на примере T=90). Этот процесс повторяется 4 раза (рис. 2-в).

а) б) в) г)

Рис.2. Этапы обработки изображения: а) – исходное изображение, б) – изображение после улучшения качества, в) – изображение после утончения линий, г) – изображение с минуциями

После процесса обработки изображение применяется конкретный метод аутентификации. Методы аутентификации по отпечатку пальца имеют дело не с реальными биометрическими образцами, а с цифровыми изображениями или их шаблонами. Решение о степени сходства двух дактилоскопических изображений (ДИ) A_1 и A_2 или их шаблонов $T_1 = f(A_1)$ и $T_2 = f(A_2)$ без потери общности лежит в диапазоне 0–1, где f — функция вычисления шаблона. Под шаблоном понимается математическая модель биометрического образца, например набор особенностей, представленных координатами и углом направления. Большинство алгоритмов оперирует с шаблонами T_1 и T_2, и только некоторые из них — непосредственно с серыми изображениями A_1 и A_2.

Известно, что сопоставление пары ДИ крайне сложная задача, главным образом из-за бесчисленного множества вариаций отпечатков одного и того же пальца. В целом все алгоритмы сопоставления ДИ или их шаблонов можно разбить на четыре большие группы:

- сопоставление изображений, основанное на различных модификациях корреляции многомерных сигналов;
- сопоставление шаблонов, основанное на характеристиках особенностей: координаты, угол направления, тип особенности (окончание и разветвление), вероятность наличия особенности, кривизна в окрестности особенности;
- сопоставление шаблонов, основанное как на характеристиках особенностей, так и на гребневом счете между особенностями;
- сопоставление шаблонов, основанное как на характеристиках особенностей, так и на топологических характеристиках особенностей.

В работе рассматриваются такие методы аутентификации по отпечатку пальца: на основании фильтра Габора, фильтра быстрого преобразования Фурье, с использованием момента Цернике, с помощью матрицы взаимного расположения. Основными показателями при оценке биометрических систем являются ошибки первого (FRR) и второго (FAR) рода. Результаты сравнений методов приведены в таблице 1.

Таблица 1. Сравнительный анализ методов аутентификации по отпечатку пальца

Метод	Фильтр Габора	Фильтр БПФ	Момент Цернике	Матрица взаимного расположения
FAR(%)	1,6	0,48	7,108	0,35
FRR(%)	18	12,5	7,151	0,21

Из таблицы можно сделать вывод о том, что наилучшим методом аутентификации по отпечатку пальца является метод на основе матриц взаимного расположения.

ОБЗОР КРИПТОГРАФИЧЕСКИХ СИСТЕМ В ГРУППАХ КОС

Паршина Д.А., Горбенко И.Д.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Безопасности Информационных Технологий,
тел. (057) 702-14-25, E-mail: dashaparshina@mail.ru

The past several years have seen an explosion of interest in the cryptographic applications of non-commutative braid groups in particular are especially desirable, as they provide difficult computational problems and can be implemented quite efficiently. Several different groups of researches have proposed numerous cryptographic protocols that make use of braid groups. This expository paper discusses the specifications and responses of both the M.Anshel,I.Anshel, and Goldfeld Commutator and the Co et al. Diffie-Hellman Conjugacy key exchange protocols.

На протяжении нескольких последних лет заметно вырос интерес к криптографическим приложениям, основанным на преобразованиях в некоммутативных группах. Группы кос в частности представляют особый интерес в силу своей эффективности при обеспечении трудоёмких вычислительных процессов. Различными группами исследователей были предложены протоколы с преобразованиями в группе кос. Данная работа посвящена описанию основных криптографических преобразований в кос-группах, обзору некоторых протоколов, использующих данные преобразования, а также рассмотрению самых распространённых вопросов в этой области[1].

Коса из n-ломаных нитей – объект который состоит из двух параллельных плоскостей P_0 и P_1 в трёх мерном пространстве R^3, который состоит из упорядоченног множества точек a1,a2,… an ϵ P0 , b1,b2,… bn ϵ P1 и из n – простых ломаных $l_1,l_2,\dots l_n$, которые не пересекаются между собой, пересекая каждую плоскость P_t между P_0 и P_1 и соединяют точки $\{a_i\}$ с точками $\{b_i\}$.

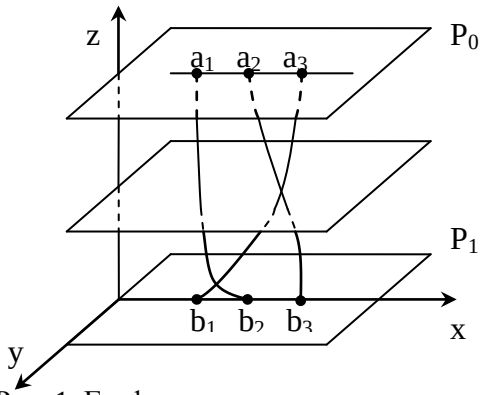


Рис. 1. Графическое представление косы

Косы из n-нитей, аналогично перестановкам владеют природной структурой групп. Пусть есть две косы A и B. Операция умножения кос определяется как: вертикальное сжимание и расположение одна над одной (рис. 2а). Нейтральным элементом в группе кос является коса с вертикально расположенными нитями (рис. 2б). Обратный элемент в группе кос задаётся вертикальным отображением (рис. 2в).

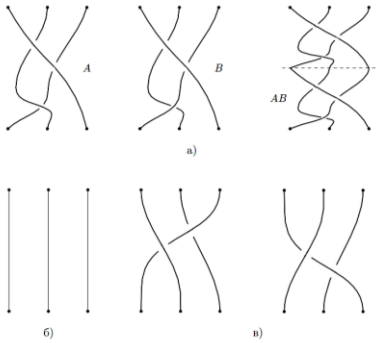


Рис. 2. Операции в группе кос: а)умножение б)нейтральный элемент в)обратный элемент

Фундаментальная коса - $\Delta_n \in B_n$, это коса алгебраическое представление которой имеет вид: $\Delta_n = (\sigma_1 \ldots \sigma_{n-1})(\sigma_1 \ldots \sigma_{n-2}) \ldots \sigma_1$, где σ_i – образующий элемент.

Основные соотношения в группе кос направлены на изменение формы записи, при этом не изменяя изоморфного класса косы.

Дальняя коммутативность – если существует два пересечения, которые находятся на большом расстоянии друг от друга по горизонтали, но близко по вертикали (не существует ни одного пересечения, которое находится выше одного из них, но ниже другого), порядок существующих элементов σ_i и σ_j изменится на σ_j и σ_i:

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \text{ при условии } |i-j| \geq 2 \quad (1)$$

Второе движение Рейдемейстра – пусть две нити косы находятся на близком расстоянии друг от друга и не пересекаются, тогда одну из этих нитей можно «накласть» на другую, то есть провести сверху другой, что можно описать соотношением:

$$\sigma_i^{-1}\sigma_i = \sigma_i\sigma_i^{-1} = e, \text{ где } e \text{ – нейтральный элемент.} \quad (2)$$

Третье движение Рейдемейстра – движение, которое в теории узлов описывается формулой:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \text{ при условии } 1 \leq i \leq n-2 \quad (3)$$

Если для некоторой косы существуют три точки попарных пересечений трёх разных нитей косы, которые находятся рядом, при этом одна из нитей проходит выше (ниже) других двух, тогда используя соотношение (3) можно протянуть над (под) двумя другими (рис. 3).

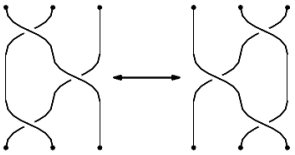


Рис. 3. Третье движение Рейдемейстра

Фундаментальной в теории кос является теорема Артина: группа кос B_n, изоморфна абстрактной группе, порождённой образующими $b_1, b_2, \ldots b_{n-1}$, которые удовлетворяют соотношениям (1), (2), (3). В алгебраическом виде это можно записать так:

$$\left\langle \sigma_1,\ldots,\sigma_{n-1} \middle| \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \text{для} \, |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{для} \, |i-j| = 1 \end{array} \right\rangle \quad (4)$$

Приступим к рассмотрению криптографических алгоритмов, базирующихся на группах кос, предварительно разбив их на четыре класса: системы обмена ключами, системы шифрования – расшифрования, системы аутентификации и системы подписи [2].

Среди ***систем обмена ключами*** выделяют две основных – это схема Аншеля-Аншеля –Гольдфельда и схема, аналогичная алгоритму Диффи-Хеллмана. Итак, в криптоалгоритме Аншеля-Аншеля-Гольдфельда в качестве открытого ключа принимается два набора кос $\{\{p1, \ldots, pn\}, \{q1, \ldots, qm\}\} \in Bn$. Секретный ключ U, принадлежащий A, состоит из l нитей и их инверсий. Аналогично секретный ключ V, принадлежащий B, состоит из m нитей и их инверсий. Обмен происходит следующим образом:

• A генерирует косу $s = u(p_1, \ldots, p_l)$, и использует её, чтобы сгенерировать сопряжённые $q_1' = sq_1s^{-1}, \ldots, q_m' = sq_ms^{-1}$; пересылает $q_1' \ldots q_m'$.

• B генерирует косу $r = v(q_1, \ldots, q_m)$, и использует её, чтобы сгенерировать сопряжённые $p_1' = rp_1r^{-1}, \ldots, p_m' = sq_ms^{-1}$; пересылает $p_1' \ldots q_l'$.

• A вычисляет $t_A = su(p_1, \ldots, p_l)^{-1}$.

• B вычисляет $t_B = v(q_1, \ldots, q_m)r^{-1}$.

• Искомый ключ $t_A = t_B$[3].

Далее рассмотрим протокол, предложенный К.Н. Ко, основой которого является протокол Диффи-Хеллмана. Здесь, открытый ключ p это определённая коса в группе B_n. Секретный ключ принадлежащий A представляет собой косу s из подгруппы L B_n, а секретный ключ B – косу r из подгруппы U B_n. Обмен ключами происходит таким образом:

• A генерирует сопряжение $p' = sps^{-1}$ и пересылает его B;

• B генерирует сопряжение $p'' = rpr^{-1}$ и пересылает его A;

• A вычисляет $t_A = sp''s^{-1}$;

• B вычисляет $t_B = rp'r^{-1}$;

Искомый ключ $t_A = t_B$.

Схема шифрования - расшифрования. Данная схема была предложена К.Н.Ко. Пусть есть группа кос B_n, и её подгруппа L B_n (соответственно U B_n), порождённая элементами $\sigma_1, \ldots, \sigma_{m-1}$ (соответственно $\sigma_{m+1}, \ldots, \sigma_{n-1}$) из m=n/2. Каждая коса из L B_n будет коммутативна каждой косе из U B_n. h – безколизийная однонаправленная хеш-функция. $(h(b_1) \neq h(b_2))$, $B_n \rightarrow \{0, 1\}^N$.

Алгоритм генерации ключевой пары:

Выбирается открытая коса p∈ Bn;

Выбирается персональный ключ s ∈ LBn;

• Вычисляется открытый ключ p` = sps^{-1};

• В качестве персонального ключа используется s, в качестве открытого ключа используется (p, p`).

Алгоритм зашифрования:

Вход: открытый ключ (p, p`), сообщение m из пространства $\{0, 1\}^N$, h – хеш- функция.

Выход: криптограмма e.

• Абонент выбирает случайную косу r из U B_n, и вычисляет $p'' = rpr^{-1}$

• Зашифровывает сообщение: $e = m \oplus h(rp'r^{-1})$

• В качестве криптограммы на выход подаётся (e, p″).

Алгоритм расшифрования:

Вход: персональный ключ s, криптограмма (e, p″), h – хеш- функция.

Выход: сообщение m.

• Абонент используя персональный ключ s вычисляет $m = e \oplus h(sp''s^{-1})$[4].

Системы аутентификации.. Как и в предыдущих системах, открытый ключ – это пара сопряжённых кос (p, p'), причём $p' = sps^{-1}$, принадлежащих группе B_n, сопряжённая коса s является секретным ключём A. В отличие от предыдущих систем и p и s принадлежат группе B_n, т.е мы не можем предположить, что s принадлежит какой-нибудь из подгрупп L B_n или же U B_n. Однако по прежнему предположим, что h-это односторонняя хэш-функция, в которой не происходит коллизий, заданная в группе B_n как $\{0,1\}^N$. Процедура аутентификация заключается в повторении *k* раз следующих трёх шагов:

• A выбирает случайную косу r, принадлежащую B_n и пересылает запрос $x = h(rp'r^{-1})$;

• B выбирает случайный бит c и пересылает его A;

• Для c=0, A пересылает $y=r$, и B проверяет $x = h(yp'y^{-1})$;

• Для c=1, A пересылает $y=rs$, и B проверяет $x= h(yp'y^{-1})$.

Электронная цифровая подпись. Две системы электронной подписи были предложны К.Н.Ко: применение второй схемы рекомендовано автором, однако на примере первой легче разобраться в самом алгоритме подписи, он является более наглядным и легко читаемым. Как и ранее открытый ключ представляет собой пару кос (p, p'), $p' = sps^{-1}$, принадлежащих группе B_n, а сопряжённая им коса s, принадлежащая B_n, является персональным ключом A. Будем использовать однонаправленную хэш-функцию H из {0,1}* в B_n.

На первом шаге выполняются следующие действия:

• A подписывает сообщение m при помощи $q' = sqs^{-1}$, где $q=H(m)$;

• B проверяет $q' \sim q$ и $p'q' \sim pq$.

Если A использует секретный ключ s, то получаем $q' = sqs^{-1}$ и $p'q' = spqs^{-1}$, то есть подпись принята. Возможная слабость данной системы может быть обусловлена тем, что возможно возникающие повторения могут раскрыть достаточно большое кол-во сопряжённых пар (q_i, q_i'), связанных с начальным сопряжением s, что делает возможным осуществление атаки на такую систему. Чтобы избежать этого, автор впоследствии несколько изменил общую схему путём включения дополнительных случайных кос.

Анализ рассмотренных криптографических систем показывает, что разработка алгоритмов, использующих группы кос является перспективным направлением в развитии современной криптографии[4]. Основные характеристики подобных систем приведены в таблице 1.

Таблица 1. Основные характеристики криптографических систем, базирующихся на группах кос

Входящее сообщение, бит	pnlog(n)
Зашифрованное сообщение, бит	4pnlog(n)
Скорость зашифрования, операций	$O(p^{2n}\log(n))$
Скорость расшифрования, операций	$O(p^{2n}\log(n))$
Длина персонального ключа, бит	0.5pnlog(n)
Длина открытого ключа, бит	3pnlog(n)
Сложность атаки «грубая сила»	$((n/2)!)^p = \exp(0.5pn\log(n))$

Литература:

1. D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, Length-based conjugacy search in the braid group, Contemp. Math. 418 (2006), 75–87.

2. E. Artin, Theory of Braids, Ann. of Math. 48 (1947) 101–126.

3. I. Anshel, M. Anshel, & D. Goldfeld, An algebraic method for public-key cryptography, Math.Research Letters 6 (1999) 287–291.

4. J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, J.H. Cheon, An efficient implementation of braid groups, AsiaCrypt 2001, Springer Lect. Notes in Comput. Sci., 2048 (2001) 144–156.

ОЦЕНКА ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С ПОНИЖЕННОЙ ЧАСТОТОЙ

Пашинцев В. П., Чипига А. Ф., Сенокосова А. В., Дагаев Э. Х.
Северо-Кавказский государственный технический университет
355000, Россия, Ставрополь, пр. Кулакова, кафедра защиты информации,
тел. (8652) 95-65-46, E-mail: zik@ncstu.ru

Assessment method for energetic concealment of satellite communication systems with lowered carrier frequency (up to $f_0 = 60\ldots70\,\text{MHz}$) and space diversity reception on some antennas with collocated intercept receiver is developed.

Условием обеспечения ПУ ССС является превышение энергетического отношения сигнал/шум (С/Ш) h^2 на входе приемника (ПРМ) над допустимым значением $h^2_{\text{доп}}$ (т. е. $h^2 \ge h^2_{\text{доп}}$). Величина $h^2_{\text{доп}}$ определяется по функциональной зависимости $P_{\text{ош}} = \Psi(h^2)$ вероятности ошибки от отношения С/Ш при допустимом для ССС значении $P_{\text{ош доп}} = 10^{-5}$.

Условием обеспечения энергетической скрытности ССС при решении системой несанкционированного доступа (разведки) задачи радиоперехвата является непревышение $h^2_{\text{р}} < h^2_{\text{доп р}}$ достижимого на входе ПРМ радиоперехвата энергетического отношения С/Ш $h^2_{\text{р}}$ над допустимым значением $h^2_{\text{доп р}}$, или обеспечение коэффициента энергетической скрытности $\gamma_{\text{эс}} = h^2_{\text{доп р}} \big/ h^2_{\text{р}} > 1$.

Очевидно, что при близком размещении ПРМ радиоперехвата от ПРМ ССС ($R_{\text{р}} < 10\,\text{км}$), когда $h^2_{\text{р}} = h^2$ и одинаковых характеристиках этих ПРМ выполнение условия обеспечения ПУ при минимальном отношении С/Ш $h^2 = h^2_{\text{доп}}$ сопровождается достижением равенства $h^2_{\text{р}} = h^2_{\text{доп р}}$ (или $\gamma_{\text{эс}} = 1$), а не условия обеспечения энергетической скрытности ССС $\gamma_{\text{эс}} = h^2_{\text{доп р}} / h^2_{\text{р}} > 1$.

Согласно [2, 3] выполнение условия $\gamma_{\text{эс}} > 30$ дБ возможно за счет использования в ССС пониженной несущей частоты (f_0 = 60…80 МГц) и пространственно-разнесенного приема на несколько ($n \ge 4$) антенн. Однако аналитическое выражение для $\gamma_{\text{эс}}$ в [2, 3] отсутствует.

Целью работы является разработка метода аналитической оценки коэффициента энергетической скрытности ССС ($\gamma_{\text{эс}}$), использующих пониженные частоты (f_0 = 60…70 МГц) и пространственно-разнесенный прием на несколько ($n \ge 4$) антенн при близком размещении приемника радиоперехвата от приемника связи.

Наиболее широко известными способами повышения энергетической скрытности систем связи (в том числе ССС) являются:

1) уменьшение мощности излучения передатчика (P_t);
2) применение широкополосных сигналов (ШПС) с большой базой ($B_s >> 1$);
3) улучшение направленности антенн передатчика и приемника.

Уменьшение мощности передатчика P_t ограничено таким ее значением, при котором условие $h^2 \ge h^2_{\text{доп}}$ сводится к равенству $h^2 = h^2_{\text{доп}}$. Поэтому достижение минималь-

ного значения $P_t \sim h^2 = \min$ возможно только в обмен на применение оптимальной схемы обработки сигналов в ПРМ (обеспечивающей $P_{\text{ош}} = P_{\text{ош доп}}$ при $h^2_{\text{доп}} = \min$).

Обеспечение энергетической скрытности ССС при решении задачи радиоперехвата (РПХ) не зависит от базы (B_s) сигнала (в отличие от решения традиционной задачи энергетического обнаружения сигналов).

Недостатком третьего способа является низкая эффективность при близком размещении ПРМ РПХ от ПРМ ССС (например, на расстоянии $R_{\text{р}} \le 10\,\text{км}$).

Анализ путей выполнения условия обеспечения энергетической скрытности ($\gamma_{\text{эс}} = h^2_{\text{доп}_{\text{р}}} / h^2_{\text{р}} > 1$) показал, что его можно реализовать только за счет вынуждения использовать в ПРМ РПХ менее эффективную по сравнению с ПРМ ССС схему обработки ($h^2_{\text{доп р}} > h^2_{\text{доп}}$). Однако это требует знания функциональных зависимостей:

$$P_{\text{ош}} = \Psi_i(h^2); \quad h^2_{\text{доп}} = \Psi_i^{-1}(P_{\text{ош доп}}); \qquad (1), (2)$$

$$P_{\text{ош р}} = \Psi_j(h^2_{\text{р}}); \quad h^2_{\text{доп р}} = \Psi_j^{-1}(P_{\text{ош доп р}}), \qquad (3), (4)$$

где функция Ψ и обратная ей Ψ^{-1} определяются типом математической модели радиоканала (принимаемого сигнала) и схемы обработки сигнала в приемнике.

Если требования к качеству различения сигналов в ПРМ РПХ такие же, как и в ПРМ ССС (т.е. $P_{\text{ош доп р}} = P_{\text{ош доп}} = 10^{-5}$), то при одинаковых моделях радиоканала и схемах обработки сигналов (т.е. одинаковых функциональных зависимостях $\Psi_i^{-1} = \Psi_j^{-1} = \Psi^{-1}$) выполняется равенство $h^2_{\text{доп}} = h^2_{\text{доп р}}$, а не условие $\gamma_{\text{эс}} > 1$. Если изменить тип модели радиоканала на более сложный (например, с многолучевостью и замираниями) и/или применить более сложную схему обработки сигналов в ПРМ ССС (например, разнесенного приема) по сравнению с используемой в ПРМ РПХ (например, одиночного приема), то изменятся функциональные зависимости $\Psi_i^{-1} \ne \Psi_j^{-1}$ и принципиально возможным станет выполнение неравенства: $h^2_{\text{доп}} < h^2_{\text{доп р}}$.

Более глубокий анализ возможности выполнения условия обеспечения энергетической скрытности показывает следующее [2, 3]. При использовании в ССС традиционного диапазона несущих частот $f_0 = 1...10\,\text{ГГц}$ канал связи описывается моделью с флуктуирующей фазой (т.е. без замираний). Если в ССС использовать пониженные частоты $f_0 = 30...100\,\text{МГц}$, то процесс распространения радиоволн (РРВ) будет сопровождаться рассеянием на неоднородностях ионосферы, многолучевостью и появлением быстрых замираний (БЗ) принимаемых сигналов. Для случая модели спутникового канала связи с БЗ райсовского типа и применения некогерентной (НК) схемы обработки ортогональных сигналов функциональная зависимость (Ψ_1) между $P_{\text{ош}}$ и h^2 существенно изменится по сравнению со случаем отсутствия БЗ $P_{\text{ош}} = 0{,}5\exp(-0{,}5h^2)$ при неизменном $h^2 = const$:

$$P_{\text{ош}} = \Psi_1(h^2) = \frac{\gamma^2 + 1}{h^2 + 2(\gamma^2 + 1)} \exp\left[-\frac{\gamma^2 h^2}{h^2 + 2(\gamma^2 + 1)}\right], \qquad (5)$$

где $\gamma^2 = a^2_{\text{р}} / a^2_{\text{фл}}$ - отношение мощностей регулярной ($a^2_{\text{р}}$) и флуктуационной ($a^2_{\text{фл}}$) составляющих замираний ($0 \le \gamma^2 \le \infty$).

При РРВ с пониженной частотой ($f_0 = 30...100\,\text{МГц}$) через ионосферу, в которой всегда присутствуют флуктуации (ΔN_i) электронной концепции (ЭК) $N_i = < N > + \Delta N_i$ относительно их среднего (фонового) значения ($< N >$), к ПРМ ССС приходит множество ($i = 1....M$) рассеянных неоднородностями (ΔN_i) лучей с относительными фазовыми сдвигами $\Delta\varphi_i \sim \Delta N_i / f_0$ [3, 5]. Значения $\Delta\varphi_i$ определяют условия возникновения БЗ райсового или рэлеевского типа: $0 < \Delta\varphi_i \sim \Delta N_i / f_0 << 2\pi$; $\Delta\varphi_i \sim \Delta N_i / f_0 >> 2\pi$, при которых $0 < \gamma^2 < \infty$ и $\gamma^2 = 0$ соответственно.

Зависимость между коэффициентом γ^2 и среднеквадратическим отклонением (СКО) фазовых сдвигов ($\Delta\varphi_i \sim \Delta N_i / f_0$) приходящих лучей $\sigma_\varphi = < \Delta\varphi_i^2 >^{0.5}$ при трансионосферном РРВ описывается выражением вида:

$$\gamma^2 = \frac{a_{\text{р}}^2}{a_{\text{фл}}^2} = \frac{1}{[\exp(\sigma_\varphi^2) - 1]}. \qquad (6)$$

Здесь

$$\sigma_\varphi \approx \sqrt[4]{\pi}\left(80{,}8\frac{\pi}{c}\right)\sqrt{l_s z_э \sec\alpha}\left(\frac{\sigma_{\Delta N}}{f_0}\right) \approx 1{,}6\cdot 10^{-2}\left(\frac{\sigma_{\Delta N}}{f_0}\right)\sqrt{\sec\alpha},\ (\text{рад}). \qquad (7)$$

где $c = 3\cdot 10^8$ м/с – скорость света; $l_s \approx 390$ м – характерный размер ионосферных неоднородностей; $z_э \approx 5\cdot 10^5$ м – эквивалентная толщина ионосферы; α - угол РРВ относительно вертикали; $\sigma_{\Delta N} = < \Delta N_i^2 >^{0.5}$ - СКО флуктуаций ЭК (ΔN_i) в неоднородностях ионосферы ($2\cdot 10^9 ... 4\cdot 10^9$ эл/м^3); f_0 - несущая частота (Гц).

Чтобы получить искомую зависимость (2) для случая БЗ райсовского типа $(0 < \gamma^2 < \infty)$, можно вместо формулы (5) воспользоваться аппроксимацией

$$P_{\text{ош}} = \Psi_1(h^2, \gamma^2) \approx (1 + \gamma^2)\exp(-\gamma^2)/h^2, \qquad (8)$$

справедливой при условии $h^2 >> 1 + \gamma^2$.

В соответствии с (8) при $0 < \gamma^2 < \infty$ и $h_{\text{доп}}^2 >> 1 + \gamma^2$ будем иметь

$$h_{\text{доп}}^2 = \Psi_1^{-1}(P_{\text{ош доп}}, \gamma^2) \approx (1 + \gamma^2)\exp(-\gamma^2)/P_{\text{ош доп}}. \qquad (9)$$

Если в ПРМ ССС вместо НК схемы обработки сигналов применить схему пространственно-разнесенного приема на несколько (n) антенн с НК объединением ветвей (квадратичным сложением), то произойдет существенное изменение по сравнению с (8) функциональной зависимости (Ψ) между $P_{\text{ош}}$ и h^2, определяемой при условии $h^2 >> 1 + \gamma^2$ как:

$$P_{\text{ош}} = \Psi_4(h^2, \gamma^2) \approx C_{2n-1}^n (1 + \gamma^2)^n \exp(-n\gamma^2)/(h^2)^n, \qquad (10)$$

где $C_{2n-1}^n = (2n-1)!/n!(n-1)!$, а входное отношение С/Ш $h^2 \sim G_r$ определяется так же, как при одиночном приеме.

Согласно (10) зависимость (2) $h_{\text{доп}}^2 = \Psi_4^{-1}(P_{\text{ош доп}}, \gamma^2)$ будет иметь вид

$$h_{\text{доп}}^2 = \Psi_4^{-1}(P_{\text{ош доп}}, \gamma^2) \approx \left[C_{2n-1}^n (1 + \gamma^2)^n \exp(-n\gamma^2)/P_{\text{ош доп}}\right]^{\frac{1}{n}}. \qquad (11)$$

В частном случае одиночного (n = 1) НК приема сигналов с БЗ райсового типа $(0 < \gamma^2 < \infty)$ выражения (10) и (11) сводятся к видам (8) и (9).

Отсюда следует, что применение в ССС пониженных частот $f_0 = 30...70$ МГц и одновременно пространственно-разнесенного приема на $n = 4$ антенны может рассматриваться как новый способ обеспечения очень высокой энергетической скрытности и помехозащищенности при близком размещении ($R_{\text{р}} \le 10$ км) ПРМ РПХ от ПРМ ССС.

Искомое аналитическое выражение для оценки коэффициента энергетической скрытности ($\gamma_{\text{эс}}$) ССС, использующих пониженные несущие частоты $f_0 = 60...70$ МГц и пространственно-разнесенный прием на несколько ($n \ge 4$) антенн, в условиях близкого размещения ПРМ РПХ можно получить на базе выражений (9) и (11), справедливых при условиях $h^2 >> 1 + \gamma^2$ и $\gamma^2 = 0...1{,}56$, в следующем виде:

$$\gamma_{\text{эс}} = \frac{h^2_{\text{допр}}}{h^2_{\text{р}}} \approx \frac{(1+\gamma^2)\exp(-\gamma^2)/P_{\text{ошдоп}}}{\left[C^n_{2n-1}(1+\gamma^2)^n \exp(-n\gamma^2)/P_{\text{ошдоп}}\right]^{\frac{1}{n}}} = \frac{\left(P_{\text{ошдоп}}\right)^{\frac{1-n}{n}}}{\left(C^n_{2n-1}\right)^{\frac{1}{n}}}. \qquad (12)$$

Согласно (12) при $n = 4$ и $P_{\text{ошдоп}} = 10^{-5}$ будем иметь значение $\gamma_{\text{эс}} = 33{,}5$ дБ, а при $n = 1$ величина $\gamma_{\text{эс}} = 1$. Очевидно, что в ПРМ РПХ (в отличие от ПРМ ССС) применение пространственно-разнесенного приема на $n \ge 4$ антенны проблематично, т.к. главным требованием к приемнику радиоперехвата, размещенному вблизи от ПРМ ССС, являются малые массогабаритные показатели.

Следует заметить, что в ССС более целесообразно использовать диапазон пониженных частот не 30...70 МГц, а $f_0 = 60...70$ МГц, т.к. на частотах ниже 60 МГц наблюдаются значительные [6] потери на поглощение в ионосфере ($L_T > 1$ дБ при $\alpha = 65^o$) и труднее выполнить условие обеспечения ПУ ($h^2 \sim 1/L_T = h^2_{\text{доп}n}$).

На основании изложенного выше можно сделать следующие выводы:

1). Применение в ССС пониженных несущих частот $f_0 = 60...70$ МГц (на которых процесс РРВ сопровождается рассеянием на неоднородностях ионосферы и замираниями сигналов на входах приемников) в совокупности с пространственно-разнесенным приемом на $n = 4$ антенны (рис. 2) позволяет обеспечить наряду с требуемой помехоустойчивостью ($h^2 = h^2_{\text{доп}n}$ =16,5…13,5 дБ) достижение очень высокой энергетической скрытности ($\gamma_{\text{эс}} = 33{,}5$ дБ).

2). Совокупность указанных мер можно рассматривать как новый способ повышения помехозащищенности ССС при близком размещении ПРМ радиоперехвата, в которых использовать пространственно-разнесенный прием нельзя из-за ограничений по массогабаритным показателям.

3). Для оценки коэффициента энергетической скрытности ($\gamma_{\text{эс}}$) ССС, использующих пониженные несущие частоты ($f_0 = 60...70$ МГц) и пространственно-разнесенный прием на несколько (n) антенн, при близком размещении ПРМ РПХ получено приближенное аналитическое выражение (12), справедливое при рэлеевских и глубоких райсовских БЗ ($\gamma^2 = 0...1{,}56$) и больших входных отношениях С/Ш ($h^2 >> 1 + \gamma^2$).

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ НА ОСНОВІ КІНЦЕВИХ АВТОМАТІВ У РАДІОЛІНІЇ ОБМІНУ ІНФОРМАЦІЄЮ З БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

Поздняков П. В.
Житомирський військовий інститут Національного авіаційного університету
10004, Житомир, проспект Миру 22, тел. (0412) 25-04-91
E-mail: pozdnjakovv@mail.ru

The realisation of cryptographic protocol on the basis of finite automata with delay is suggested. The application of linear and non linear automata enables to reach effective hardware representation of cryptosystem for traffic encryption in communication links with UAV. The practical secrecy of this system is based on complexity of finite automata inversion during satisfiable for attacker time. The streaming mode of encryption and short length key provide high productivity and enable to use finite automata in communication links with limited resources.

Основною тенденцією сучасних систем дистанційного моніторингу є використання невеликих за розміром, малопомітних, багатофункціональних безпілотних літальних апаратів (БПЛА). Ефективність функціонування таких систем значною мірою визначається якістю командного та інформаційного радіоканалів. Базові характеристики радіоканалу, включаючи надійність, якість та крипостійкість зв'язку між БПЛА та наземною системою управління і обробки сигналів, суттєво залежать від наявних обчислювальних ресурсів (продуктивності центрального процесора та спеціалізованих пристроїв) на БПЛА. Оскільки бортові засоби обробки та передачі інформації працюють в умовах багатьох обмежень (по продуктивності процесорів, точності, швидкодії обробки даних, обсягу пам'яті, а також при обмеженому часі обробки даних і наявності шумів у тракті передачі та потужних завад у каналах зв'язку), то актуальними є дослідження по розробці ефективних за швидкодією методів формування та передачі даних, які оптимізують обмін інформацією між наземною системою управління та БПЛА і вимагають незначних програмно-апаратних засобів.

Ефективне використання каналу зв'язку в значній мірі залежить від протоколів передачі, за допомогою яких реалізовується інформаційний обмін. Звичайний комунікаційний протокол у радіолінії обміну інформацією з БПЛА встановлює послідовність дій учасників при інформаційному обміні, забезпечує встановлення сеансу, визначення маршруту передачі, виявлення спотворень і відновлення спотвореної інформації. Криптографічний протокол, як правило, вбудовується в комунікаційний та реалізовується за допомогою окремих криптографічних модулів. Для практичного вирішення завдань захисту інформації в радіолінії обміну інформацією з БПЛА використовують прикладні криптографічні протоколи, які виконують функції криптографічної системи, їх реалізація в залежності від функцій-сервісів безпеки (конфіденційність, аутентифікація, цілісність, формування та передача ключів) є обмеженою по швидкості, технологічних можливостях та пропускній здатності радіоканалу, який є спільним ресурсом. Тому метою досліджень є визначення оптимальних за часом та за наявними в радіолінії обміну інформацією з БПЛА ресурсами криптографічних протоколів, які забезпечують необхідний рівень практичної стійкості з використанням нескладних програмно-апаратних засобів.

Серед відомих методів оперативного захисту інформації найбільш поширеним є використання потокових шифрів з одноразовим ключем, які вимагають генерацію довготривалих псевдовипадкових послідовностей на передавальній та приймальній стороні радіоканалу. Ключовим потоком для них служить, як правило, вихідна послідовність деякого автономного автомату, кількість внутрішніх станів якого співпадає з кількістю ключів шифру. Задамо математичну модель такого шифру. Нехай X і Y — певна кількість відкритих та закритих символів, з якими оперує деякий шифр заміни $|X|>1$, $|Y|>1$, $|Y|\geq|X|$. Це означає, що відкриті та зашифровані повідомлення подаються словами алфавітів X та Y відповідно. Процес зашифрування відкритого тексту $x=x_1..x_i$ полягає в

заміні кожного символу відкритого повідомлення x_i на деяке позначення закритого y_i, $i=\overline{1,l}$, відповідно до одного з n ($n>1$) ін'єктивних відображень $e_j : X \to Y$, що проіндексовані числами $j \in K = \{0,1,...,n-1\}$ та називаються простими замінами. Максимальне число n простих замін, складових такого шифру, не перевершує числа розміщень $A_{|Y|}^{|X|}$. Відображення визначається як $e_j(X) = \{e_j(x),\ x \in X\}$, $j=\overline{0,n-1}$. Через d_j позначимо відображення $e_j(X) \to X$, таке що $d_j(e_j(x)) = x$ для будь-якого $x \in X$. Тоді $Y = \bigcup\limits_{j \in K} e_j(X)$, а опорний шифр заміни можна представити п'ятіркою $\sum = (X, K, Y, E, D)$.

Практична реалізація шифру з одноразовим ключем заснована на тому, що основу наступних пакетів даних утворюють криптографічні інформаційні кадри, при формуванні яких використовуються інші послідовності бітів шифру. Слід зазначити, що хороший алгоритм криптозахисту інформації утворює шифровані дані з практично рівномірним розподілом q- бітових символів, де q – кількість біт символу. Величина ступеня захисту інформації пропорційна величині масиву даних, що підлягає шифруванню.

Створення таких алгоритмів захисту засноване на використанні ефективних генераторів псевдовипадкових чисел, які застовують для того, щоб одержати лінійні послідовності елементів гами, довжина яких перевищує розмір шифрованих даних. На основі теорії груп були розроблені декілька типів таких пристроїв. На сьогодні найефективнішими є конгруентні генератори псевдовипадкових чисел. Для цього класу генераторів розроблені математично строгі висновки, якими властивостями володіють вихідні сигнали цих генераторів з погляду періодичності та випадковості.

Якість шифру, побудованого на основі генератора псевдовипадкових чисел, визначається не тільки і не стільки характеристиками генератора, скільки алгоритмом одержання гами та безпосередньо процесом шифрування даних. Швидкодіючий метод захисту інформації з використанням шифру з одноразовим ключем ґрунтується на виконанні таких операцій: первинної операції гамiювання бітів інформаційного кадру з попередньо генерованими бітами комплексної довготривалої псевдовипадкової послідовності; операції визначення бітів коду перевірки (імітовставка) для гамійованого кадру, які служать для виявлення факту підміни інформації з боку атакуючої сторони; операції перемішування бітів імітовставки з бітами гамійованого інформаційного кадру; операції перемішування послідовності гамійованого інформаційного кадру з випадковим вибором номера вихідного (хаотичного) кадру, з яким здійснюється обмін біту (серії бітів) поточного гамійованого кадру. Для генерації довготривалих псевдовипадкових послідовностей використовується таблиця кодових ключів, які відповідають булевим послідовностям многочленів, що визначають генерацію первинних масивів псевдовипадкових послідовностей. З метою підвищення ступеня захисту інформації змінюються секретні коди на кожному циклі формування довготривалої псевдовипадкової послідовності. Для цього на завершальному етапі генерації довготривалої псевдовипадкової послідовності, на i-му циклі після використання останнього кодового ключа генерації первинної псевдовипадкової послідовності із кінцевого фрагмента довготривалої псевдовипадкової послідовності виділяються останні m-бітові випадкові послідовності (m – довжина секретного коду), які на $(i+1)$-му циклі використовуються як біти секретного коду.

Реалізація вищевказаного алгоритму в радіолінії обміну інформацією з БПЛА забезпечує високу швидкодію, однак необхідність передачі значних масивів з даними ставить під сумнів його практичну стійкість. Так як сучасні методи криптоаналізу з використанням набору статистики на тривалому проміжку дозволяють дешифрувати повідомлення практично в реальному масштабі часу. Крім того, зберігання таблиць з набором кодових ключів вимагає значних ресурсів пам'яті бортових засобів обробки, оскільки розмір системи булевих функцій може досягати неприйнятно великих розмірів, що неприпусти-

мо у випадку застосування БПЛА. Удосконалити криптографічний протокол можливо за рахунок динамічної зміни кодових ключів, передачу яких на борт можливо реалізувати використовуючи засоби асиметричної криптографії в радіолінії управління БПЛА.

Існує небагато асиметричних шифрів (RSA, El-Gamal, ECC), які використовують на практиці. Основним їх недоліком є низька швидкодія, тому питання синтезу стійкої асиметричної криптосистеми з невеликим розміром ключа й надалі залишається актуальним та потребує подальших досліджень. В останній час у світі проводяться інтенсивні дослідження в області побудови швидкісних асиметричних криптосистем з використанням теорії автоматів. Зокрема, в роботі Renji Tao розглядаються різні варіанти побудови асиметричної криптосистеми на основі кінцевих автоматів FAPKC (Finite Automata Public Key Cryptosystem).

Кінцевий (повністю визначений) автомат з множиною вхідних символів X, вихідних символів Y та станів S і з функціями переходів $\delta: S \times X \to S$ і виходів $\lambda: S \times X \to Y$ записується як $M = \langle X, S, Y, \delta, \lambda \rangle$. Принцип функціонування кінцевого автомату зображено на рис. 1. При шифруванні до відкритого тексту додається певна кількість символів τ. Шифртекстом є реакція автомату на розширене вхідне слово. Вихідний відкритий текст отримується як реакція автомату оберненого до автомата-кодера на вхідний шифртекст.

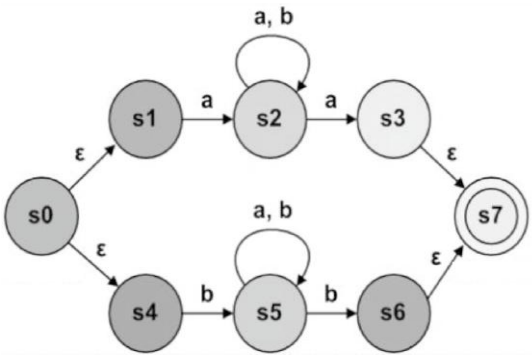


Рис. 1. Структура кінцевого автомату

Застосування кінцевих автоматів в криптографії припускає існування як мінімум пари кінцевих автоматів, один з яких виконує функцію кодера, а інший, інверсний кодеру, функцію декодера.

Для реалізації асиметричного криптоалгоритму у FAPKC закритий ключ утворюється з двох слабко оборотних автоматів, обернені до яких можуть бути легко (з поліноміальною складністю) побудовані, а відкритий ключ є послідовною композицією автоматів (один з яких обовязково нелінійний) в закритому ключі. Стійкість FAPKC заснована на складності вирішення задачі декомпозиції нелінійного оберненого з затримкою r автомата. Часова складність задачі безпосереднього інвертування композиційного автомату для вхідного слова довжиною k дорівнює $T(k) = \sum_{j=0}^{k-1} |S|^{k-j}$, де k - число тактів, що визначає затримку композиції автоматів, S - множина станів композиційного кінцевого автомата. Автомат зображений на рис. 2 є кінцевим автоматом з пам'яттю. Запропонована криптосистема може бути використана як для шифрування (відкритим ключем) і розшифрування(автоматом, зворотним до відкритого ключа), так і для підписання (цим автоматом) і для перевірки підпису (відкритим ключем).

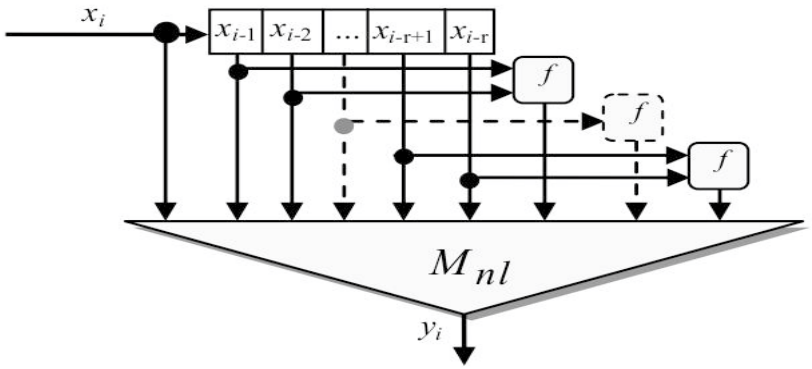


Рис. 2. Реалізація комбінованого автомату

Оскільки один з компонентів композиційного автомату є нелінійним, декомпозиція відкритого ключа з метою отримання його закритих компонент і побудова автомата, зворотного до відкритого ключа, з метою дешифрування і підписання без знання закритого ключа є важким завданням (експоненціальної складності). Отже, така криптосистема може як зашифрувати повідомлення, так і перевірити підписи, використовуючи відкритий ключ.

Проведений аналіз показав, що перевагами криптосистеми побудованої на основі кінцевих автоматів є:

1) Висока швидкодія, яка визначається часом переходу кінцевого автомата з одного стану в інший, та залежить від тактової затримки комбінації автоматів.
2) Проста перебудова кінцевого пристрою для реалізації наступного криптографічного алгоритму.
3) Проста реалізація у вигляді апаратного пристрою на базі програмованих логічних схем.
4) Реалізація алгоритмів на базі кінцевих автоматів передбачає тільки логічні операції та забезпечує коефіцієнт ефективності (відношення продуктивності до кількості використаних ресурсів) на порядок вищий ніж, наприклад у RSA.

Враховуючи високу інтенсивність інформаційного обміну в радіолінії, різнорідність трафіку та необхідність забезпечення заданого рівня практичної стійкості доцільно застосовувати композиції кіцевих лінійних та нелінійних автоматів у командному радіоканалі та реалізовувати симетричні методи потокового шифрування в інформаційному радіоканалі. Використання такого криптографічного протоколу дозволяє оптимально використовувати обмежені ресурси радіолінії зв’язку з БПЛА.

МОДЕЛЬ ТРАФИКА ETHERNET В ВИДЕ ON/OFF ПРОЦЕССА

Роздымаха Е.А., Омельченко А.В., Федоров А.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. сетей связи, тел. (057) 702-13-06,
E-mail: rozdy@mail.ru ; факс (057) 702-11-13

A model of fractal traffic based on the on/off model has been considered. A way to estimate mean queue length in a buffer of telecommunication equipment that is necessary to serve traffic properly has been suggested.

Введение

Исследования, проводимые в течение последних двух десятилетий, показали, что трафик данных в сетях с коммутацией пакетов, построенных согласно различных технологий, имеет ярко выраженную фрактальную природу [1]. Поэтому, для обеспечения требуемого качества обслуживания, соответствующее телекоммуникационное оборудование должно создаваться с учетом фрактальных свойств конкретного трафика. Для описания и моделирования фрактального трафика были предложены различные модели: на основе процессов авторегрессии дробно-проинтегрированного скользящего среднего (ARFIMA), на основе фрактального броуновского движения, on/off модели и другие. Важно отметить, что каждая из моделей наилучшим образом описывает только определенные виды фрактального трафика. Целью данной работы является анализ применимости модели on/off для описания трафика сетей Ethernet.

Математическая модель трафика Ethernet виде on/off процесса

On/off процесс может иметь два возможных состояния: on-интервалы, во время которых источник генерирует трафик фиксированного уровня, и off-интервалы, во время которых трафик не генерируется. Обычно on/off модели используют для моделирования трафика генерируемого одним источником. Общесетевой трафик может быть получен как суперпозиция трафика от нескольких источников. Пусть X_j и Y_j – длины j-го on и off периодов соответственно. В большинстве on/off моделей принято считать, что X_j и Y_j – независимо распределённые случайные величины. Для того чтобы сгенерированный с помощью on/off модели процесс был самоподобным, хотя бы одно из распределений интервалов (on или off) должно обладать тяжелым хвостом. Одним из таких распределений является распределение Парето, функция надежности которого для $x_m, k > 0$ имеет вид:

$$P(X > x) = \begin{cases} (\frac{x_m}{x})^k, & x \geq x_m, \\ 1, & x < x_m. \end{cases}$$

Степень самоподобия процесса обычно оценивают параметром Хёрста H. Для того, чтобы процесс являлся самоподобным параметр Хёрста должен лежать в пределах $\frac{1}{2} < H < 1$.

На рис. 1 представлены фрагменты реального Ethernet-трафика BC-pOct89 [3] и трафика, сгенерированного с помощью on/off модели. Спектры процессов, описывающих указанные два трафика, приведены на рис. 2. В сгенерированном on/off процессе on-интервалы распределены по закону Парето с параметрами $x_m = 1,\ k = 1{,}3$; а off-интервалы распределены согласно экспоненциальному закону с параметром 0,05.

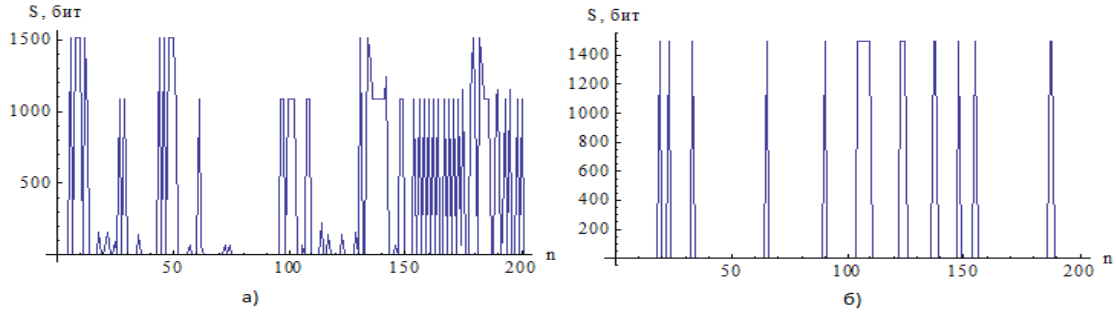


Рис. 1. а) фрагмент реального трафика, б) фрагмент трафика, сгенерированного с помощью on/off модели.

В работах [1, 4] показано, что для самоподобного трафика с параметром Хёрста H зависимость необходимого размера буфера q от среднего коэффициента использования ρ имеет вид:

$$q = \frac{\rho^{1/2(1-H)}}{(1-\rho)^{H/(1-H)}}. \qquad (1)$$

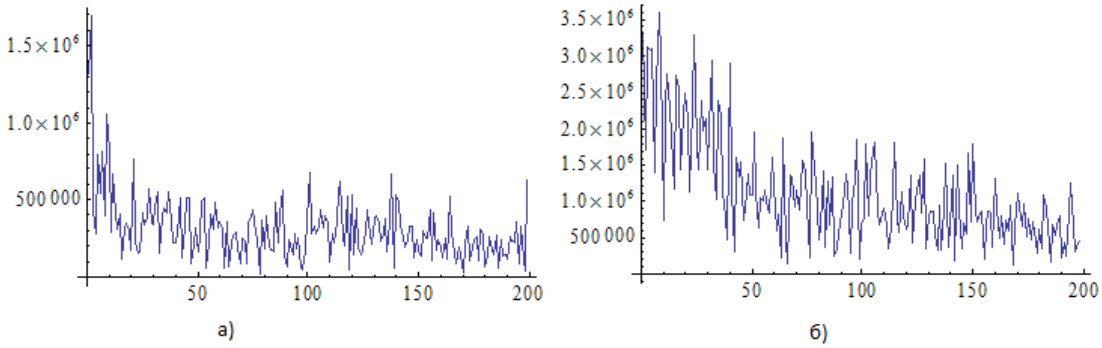


Рис. 2. а) спектр процесса, описывающего реальный трафик, б) спектр процесса, описывающего трафик, сгенерированный с помощью on/off модели.

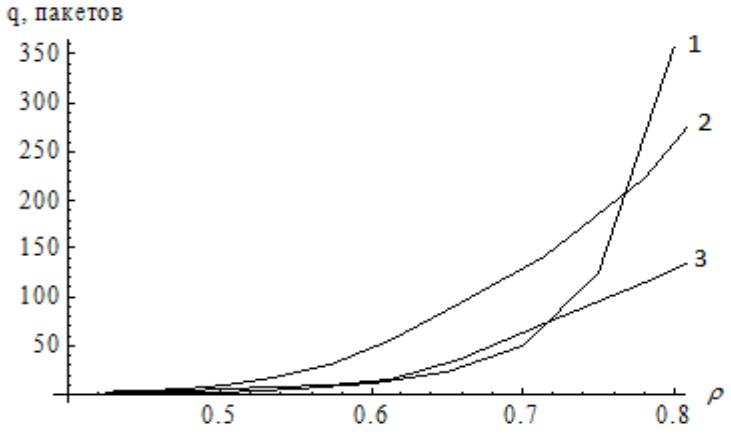


Рис. 3.Зависимость средней длины очереди в буфере от нагрузки: 1 – теоретическая зависимость (1),2 – сгенерированный трафик, 3 – реальный трафик.

На рис. 3 приведены графики зависимости средней длины буфера сетевого устройства от поступающей нагрузки. Для описания работы буфера использовалось следующее рекуррентное соотношение:

$$S_t = S_{t-1} + Z_t - r_t,$$

$$r_t = \begin{cases} c\Delta, & S_{t-1} \geq c\Delta, \\ S_{t-1}, & S_{t-1} < c\Delta, \end{cases}$$

где S_t – длина очереди в буфере, выраженная в битах, Z_t – входной трафик, c – пропускная способность канала, обслуживаемого буфером.

Выводы

В работе показано, что применение on/off модели позволяет генерировать самоподобные процессы, статистические свойства которых близки свойствам Ethernet-трафика. Такие модели позволяют вычислять требуемые характеристики телекоммуникационного оборудования, обслуживающего фрактальный трафик с заданной степенью самоподобия.

Литература:

1. Столлингс В. Современные компьютерные сети / Столлингс В. - СПб.: Питер, 2003. - 783 с.

2. Willinger W. Self-similarity and heavy tails: Structurel modeling of network traffic // A Practical Guide to Heavy Tails Statistical Techniques and Applications: articles / Willinger W., Paxson V., Taqqu M.S. - Birkhauser Boston Inc., 1998. – Vol. 23. – P. 27 – 53.

3. The Internet Traffic Archive [Ethernet traces of LAN and WAN traffic] URL: http://ita.ee.lbl.gov/html/contrib/BC.html (дата обращения: 12.05.2011).

4. Norros I. A Storage Model with Self-Similar Input / Norros I. // Queueing Systems. – 1994. – Vol. 16. – P. 387 – 396.

МОДЕЛЬ СТЕНДУ ДЛЯ ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ VOIP

Слюсар І.І., Уткін Ю.В., Янко А.С.
Полтавський національний технічний університет ім. Ю. Кондратюка
36000, Полтава, пр. Першотравневий, 24, кафедра комп'ютерної інженерії,
тел. (05322) 7-18-55,
E-mail: islyusar@inbox.ru

The given work is devoted the complex approach to research of properties and possibilities of technologies VoIP. It provides formation of independent, logically complete stages and is based on the open software. Technical aspects of its sharing with modern hardware in interests of studying of a spectrum of services and services VoIP are considered.

Розвиток internet-технологій призводить до постійного розширення номенклатури послуг і сервісів для абонентів, що передбачає розробку сучасних корпоративних рішень, в тому числі оперативного розгортання Call-центрів, віртуальних офісних і т .ін. Дана тенденція також спостерігається в сфери поширення VoIP.

Як наслідок, для реалізації зазначених технологій IT-фахівці повинні мати відповідну кваліфікацію та досвід. Тому, досить актуальною є задача розробки інструментарія для дослідження властивостей та можливостей технологій IP-телефонії в інтересах підготовки сучасних спеціалістів за напрямком «Телекомунікації».

В якості рішення зазначеної проблематики пропонується впровадження у навчальний процес лабораторного практикуму на базі стенду з відповідними програмними, апаратними засобами та системами.

Метою його створення є комплексний підхід щодо формування фундаментальних знань технологій VoIP, а також варіантів їх практичної реалізації. При цьому, лабораторний практикум повинен забезпечувати можливість дистанційного навчання та відповідати мінімуму витрат на його розгортання та підтримку. В роботі пропонується модель стенду для дослідження технологій VoIP, яка містить програмні та апаратні засоби, що вирішують вказані задачі, а також має модульну структуру.

Під час вибору програмного забезпечення враховувались наступні вимоги. Воно повинно бути відкритим і мати статус FreeWare. Через домінування кількості робочих станцій на базі ОС Windows, впровадженню підлягає тільки сумісне забезпечення з зазначеною ОС. Можливість подальшого вдосконалення та масштабування без прив'язки до конкретних апаратних засобів і мережних вузлів. Наявність автономного режиму роботи без підключення до зовнішніх ресурсів Internet, а також реалізація автоматизованого робочого місця на базі віртуальної машини. Спільна робота з сучасними та перспективними апаратними засобами. Надання найбільш поширених послуг і сервісів на основі VoIP, в тому числі аудіо- відоеконфренцзв'язку, автосекретаря, переадресації, планування трафіку, режимів роботи згідно з регламентом співробітників підприємства, можливістю входу/виходу з/на провайдерів GSM і CDMA.

Для дослідження всього спектру послуг і можливостей технологій VoIP, за думкою авторів, апаратна частина повинна передбачати можливості: спільної роботи з персональним комп'ютером; незалежної від нього роботи в мережах LAN, корпоративній або міської телефонній мережі загального користування, а також оперативного їх розгортання на базі мережі електроживлення підприємства; моделювання ділянок (сегментів) транспортної мережі та мереж доступу на базі технологій волоконної оптики або xDSL.

Концепція створення стенду для лабораторного практикуму передбачає наявність умовного розподілу на кілька етапів навчання та дослідження сервісів і послуг технологій VoIP. Вони є логічно завершеними та незалежними між собою, що дозволяє певною мірою здійснювати диференційний підхід щодо навчального процесу, а також оптимального використання навчально-матеріальної базі. Для тих хто навчається, кожен з етапів передбачає отримання конкретних навичок і умінь в питаннях практичної реалізації технологій VoIP.

Перший етап передбачає отримання навичок в проектуванні окремих елементів ко-

рпоративної мережі IP-телефонії, дослідження сутності зазначених технологій, можливості та властивості програмних продуктів для їх реалізації. З цією метою застосовувалась програмна IP-АТС 3CX Phone System (Free Edition), яка може повністю замінити аналогові міні-АТС, підтримує стандартні програмні та апаратні SIP-телефони, послуги VoIP і традиційні телефонні лінії загального користування, а також програмне забезпечення NetSpeakerphone. В рамках зазначено етапу досліджень передбачені розгортання та програмування конфігурації IP-АТС 3CX Phone System, реалізація спільної роботи з віртуальними машинами, софтфонами (наприклад: 3CXPhone, Sippoint, NetSpeakerphone, X-Lite і т. ін.) без залучення зовнішніх internet-ресурсів, формування політик надання послуг і доступів до окремих сервісів внутрішнім абонентам, імітація територіально рознесених сегментів корпоративної мережі IP-телефонії. Відповідно, все це передбачає наявність LAN.

Другий етап спрямований на отримання навичок і умінь в роботі з апаратними засобами. В якості базових були обрані IP-телефони типу Grandstream GXV 3000 (підтримує відеоконференцзв'язок, вибір протоколу, має вбудований web-браузер і . ін.), USB-телефони типу Skypemate USB-P4K (підтримує роботу зі Skype і SIP), VoIP-шлюзи (виробництва D-Link). При цьому досліджуються можливості спільної роботи з зовнішніми internet-ресурсами VoIP (наприклад: http://www.skype.com, http://www.oovoo.com, http://www.sip.net.ru) і вказаними вище софтфонами. До моделювання транспортного середовища залучаються гнучкі мультиплексори МП-30Е (виробництва ЧеЗаРа, м.Чернігов), які забезпечують потоки Е1 та мають на канальному боці – обладнання LAN (блок ЦК-05(К)), а на лінійному – модеми для роботи по оптичному волокну або за технологією SHDSL (відповідно ОЛО-01 (ОЛО.07-01) або ВС-01(К)).

Третій етап присвячений існуючим протоколам (G.711, G.723x, G.729x, SIP, H.263, H.264) для реалізації IP-телефонії. При цьому, досліджуються їх властивості та вплив на якість надання послуг і сервісів, формуються навички у виборі більш оптимальних з них для конкретних додатків і ситуацій. Також розглядається спільне використання програмних і апаратних засобів для надання послуг VoIP, одночасна робота внутрішніх абонентів з зовнішніми ресурсами, організація транків, узгодження з апаратними АТС, сценаріїв обслуговування абонентів, переадресації, реалізація різних варіантів конференцзв'язку на існуючій матеріальній базі і т. ін.

Четвертий етап передбачає дослідження впливу транспортного середовища на якість IP-телефонії. Для цього використовуються оптичні атенюатори (у разі роботи МП-30Е по оптичному волокну) або штучні лінії (при роботі модемами SHDSL). Одночасно визначається за допомогою аналізатор у потоку Е1 зі складу МП-30Е взаємозв'язок коефіцієнта помилок і якістю надання послуг і сервісів VoIP. Додатково може застосовуватись комплект із 2-ох PLC Ethernet-адаптерів 85Mbps IEEE 802.3/ 802.3U для організації LAN за допомогою мережі електроживлення.

Таким чином, розглянута модель стенду дозволяє реалізувати комплексне та всебічне дослідження технологій VoIP. Практична значимість запропонованого підходу полягає в тому, що частина елементів моделі може бути безпосередньо використана для відпрацювання окремих мережних і офісних рішень. Наприклад, вона була вдало апробована в якості сегменту віртуального офісу на обласні міжвузівській виставці «Освіта-2011» (м. Полтава, березень 2011року.). Крім того, її відкритість і модульність дозволяє проводити без ускладнень нарощування апаратної бази стенду, конфігурацію програмних засобів.

Подальші перспективні дослідження спрямовані на практичну реалізацію запропонованої моделі спільно з технологіями VPN і MPLS.

УЛУЧШЕНИЕ СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ БИТ

Торба А.А., Бобкова А.А.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. ЭВМ, тел. (057) 702-13-54,
E-mail: august@kture.kharkov.ua

Were carried out theoretical research of mathematical algorithms cryptographic hash function SHA-1. It is shown that the output bit sequence are much smaller dislocation and lower correlation than the input bit variables.

Введение

В международном стандарте ISO/IEC 18031:2005 приведен пример недетерминированного генератора случайных бит (НГСБ) с шумовым диодом (рис. 1). В этом генераторе внутреннее состояние – это 160-битовый регистр, в который записывается текущее значение криптографической Хеш-функции SHA-1 и случайное число от источника энтропии – шумового диода.

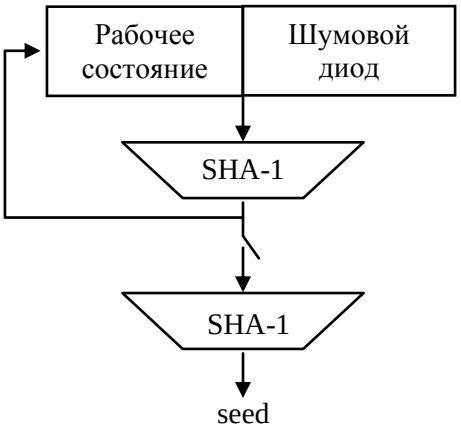


Рис. 1. Пример НГСБ для формирования бит с использованием физического датчика

Функция перехода внутреннего состояния – SHA-1 стандартная Хеш-функция текущего рабочего состояния и дополнительных выходных данных источника энтропии.

Функция генерации выходных данных – Хеш-функция SHA-1 рабочего состояния, которая генерирует 160-ти битовые выходные данные.

К источнику энтропии на основе шумового диода не выдвигаются требования несмещенности выходных бит (т.е. равенства вероятностей нулевых и единичных бит), а также требование независимости (некоррелированности) бит на выходе источника энтропии.

Выходные случайные биты НГСБ (seed) должны быть несмещенными и некоррелированными.

Как указано в стандарте ISO/IEC 18031:2005: «алгоритм безопасного Хеширования SHA-1 на практике позволяет выровнять вероятности выходных бит, если входные биты смещенные или коррелированны (**хотя это и не доказуемо**)».

Целью статьи является показать доказуемость этих практических результатов.

Основные математические преобразования Хеш-функций

Функция хеширования (Хеш-функция) представляет собой отображение, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины H(M). Основные математические преобразования известных алгоритмов хеширования можно показать на примере алгоритма безопасного хеширования SHA-1 (Secure Hash Algorithm), принятого в качестве стандарта США в 1992 г. и предназначенного для использования совместно с алгоритмом цифровой подписи.

Исходное сообщение M дополняется битами так, чтобы его длина стала кратной 512 битам. Далее математический алгоритм обрабатывает блоки по 512 бит основными логическими функциями:

- циклический сдвиг;
- суммирование по модулю, кратному длине блока;

- побитовая функция: XOR – суммирование по модулю 2;
- побитовая функция: $F1 = X \,\&\, Y \vee \overline{X} \,\&\, Z$;
- побитовая функция: $F2 = X \oplus Y \oplus Z$;
- побитовая функция: $F3 = X \,\&\, Y \vee X \,\&\, Z \vee Y \,\&\, Z$ и др.

В статье [1] с использованием вероятностной модели показано, что побитовая функция XOR над независимыми битами уменьшает разность вероятностей «логических нулей» и «логических единиц» (смещение случайных битов) в соответствии с алгоритмом «Дельта-квадрат». В статье [2] доказано, что многократное использование операции XOR значительно уменьшает смещение в соответствии с показательной функцией:

$$\Delta = P(0) - P(1) = \delta^n, \qquad (1)$$

где Δ – разность вероятностей случайных битов на выходе элемента XOR;
δ – разность вероятностей случайных битов на входах элемента XOR;
n – количество объединяемых независимых случайных битовых потоков.

В таблице 1 приведены состояния входных битовых переменных X, Y, Z, а также вероятности каждой комбинации входных битовых переменных и выходные функций F1, F2 и F3 для алгоритма SHA-1. Вероятность «логического нуля» входной битовой переменной X в этой таблице обозначена: Px(0) = px. Вероятность «логической единицы» входной битовой переменной X обозначена Px(1) = (px + α), где α = Px(1) – Px(0) – разность вероятностей логических уровней переменной X. Аналогично: Py(0) = py; Py(1) = (py + β) – вероятности логических уровней переменной Y; β = Py(1) – Py(0) – разность этих вероятностей. Pz(0) = pz; Pz(1) = (pz + γ) – вероятности логических уровней переменной Z; γ = Pz(1) – Pz(0) – разность этих вероятностей (α, β, γ – очень малые величины, могут иметь положительные или отрицательные значения).

Таблица 1. Вероятности входных битовых переменных

X	Y	Z	F1	F2	F3	Вероятности
0	0	0	0	0	0	px · py · pz
0	0	1	1	1	0	px · py · (pz + γ)
0	1	0	0	1	0	px · (py + β) · pz
0	1	1	1	0	1	px · (py + β) · (pz + γ)
1	0	0	0	1	0	(px + α) · py · pz
1	0	1	0	0	1	(px + α) · py · (pz + γ)
1	1	0	1	0	1	(px + α) · (py + β) · pz
1	1	1	1	1	1	(px + α) · (py + β) · (pz + γ)

Из этой таблицы можно сделать вывод о том, что все логические функции F1, F2 и F3 являются линейными, потому что количество «логических нулей» для каждой функции равно количеству «логических единиц». Поэтому разности вероятностей логических уровней для этих функций будут не более, разности вероятностей логических уровней входных битовых переменных – α, β, γ.

Рассчитаем разность вероятностей логических уровней выходной логической функции F2. Для расчета вероятности «логического нуля» на выходе функции F2 необходимо сложить вероятности первой, четвертой, шестой и седьмой строк в таблице 1:

P”(0) = [px · py · pz] + [px · (py + β) · (pz + γ)] + [(px + α) · py · (pz + γ)] + [(px + α) · (py + β) · pz].

Для расчета вероятности «логической единицы» на выходе функции F2 необходимо сложить вероятности второй, третьей, пятой и восьмой строк в таблице 1:

$$P''(1) = [px \cdot py \cdot (pz + \gamma)] + [px \cdot (py + \beta) \cdot pz] + [(px + \alpha) \cdot py \cdot pz] + [(px + \alpha) \cdot (py + \beta) \cdot (pz + \gamma)]$$

Разность этих вероятностей значительно меньше разностей вероятностей входных битовых переменных:

$$\Delta'' = P''(1) - P''(0) = \alpha \cdot \beta \cdot \gamma \qquad (2)$$

Аналогично можно показать значительное уменьшение разности вероятности логических уровней на выходе функций F1 и F3.

Используя вероятностную модель, можно показать, что при суммировании статистически независимых чисел «по модулю n» – результирующие числа будут иметь меньшую разность вероятностей, чем входные операнды.

Воспользуемся известным соотношением:

$$\mathrm{mod}_n (X + Y) = \mathrm{mod}_n (\mathrm{mod}_n (X) + \mathrm{mod}_n (Y)).$$

При n =4 входные числа X и Y и результат могут иметь значения:

$$\mathrm{mod}_4 (X) \in \{0,1,2,3\};\ \mathrm{mod}_4 (Y) \in \{0,1,2,3\};\ \mathrm{mod}_4 (X + Y) \in \{0,1,2,3\}.$$

В таблице 2 приведены входные числа $\mathrm{mod}_4 (X)$ и $\mathrm{mod}_4 (Y)$ и результирующие значения $\mathrm{mod}_4 (X + Y)$. Вероятность входного числа 0 обозначена p. Входное число 1 имеет вероятность (p + α); число 2 имеет вероятность (p + β); число 3 имеет вероятность (p + γ) – α, β, γ – очень малые величины, могут иметь положительные или отрицательные значения.

Сумма всех вероятностей входных чисел:

$$P(0) + P(1) + P(2) + P(3) = 4p + \alpha + \beta + \gamma = 1$$

Таблица 2. Вероятности входных и выходных переменных

$\mathrm{mod}_4 (X + Y)$	Вероятности
0 + 0 = 0	p · p
0 + 1 = 1	p · (p + α)
0 + 2 = 2	p · (p + β)
0 + 3 = 3	p · (p + γ)
1 + 0 = 1	(p + α) · p
1 + 1 = 2	(p + α) · (p + α)
1 + 2 = 3	(p + α) · (p + β)
1 + 3 + 0	(p + α) · (p + γ)

$\mathrm{mod}_4 (X + Y)$	Вероятности
2 + 0 = 2	(p + β) · p
2 + 1 = 3	(p + β) · (p + α)
2 + 2 = 0	(p + β) · (p + β)
2 + 3 = 1	(p + β) · (p + γ)
3 + 0 = 3	(p + γ) · p
3 + 1 = 0	(p + γ) · (p + α)
3 + 2 + 1	(p + γ) · (p + β)
3 + 3 = 2	(p + γ) · (p + γ)

Вероятности результирующих чисел рассчитаем суммированием вероятностей соответствующих строк в таблице 2:

$$P''(0) = [p \cdot p] + [(p + \alpha) \cdot (p + \gamma)] + [(p + \beta) \cdot (p + \beta)] + [(p + \gamma) \cdot (p + \alpha)] = 4p^2 + 2p\alpha + 2p\beta + 2p\gamma + 2\alpha\gamma + \beta^2.$$

Обозначим: $4p^2 + 2p\alpha + 2p\beta + 2p\gamma = P.$

Тогда: $P''(0) = \mathbf{P + 2\alpha\gamma + \beta^2}.$ (3)

$$P''(1) = [p \cdot (p + \alpha)] + [(p + \alpha) \cdot p] + [(p + \beta) \cdot (p + \gamma)] + [(p + \gamma) \cdot (p + \beta)] = 4p^2 + 2p\alpha + 2p\beta + 2p\gamma = \mathbf{P}. \qquad (4)$$

$$P''(2) = [p \cdot (p + \beta)] + [(p + \alpha) \cdot (p + \alpha)] + [(p + \beta) \cdot p] + [(p + \gamma) \cdot (p + \gamma)] = 4p^2 + 2p\alpha + 2p\beta + 2p\gamma + \gamma^2 = \mathbf{P + \gamma^2}. \qquad (5)$$

$$P''(3) = [p \cdot (p + \gamma)] + [(p + \alpha) \cdot (p + \beta)] + [(p + \beta) \cdot (p + \alpha)] + [(p + \gamma) \cdot p] = 4p^2 + 2p\alpha + 2p\beta + 2p\gamma + 2\alpha\beta = \mathbf{P + 2\alpha\beta}. \qquad (6)$$

Из равенств (3), (4), (5), (6) следует, что разности вероятностей результирующих чисел значительно меньше, чем разности вероятностей входных чисел – α, β, γ.

Аналогично можно показать, что суммирование статистически независимых чисел с другими модулями значительно уменьшает разности вероятностей результирующих чисел.

В статье [3] с использованием вероятностной модели случайных битовых последовательностей показано, что «суммирование по модулю 2» (XOR-ing) статистически независимых случайных процессов приводит к значительному уменьшению коэффициентов автокорреляционной функции результирующей битовой последовательности. Это означает, что если один из случайных процессов имел статистические связи между соседними битами, то в результирующей случайной битовой последовательности эти корреляционные связи будут значительно меньше. XOR-ing независимых случайных битовых процессов позволяет добиться выполнения условия независимости формируемых случайных бит – попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$ [3].

Выводы

Как указано в стандарте ISO/IEC 18031:2005: к источнику энтропии в недетерминированных генераторах случайных бит (НГСБ) не выдвигаются требования несмещенности выходных бит (т.е. равенства вероятностей нулевых и единичных бит), а также требование независимости бит на выходе источника энтропии. В этом стандарте на основе практического опыта рекомендуется использовать Хеш-функции в качестве функции перехода внутреннего состояния и Функции генерации выходных данных для уменьшения смещения выходных бит и уменьшения корреляционных связей между выходными битами.

Применение вероятностных моделей случайных битовых сигналов позволяет теоретически доказать, что основные математические алгоритмы, используемые в Хеш-функциях, значительно уменьшают разность вероятностей входных операндов (т.е. уменьшают смещение битовых операндов), а также уменьшают статистические связи между выходными случайными битами

В статье показано, что утверждение авторов стандарта ISO/IEC 18031:2005 о недоказуемости используемых практических результатов применения Хеш-функций – является всего лишь особым мнением этих авторов.

Литература:

1. А.А. Торба, С.Г. Елаков, А.З. Степченко Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119, с. 108-113.

2. А.А. Торба Методы статистической обработки случайных сигналов // Системи обробки інформації. Збірник наукових праць. Харків: ХУПС. – 2009. Вип. 3(77). с. 105-107.

3. А.А. Торба, В.А. Бобух, А.А. Торба Анализ автокорреляционных функций случайных сигналов // Прикладная радиоэлектроника. 2010.– Том 9, № 3.– с. 411-417.

MULTICRITERIA OPTIMIZATION IN TELECOMMUNICATION NETWORKS PLANNING, DESIGNING AND CONTROLLING

Bezruk V.M., Bukhanko O.M.
Kharkov National University of Radio Electronics
Communication Networks Department, 14, Lenin Ave., 61166, Kharkov
Tel. (057) 702-14-29, E-mail: bezruk@kture.kharkov.ua

Some features of methodology of telecommunication networks optimal design variants choice taking into account of the quality indicators are represented. In the presented work multycriteria optimization methods application in planning of cellular networks, optimal routing, choice of speech codec, controlling network resources are given too.

Introduction. The optimal problem solution of planning, designing and controlling in telecommunication networks involves definition of the initial set of the decisions, formation of a subset of the system acceptable variants, definition a criterion of optimality, and also the choice of variants of structure and network parameters, optimal by particular criterion. It is the tasks of a general decision making theory, which are reduced to implementation of some choice function of the best (optimal) system on the valid variants set. At an optimum variants choice taking into account the set of quality indicators methods we have used multicriteria optimization.

The initial set of acceptable variants of a telecommunication network is formed through the definition of different network topologies, transmission capacities of communication channels, various disciplines of service requests, applied to different routing ways choices etc. The obtained variants of a telecommunication network construction are estimated on a totality of given metrics describing the information transmission quality. Thus, the formed set of the acceptable design decisions is represented in the space of criteria ratings of quality indicators, where with usage of unconditional criterion of preference, the subset of effective (Pareto-optimal) variants of the telecommunication network is selected.

This short paper discusses some theoretical and practical aspects of the multicriteria optimization application in telecommunication networks planning, designing and controlling. It considers the particularities of application of the methods of multicriteria optimization at operation management of the telecommunication systems.

Methods of Pareto-optimal systems finding. In the general case, a telecommunication network is the system that may be considered as an ordered set of elements, relations and their properties. Their unique setting defines the goal searching system.

The solution of the problem of a choice of the system optimal variants includes the following stages: formation of a set of the system admissible variants, setting of a combination of quality indicators of the system optimality, as well as a choice of the best variants of the system by the given criterion of optimality. Let's consider some features of the methodology of the telecommunication network optimal design variants choice taking into account the quality indicators. The assigned limits on the operation conditions, $s \in S_\partial$ structure and $\beta \in \mathrm{B}_\partial$ parameters of the t*e*lecommunication networks define a subset of $\Phi_\partial = S_\partial \times \mathrm{B}_\partial$ acceptable variants. When introducing the criterion of an optimality of a network there are two approaches: ordinal and cardinal. Ordinal approach appeals to the order (better - worse) and is based on the introduction of some binary relations of admissible alternatives set. The decision $\phi^{(o)} \in \Phi_\partial$ is named optimal under the ratio $\succ$, if other decisions $\phi \in \Phi_\partial$ do not exist, for which the ratio $\phi \succ \phi^{(o)}$ is fair. The set of all optimal decisions under the ratio $\succ$ is indicated through $opt_{\succ}\Phi_\partial$. The cardinal approach to the description of preferences assigns to each alternative $\phi \in \Phi_\partial$ some numerical value of the function $U(\bullet)$, defining usefulness of alternative ϕ. Each utility function defines the appropriate order (or preference) R on set Φ_∂ $((\phi' R \phi''))$ when and only when $U(\phi') \geq U(\phi'')$. In this case they say that the utility function $U(\bullet)$ is the indicate of preference R.

It is impossible to set scalar criterion of an optimality resulting in to choice of the single variant of solution $\phi^{(o)} = \underset{\phi\in\Phi_\partial}{opt}\left[U(\phi)\right]$ in a number of cases due to poor prior representations about optimality of a network in the formalized form. Therefore on the initial stages of planning the network is characterized by a totality of quality index and bound with them by the vector goal function

$$\vec{k}(\phi) = (k_1(\phi),\ldots,k(\phi)). \quad (1)$$

In this case, there occur problems of solutions optimization by a set of quality indicators, which are also called the problems of multi-criterion or vector optimization. As a result of such a solution of the problems, there is found the subset of effective (Pareto-optimal) variants of the system, containing in the general case not one but several variants non-dominated by the relation of the strict preference.

The Pareto-optimal network versions design solution can be derived immediately on $\Phi_{\ddot{a}}$ set with application of introduced binary preference relations. This subset of Pareto-optimal variants of a network can be found as well in the space of introduced quality indicators (1), which are also named the criterion space of estimates

$$V = \vec{K}(\Phi_\partial) = (\vec{v} \in R^m \left| \vec{v} = (k_1(\phi),\ k_2(\phi),\ldots \right.$$
$$\left. \ldots, k_m(\phi)),\quad \phi \in \Phi_\partial).$$

Here to each design solution ϕ corresponds its estimate of chosen quality indicators $\vec{v} = \vec{k}(\phi)$ and, vice versa, to each estimate corresponds the design solution (in the general case, not necessarily one solution).

The Pareto-optimal design solutions can be found either directly or with the use of special methods, for example, of the weight method, or of the method of operating characteristics.

$$\underset{\phi\in\Phi_\partial}{opt}\left[k_p(\phi) = \lambda_1 k_1(\phi) + \lambda_2 k_2(\phi) + \ldots + \lambda_m k_m(\phi)\right]; \quad (2)$$

$$\underset{\phi\in\Phi_\partial}{opt}\left[k_1(\phi)\right],\quad k_2(\phi) = K_{2\phi};\ k_3(\phi) = K_{3\phi},\ldots,k_m(\phi) = K_{m\phi}; \quad (3)$$

where $\lambda_1,\lambda_2,\ldots,\lambda_m$ are chosen from the condition $\lambda_i > 0,\ \sum_{i=1}^{m}\lambda_i = 1$;

$K_{2\phi}, K_{3\phi},\ldots,K_{m\phi}$ – some fixed, but arbitrary values of quality indicators.

Practical usage of multycriteria optimization methods. The investigation results are provided on the example of solving of a particular management problem considering planning of cellular networks, optimal routing and choice of the speech codec, controlling network resources.

Planning radio communication networks. Let us consider some practical particularities of application of multicriteria optimization methods, when planning radio communication networks, on an example of cellular communication network (CCN) [1].

In the considered example, there were formed a set of admissible variants of CCN of GSM standard, which were defined by different quality indicators. The finding of the subset of Pareto-optimal variants of networks is performed in criterion space of quality indicators estimates with use of unconditional criterion of preference. A single variant of the set of Pareto-optimal CCN was chosen using of the conditional criterion of preference by finding the extreme of the scalar criterion function at $c_i = \frac{1}{7},\ i = \overline{1,7}$.

As a result of Pareto-optimization, there are obtained multivariate patterns of exchange (MPE) of quality indicators being of antagonistic character. For illustration, some MPE are presented in fig. 1. Each MPE point defines the potentially best values of each index which can be attained at fixed but arbitrary values of other quality indicators. MPE also show how the improvement of some quality indicators is achieved at the expense of other indicators.

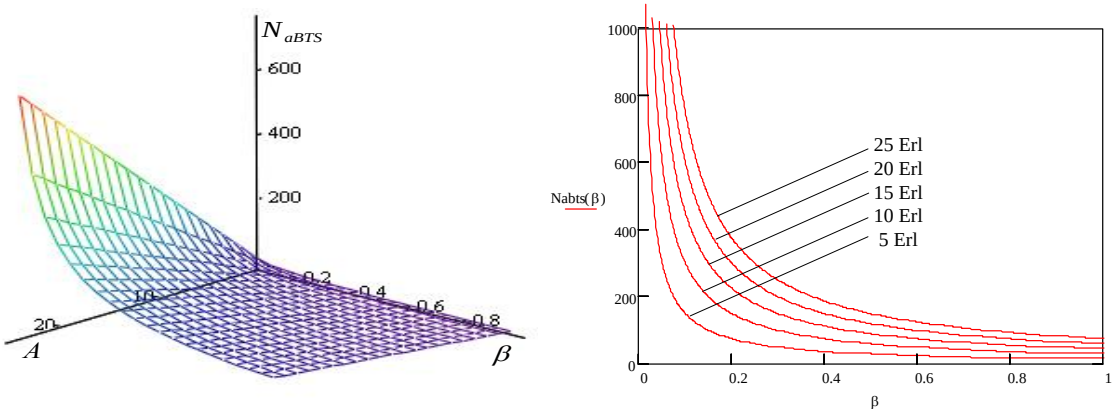


Fig. 1. MPE of quality indicators (the number of subscribers serviced by one base station, the load, the activity of subscribers) for CCN of GSM standard

Choice of speech codecs. At creation of networks of an IP-telephony there is a necessity of a choice of speech codecs, optimum taking into account set of indicators of quality [2].

For carrying out of the comparative analysis of speech codecs and a choice of optimum variants data about 23 speech codecs are taken. For their description it was used the set of 5 technical and economic indicators: speed of the coding, an estimation of quality of the coding of speech, complexity of realisation, the size of a shot, a total delay. Indicators of quality of speech codecs are connected among themselves and have competing character. From initial set of admissible variants of speech codec subset of Pareto including 23 variants of codecs is allocated. The unique design decision got out of a condition of an extreme of the scalar criterion function constructed on the basis of the theory of dim sets.

It is received, that at the set statement of a problem by the optimum speech codec the codec of series G.722b which has following values of indicators of quality: speed of coding – 64 kbit/with, an estimation of quality of coding of speech – 4,13 MOS, complexity of realisation – 11,95 MIPS, the size of a shot – 0,125 ms, a total delay – 31,5 ms.

Choosing optimal routes. The increasing volume and diversity of traffic, its demands to the quality of transmission in multiservice networks determine the need for new approaches to their management. Currently, there are a large number of routing algorithms, implemented on different principles. These algorithms solve the problem of choosing optimal routes, as a rule, taking into account one of the indicators of quality. Therefore, in modern multiservice networks raises the problem of the totality of the performance network to provide the specified quality of service requirements of different types of traffic. This determines the need for multicriteria optimization methods on networks for solving the routing [3].

In this work practical features of the application of the multicriteria approach to the decision of a problem of the optimal routing on an example of a fragment of a network of the Kharkov town are considered. For a finding of a subset of Pareto-optimum decisions it is offered to use a weight method (2).

Management of networking channel's and information resources. Multicriteria optimization could be also used in a management of networking channel's and information resources. Within existing telecommunication technologies for the solving of existing problems with the network resources controlling the protocols routing and load balancing, means, algorithms service and restrictions queues is engaged. Network resources' balancing is provided on the basis of the vector of traffic distribution [4]

$$\vec{K} = (k_1, k_2, ..., k_l), \quad \sum_i^l k_i = 1. \qquad (4)$$

Within this model the network resources controlling comes to the optimization task depended with function (5) minimization. This model takes into account the standard routing metric, the standard deviation of channels and controlling agents loading

$$\varepsilon(\vec{K}) = \min(q_1\Phi + q_2\sigma_1(\vec{K}) + q_3\sigma_2(\vec{K})). \quad (5)$$

According to investigations it can be concluded that according to changing network loading within the proposed model is able to minimize the delay time for 3 – 12% and 6 – 25%, the probability of packet loss on 6 – 11% and 6 - 20%, respectively for both methods of (5) minimization.

Optimal functioning system variant. Pareto-optimal variants of the network are obtained with the methods of vector optimization. Among them the single optimal variant of construction of a network is selected for the task of planning (fig. 2). Results of optimization were used for the task of the network control when framing optimal control actions. In the example the centralized-distributed control structure – the load control mechanism in a communication channel is implemented in each switching centre [5].

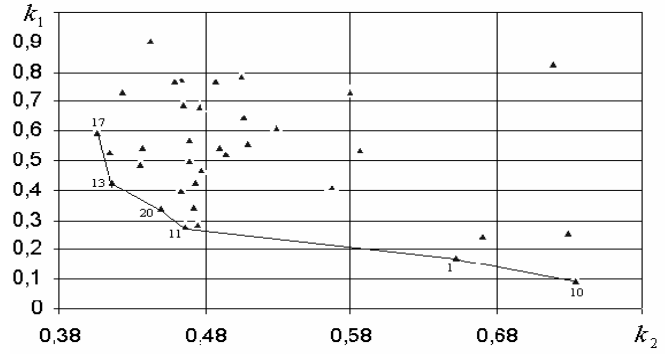


Fig. 2. Choice of Pareto-optimal variants of the telecommunication network

The quality indicators - time of delivery and probability of loss of packets are selected from the surveyed example at datagram message transmission. The given task is urgent for practical applications critical to time of the messages delivery (in telecommunication systems of video and voice intelligences, systems of banking terminals; alarm installations; systems of fault recovery on telecommunication networks).

Conclusions. The structure of the model realized with a computer, includes simulators of the messages with a Poisson distribution law and given intensities, procedures of the messages packing, their transmission by the communication channels.

The methods of the multicriteria optimization of the processes of planning and controlling the telecommunication networks in present issue considered above. They can be used when starting, upgrading both operation of analog and digital networks, cellular networks and multiservice networks, satellite networks, local and corporate networks.

References.

1. Bezruk V.M., Chebotaryova D.V, Anishchenko A.V. Automatic control of radio communication networks design // Telecommunications and Radio Engineering. – USA, 2009. – 68(5). – P. 429 – 444.

2. Безрук В.М., Скорик Ю.В. Выбор оптимальних речевых кодеков для сетей IP-телефонии с учетом совокупности показателей качества. // Радиотехника: Всеукр. межвед. науч.-техн. Сб. 2009. Вып. 159. С. 243 – 247.

3. Безрук В.М., Варич В.В. Многокритериальный подход к маршрутизации в сетях связи. // Радиотехника: Всеукр. межвед. науч.-техн. Сб. 2010. Вып. 163. С. 45 – 48.

4. Безрук В.М., Буханько А.Н. Метод управления сетевыми ресурсами в мультисервисных телекоммуникационных системах на основе распределенной системы агентов // Сб. материалов 20-й Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии». – Севастополь: Вебер. – 2010. – С. 526-527.

5. V.M. Besruk, I.V. Svid, I.V. Korsun Multicriteria optimization of management of the packet switching network // Telecommunications and Radio Engineering. – USA, 2008. – 67(1). – P. 23 – 32.

РЕШЕНИЕ ЗАДАЧИ ВЫБОРА МАРШРУТОВ С ПРИМЕНЕНИЕМ МНОГОКРИТЕРИАЛЬНОГО ПОДХОДА

Безрук В.М., Варич В.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. «Сети Связи», тел. 702-14-29,
E-mail: bezruk@kture.kharkov.ua

Abstract - Practical features of multi-criteria approach to solving the problem of optimal routing in a multiservice network considered. To solve this problem in the theory of decision-making using multi-criteria approach - a selection of some properties of objects (features), them evaluation and decision on the results of the comparisons. Network model is chosen. The network form is f MNV graph. It contain a set of nodes and links. We found a subset of the Pareto-optimal routing options based set of indicators of quality.

I. Введение

Увеличение объемов разнородной информации, передаваемой в современных мультисервисных сетях связи, а также необходимость передачи этой информации с гарантировонным качеством обусловливает поиск более совершенных подходов к планированию и управлению трафиком в мультисервисных сетях связи. Мультисервисная сеть связи представляет собой сложную систему с множеством элементов, влияющих на эффективность ее работы, и для обеспечения высокого качества обслуживания различных типов трафика необходимо решение задачи планирования маршрутизации с учетом совокупности показателей качества. Это определяет необходимость применения методов многокритериальной оптимизации при решении задач маршрутизации в таких сетях связи. Многокритериальный подход при решении поставленой задачи включает выбор некоторых свойств объектов и соответствующих показателей качества, их оценку и принятие оптимальных решений по результатам сравнений вариантов маршрутизации по совокупности показателей качества.

II. Постановка задачи

Задано множество допустимых решений (маршрутов) на конечном графе сети $G=(V,E)$, где $V=\{v\}$ – множество узлов, $E=\{e\}$ – множество линий связи. Каждый маршрут x определяется некоторым подмножеством узлов и линий связи. В задачах маршрутизации принятие оптимальных решений представляется моделью $\{X,F\}\to x^*$, где $X=\{x\}$– множество допустимых решений (маршрутов) на графе сети $G=(V,E)$; $F(x)$– целевая функция выбора маршрутов; x^* – оптимальное решение задачи маршрутизации. При многокритериальном подходе к выбору оптимальных маршрутов полагается, что выполняется декомпозиция функции $F(x)$ на совокупность (вектор) частных функций выбора. В этом случае на множестве X задается векторная целевая функция

$$F(x)=(W_1(x),\ldots,W_j(x),\ldots,W_m(x)), \qquad (1)$$

составляющие которой определяют значения совокупности показателей качества маршрутов. Показатели качества маршрутов в сетях связи, как правило, связаны между собой и антагонистичны.

Решением задачи оптимальной маршрутизации с учетом совокупности показателей качества является выбор подмножества Парето-оптимальных маршрутов [1]. Вариант маршрута $x^*\in X$ является Парето-оптимальным, если не существует другого маршрута $x\in X$, чтобы выполнялись неравенства $F_j(x^*)\le F_j(\tilde{x}), j=1,\ldots,m$, причем хотя бы одно из неравенств являлось строгим.

III. Особенности выбора Парето-оптимальных маршрутов

Рассмотрим особенности выбора Парето-оптимальных маршрутов с учетом совокупности показателей качества. Существуют разные методы выбора подмножества Парето-оптимальных решений [2]. Предлагается решать задачу нахождения Парето-оптимальных маршрутов весовым методом [3], который сводится к нахождению экстремальных значений целевой функции маршрута в виде взвешенной суммы частных функций выбора при всевозможных значениях взвешивающих коэффициентов λ_j

$$\underset{\text{var}x\in X}{extr}\left(F(x)=\sum_{j=1}^{m}\lambda_j W_j(x)\right) \qquad (2)$$

Коэффициенты λ_j характеризуют относительную ценность показателей качества маршрутов, причем $\sum_{j=1}^{m}\lambda_j = 1$.

Парето-оптимальные маршруты обладают рядом характерных свойств. В частности, Парето-оптимальным вариантам маршрутов соответствует согласованный по Парето оптимум частных целевых функций $W_1(x),\ldots,W_j(x),\ldots,W_m(x)$. При выборе подмножества Парето-оптимальных маршрутов отбрасываются безусловно худшие с точки зрения безусловного критерия предпочтения (критерия Парето) варианты маршрутов. Парето-оптимальные варианты маршрутов равнозначны по критерию Парето и поэтому могут быть использованы при организации многопутевовой маршрутизации в мультисервисных сетя связи.

IV. Пример использования многокритериального подхода к решению задачи маршрутизации

Рассмотрим некоторые практические особенности решения указанной многокритериальной задачи маршрутизации на примере фрагмента сети связи, показанной на рис. 1. Модель сети состоит из двенадцати узлов, связанных между собой линиями связи с потерями.

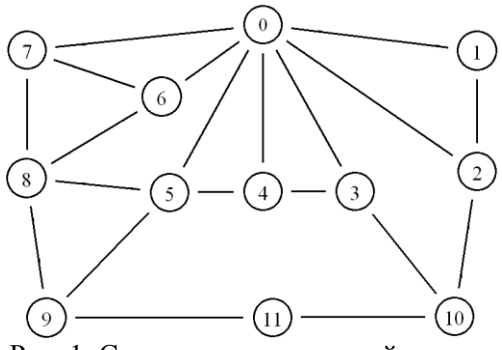


Рис. 1. Структура исследуемой сети связи

Информация передается из узла 0 во все остальные узлы. Введены следующие показатели качества маршрутов: время задержки пакетов, уровень потерь пакетов, стоимость использования линии связи. Значения нормированных к максимальным значениям показатели качества приведены в табл. 1.

Таблица 1.

Линия связи	Время задержки передачи пакетов k_1	Уровень потерь пакетов k_2	Стоимость использования линии связи k_3
0-1	0.676	1	0.333
0-2	1	0.25	1
0-3	0.362	1	0.333
0-4	0.381	0.25	1
0-5	0.2	1	0.333
0-6	0.19	1	0.333
0-7	0.571	0.25	1
7-6	0.4	0.25	0.333
7-8	0.362	0.25	0.667
8-6	0.314	0.5	0.5
8-5	0.438	0.25	0.333
8-9	0.248	0.5	0.333
9-5	0.257	0.25	1
9-11	0.571	0.25	0.667
11-10	0.762	0.25	0.333
5-4	0.381	0.25	0.667
2-10	0.457	0.25	0.333
3-10	0.79	0.25	0.333
4-3	0.286	0.25	0.333
1-2	0.448	0.25	0.333

При анализе сети видно, что для каждого узла назначения существует большое количество вариантов выбора маршрута. Например, при передаче из узла 0 в узел 8 количество маршрутов составляет 22.

Для решения задачи выбора Парето-оптимальных маршрутов применим описанный выше весовой метод. При минимизации выражения (2) с некоторыми всевозможными комбинациями весовых коэффициентов получено подмножество Парето-оптимальных вариантов маршрутов.

Для иллюстрации на рис. 2 изображено некоторое множество вариантов маршрутов между узлами 0 и 8 в пространстве показателей качества k_1 и k_2. Подмножеству Парето-оптимальных альтернатив маршрутов соответствует левая нижняя граница, включающая три варианта, обозначенные (▲). Этому подподмножеству соответствует согласованный по Парето оптимум показателей качества.

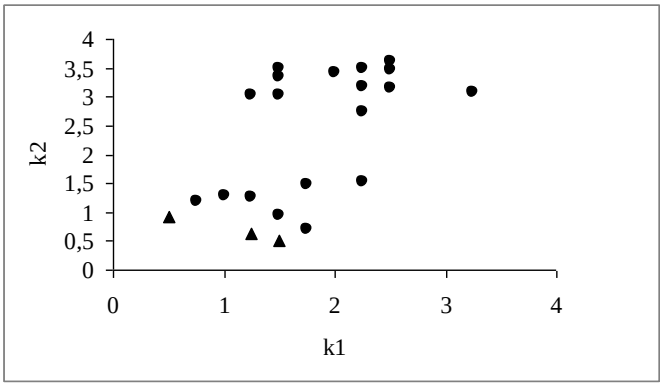


Рис. 2. Множество вариантов маршрутов в сети между узлами 0 и 8

Полученное подмножество Парето-оптимальных вариантов маршрутов может быть использовано, в частности, для организации многопутевой маршрутизации при использовании технологии MPLS. Это позволит обеспечить выравнивание нагрузки и управление трафиком, а также обеспечить заданное качество обслуживания с учетом совокупности показателей качества .

V. Выводы

1. Рассмотрены практические особенности многокритериального подхода к решению задачи маршрутизации в мультисервисной сети связи.

2. Многокритериальный подход решению задачи маршрутизации дает возможность учитывать совокупность показателей качества, которые разносторонне оценивают маршруты.

3. Оптимальным решением задачи есть подмножество Парето-оптимальных вариантов маршрутов. Это подмножество можно использовать для организации многопутевой маршрутизации с использованием технологии MPLS.

Литература:

1. Перепелица В.А. Многокритериальные задачи теории графов. Алгоритмический подход. – Киев УМК ВО, 1989.

2. Безрук В.М. Векторная оптимизация и статистическое моделирование в автоматизированном проектировании системы связи. – Харков: ХНУРЕ, 2002.

3. Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. – М.: Высшая школа, 1982.

ИНФОРМАЦИОННАЯ СИСТЕМА КОМПЬЮТЕРНОЙ ТЕЛЕФОНИИ ДЛЯ АВТОМАТИЗАЦИИ ДИСПЕТЧЕРСКИХ СЛУЖБ СВЯЗИ

Безрук В.М., Загайнов В.И., Кочкин М.И., Ляховец В.А., Мальцев В.С., Сырцов С.Л., Твердохлеб В.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. «Сети связи», тел. (057) 702-14-29,
E-mail: tkvt_mz@ktyre.kharkov.ua; факс (057) 702-11-13

The main principles of creation automized are considered is informational - help complexes with access through telephone channels and program choice of modes of their operation. On the basis of the computer technology of information processing and hardware of digital signal processing the structures of hardware-software complexes of archiving and informing through telephone channels are developed. The program part of complexes provides the automized continuous processing of the information real-time and is constructed on principles of the dialogue service system. The principal components of the program complex for creation of systems of informing of customers of municipal services about their duties are considered. The information tasks are parsed which can be decided with the help of these complexes.

Перспективным направлением в технике телекоммуникаций в настоящее время является создание информационных систем в виде аппаратно-программных комплексов на основе компьютерной технологии обработки и управления информационными потоками. Значительное количество задач в этом направлении связано с архивацией и созданием интеллектуальных баз данных речевых сигналов и другой информации на основе телефонных сетей общего пользования. Особенно эффективным может стать применение таких комплексов для создания информационных систем при модернизации диспетчерских служб связи различных предприятий энергетики, коммунального хозяйства, аварийных служб и учреждений скорой медицинской помощи и т. п.

Очевидно, что аппаратно – программные комплексы должны содержать в себе многоканальную систему аналого-цифрового преобразования и предварительной обработки сигналов телефонных сетей связи, систему формирования файлов цифровых портретов исследуемых сигналов и передачи их через стандартные компьютерные шины ISA, PCI или USB и канал прямого доступа в память персонального компьютера. Программная часть комплекса должна позволять формировать распределенные цифровые потоки сигналов для каждого канала связи. Цифровые сигналы каждого канала в реальном масштабе времени записываются на магнитный диск персонального компьютера вместе с заданным паспортом записи, привязанным к текущей дате и времени. Отдельный программный модуль позволяет формировать и выдавать в каналы компьютерной телефонии программно-управляемые тестовые сигналы.

Очевидно, что аппаратная часть программно–технического комплекса должна состоять из устройства автоматической идентификации состояния телефонной линии, многоканального устройства аналого-цифрового преобразования сигналов телефонных каналов, устройства первичной обработки цифрового потока с целью выделения служебной информации, автоматического регулирования уровня архивируемой информации и др. Аппаратная часть должна представлять собой автономную систему, взаимодействующую с персональным компьютером через стандартные шины.

Основными задачами при разработке режимов функционирования аппаратно-программного комплекса информирования по телефонным каналам являются:

- передача в телефонную линию стандартного вызывного сигнала и анализ состояния канала телефонной связи и абонента;
- передача заранее записанного при помощи такого комплекса звукового файла, выбранного из установленной базы звуковых файлов;
- автоматический анализ состояния канала телефонной связи при передаче звукового файла с целью анализа поведения абонента: ”снял трубку”, ”полностью выслушал сообщение”, ”прервал связь, не дослушав до конца” и т.п.;

- автоматическое прогнозирование событий в отдельной базе данных по всем проведенным соединениям с абонентами;

- текущее оперативное формирование каталога предполагаемых соединений с абонентами согласно заранее установленных категорий абонентов и результатов предшествующего функционирования комплекса;

- формирование процедур и алгоритмов защиты передаваемой информации.

Синтез программной части комплекса предполагает создание диалоговой сервисной системы, обеспечивающей выполнение следующих функций:

- составление каталога обслуживаемых абонентов и категорий их приоритетов;

- ввод расписания даты и времени выдачи установленных речевых сообщений;

- автоматическое ведение протокола событий и выполнение статистического анализа событий в соответствии с выбранными алгоритмами;

- формирование, просмотр и выдача стандартных и специализированных карточек отчетной документации по эффективности функционирования комплекса.

Структура аппаратно-программного комплекса на основе компьютерной технологии обработки и управления информационными потоками представлена на рис. 1.

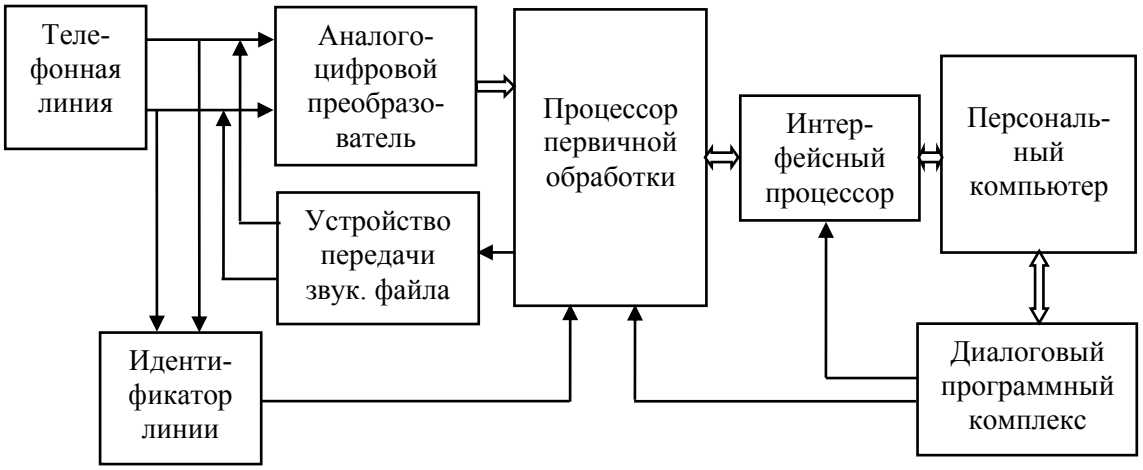


Рис. 1. Структура аппаратно-программного комплекса

С помощью такого комплекса могут быть решены следующие задачи:

- формирование фразы автоответа с сообщением о состоянии текущего счета абонента в ответ на его звонок;

- формирование последовательности звуковых сообщений для автоматического обзвона группы абонентов в соответствии с заранее выбранными категориями потребителей коммунальных услуг в зависимости от состояния их текущего счета;

- формирование информационной таблицы ответных реакций по каждому абоненту при реализации режима автоматического обзвона.

Анализ информационных задач, решаемых в диспетчерских службах связи, показывает, что основная часть их может быть осуществлена в рамках 3-х модификаций: система документирования и архивации речевой информации; информационно-справочная система, органически соединенная с набором баз данных (Call Center), и система быстрого оповещения абонентов в чрезвычайных ситуациях.

Система документирования и архивации речевой информации обеспечивает регистрацию речевой технологической информации от любого источника аудиосигнала - телефонной линии, линии селекторной связи, радиоканала, микрофона. Запись речевой информации производится на жесткий магнитный диск компьютера. Для управления системой в этом случае используется программа Recorder DTR. Главная панель управляющей программы Recorder DTR представлена на рис 2.

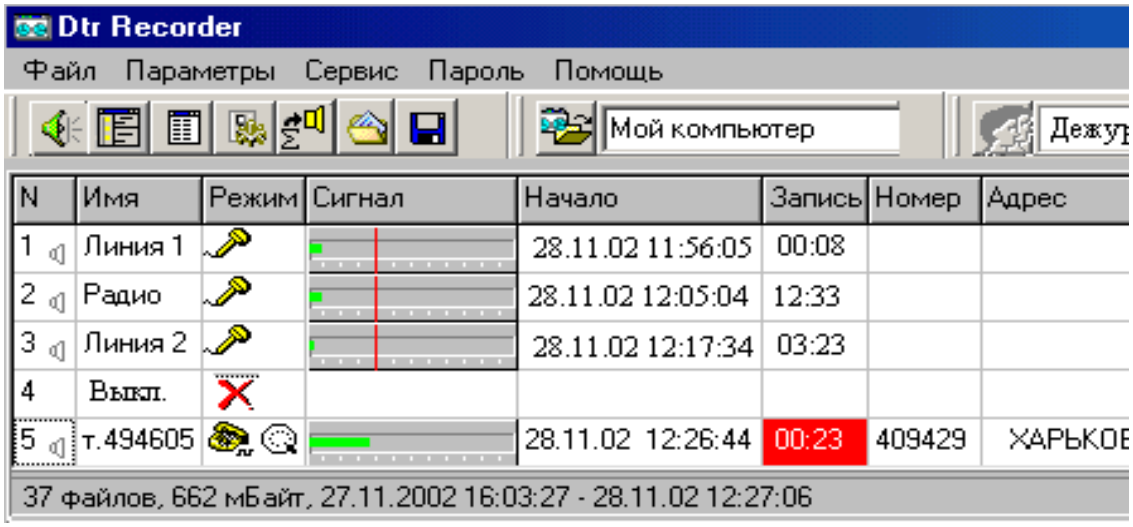


Рис. 2. Главная панель управляющей программы Recorder DTR

Прослушивание записанных разговоров может быть осуществлено с помощью програмного модуля Player DTR. Главное окно програмного модуля Player DTR представлено на рис 3.

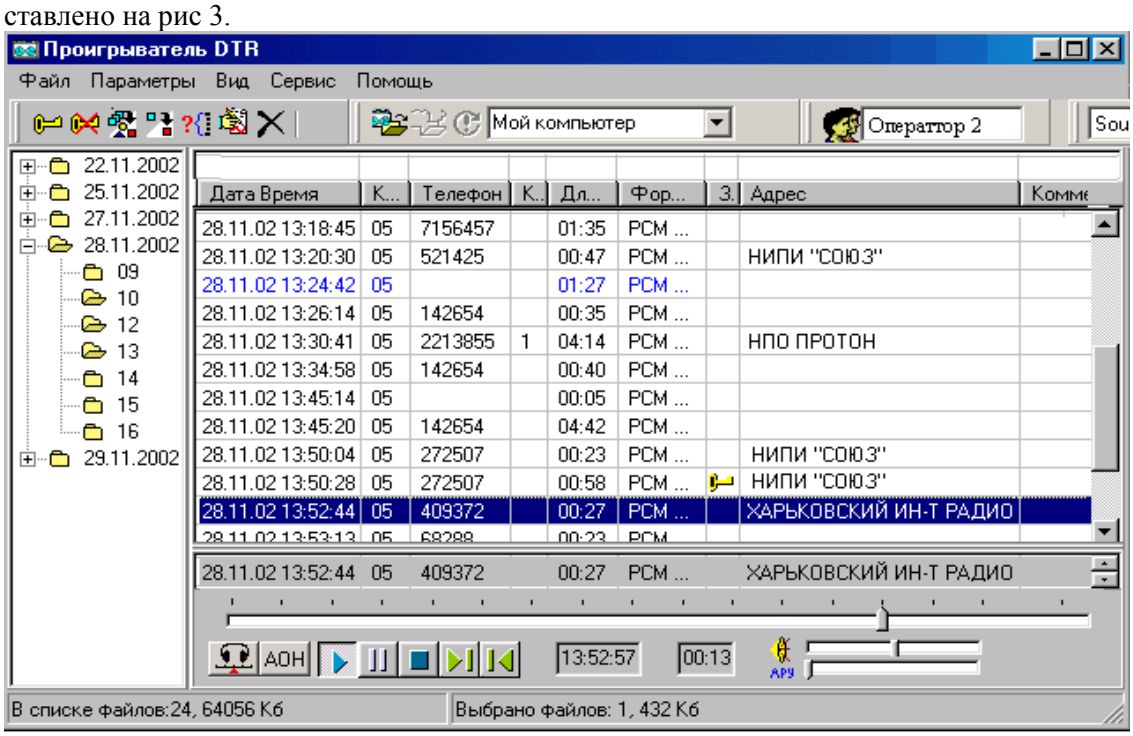


Рис. 3. Главное окно програмного модуля Player DTR

Информационно-справочная система (Call Center) предназначена для автоматического общения по телефону с клиентами - потребителями различных коммунальных услуг (электричество, тепло, газ, вода) и обмена с ними информацией. К Call Center подключается от 1 до 8 телефонных линий. Система может сообщать абонентам сумму их задолженности; принимать от абонентов показания приборов учета; воспроизводить по телефону звуковой файл с требуемой абоненту информацией; соединять абонента с оператором; передавать по телефону циркулярное сообщение для абонентов из установленного списка.

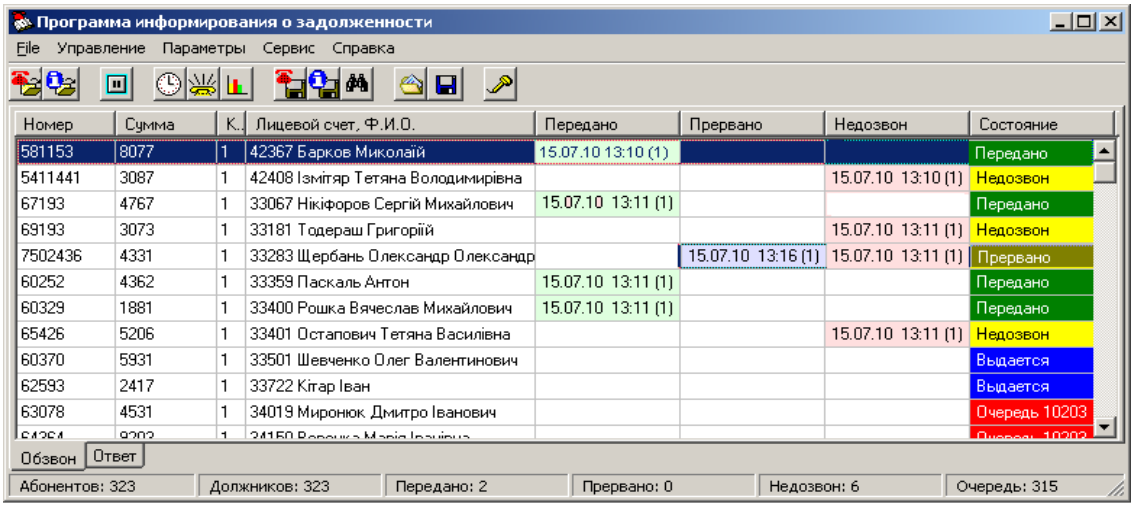


Рис. 4.Информационное окно работы комплекса в режиме информирования о задолженности.

Система оповещения предназначена для автоматического оповещения личного состава подразделений быстрого реагирования о наступлении кризисных ситуаций (МЧС, МВД, охрана, аварийные службы). Запуск программы оповещения выполняется оператором. Оповещение производится передачей по телефону звукового сообщения для абонентов из заранее подготовленного списка. Факт получения сообщения абонент подтверждает, набрав на своем телефоне определенную комбинацию цифр.

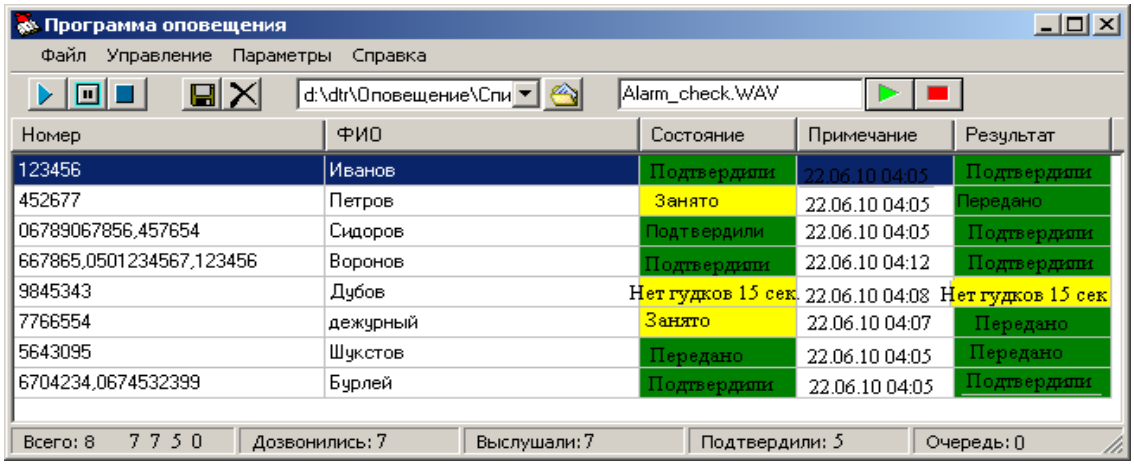


Рис. 5. Окно отображения функционирования программного модуля оповещения.

Диалоговая информационная система компьютерной телефонии, разработанная в Харьковском национальном университете радиоэлектроники по выше изложенной методологии, позволяет создавать конкурентноспособные гибкие информационные системы для решения широкого круга организационных и технических задач для автоматизации современных и перспективных диспетчерских служб связи различных предприятий.

АНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ NTRU СОГЛАСНО СТАНДАРТА ANSI X9.98

Беликова Е.С., Заросилова М.Г.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. Безопасности Информационных Технологий
тел. (057) 702-14-25 E-mail: elenochka.flame@gmail.com

This work is devoted to analysis of encryption algorithm NTRU. Here it is given a describing of key generetion, encryption and decription procedures; advantages of NTRU, such as perfomans, durability to quantum computer attack.

Существует множество ассиметричных систем. Одна из наиболее распространенных асимметричных криптосистем — RSA. RSA плохо подходит для использования во встраиваемых устройствах, потому что требует оперирования большими числами, что не всегда можно реализовать при ограниченных ресурсах. Кроме того, RSA работает довольно медленно, особенно это касается генерации ключей, и в RSA используются более длинные ключи по сравнению с другими криптосистемами с открытым ключом. Но RSA хорошо подходит для сравнения криптографической стойкости других криптосистем. Для использования криптографии в мобильных устройствах, память и вычислительная мощность которых сильно ограничены, необходимы более эффективные алгоритмы. Самая распространенная из таких криптосистем — эллиптическая криптосистема, которая требует меньше ресурсов, чем RSA. Хотя эллиптическая криптосистема не настолько хорошо исследована, как RSA, она считается надежной и используется в нескольких стандартах. Криптосистема, созданная позднее, такая как: NTRU, работают быстрее, чем эллиптическая криптосистема, но ее надежность недостаточно исследована.

NTRU был разработан в середине 1990-х годов и впервые был представлен на конференции CRYPTO'96. В этом алгоритме все операции производятся в кольце усечённых многочленов. Криптографическая стойкость алгоритма основана на сложности задачи нахождения короткого вектора в заданной решётке.

Схема шифрования SVES состоит из пяти операций генерации ключа, подтверждения правильности ключевой пары, подтверждения правильности открытого ключа, зашифрования и расшифрования.

Генерация ключа. Для заданного набора общесистемных параметров ассиметричная пара состоит из личного ключа f и открытого ключа h, которые являются полиномами степени N-1.

Ключевые пары тесно связаны с доменными параметрами и должны использоваться только вместе с конкретными общесистемными параметрами, при участии которых были сгенерированы.

Личный ключ f и вспомогательный полином g в общем случае генерируются случайным (псевдослучайным) образом лишь с тем условием, что для f должны существовать обратные полиномы как по модулю p, так и по модулю q. Для стандарта X9.98 он должен иметь вид f = 1 + p*F, где F генерируется с помощью генератора случайных чисел, p — меньший модуль, целое число (в данном стандарте p = 3).

Ключи генерируются или с использованием генератора случайных бит RBG в связке с индексной функцией генерации IGF, или с помощью генератора случайных чисел (диапазон значений от 0 до N-1). Чтобы ключи соответствовали уровню безопасности в k бит, генератор случайных чисел/бит должен быть проинициализирован хотя бы 64+k битами энтропии (т. е. выполнить 64+k холостых циклов генерации).

Шифрование. Для осуществления процедуры зашифрования необходимо сгенерировать полином r. В общем случае полином r выбирается случайным (псевдослучайным) образом (со степенью, не большей N-1). В стандарте X9.98 он детерминировано формируется из сообщения m и случайного значения *b* с помощью псевдослучайного генератора.

Процедура зашифрования определяется следующей формулой:

$$e = r*h + m \pmod q,$$

где r – случайный полином,
h- открытый ключ,
m – сообщение,
q – больший модуль (в стандарте X9.98 q=2048)
e — криптограмма.

Расшифрование. Расшифрование выполняется следующим образом. Сначала вычисляется многочлен a:

$$a = f*e \bmod q,$$

где f – секретный ключ,
e — криптограмма,
q – больший модуль (в стандарте X9.98 q=2048).

В стандарте X9.98 коэффициенты многочлена a лежат в пределах [A, A + q -1], A — общесистемный параметр, зависит от остальных ОСП, обычно большое отрицательное число.

Далее вычисляется

$$m^* = f_p^{-1}*a \bmod p,$$

где f_p^{-1} – обратный многочлен по модулю p.

Расшифрованное сообщение m*, в общем случае, может не совпадать с исходным. Это происходит из-за того, что операции производятся сначала по модулю q, а потом по модулю p. Поэтому необходимо, чтобы многочлен a имел коэффициенты из такого интервала, чтобы их не пришлось приводить по модулю q. Это позволит восстановить исходное сообщение.

NTRU имеет два основных преимущества перед другими ассиметричными алгоритмами:

1. NTRU работает быстрее, чем используемые в настоящее время криптосистемы с открытым ключом. Скорость работы NTRU гораздо выше, чем RSA и EC: он в 1300 раз быстрее 2048-битного RSA и в 117 раз быстрее ECC NIST-224 (если сравнивать количество операций в секунду), или в 1113 раз быстрее, чем 2048-битный RSA (если сравнивать пропускную способность).

2. Если задача факторизации целых чисел, задача дискретного логарифма в конечных полях и задача дискретного алгоритма на эллиптических кривых были решены (например, реализацией квантового компьютера достаточного размера), задача нахождения короткого вектора в решетке является криптостойкой к алгоритмам, выполняемым на квантовых компьютерах.

ВЕРОЯТНОСТНЫЕ МОДЕЛИ ПРОЦЕССОВ ОБСЛУЖИВАНИЯ ВЫЗОВОВ И УПРАВЛЕНИЯ ИМИ В ИНФОРМАЦИОННЫХ СЕТЯХ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Бидный Ю.М.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. сетей связи, тел. (057) 702-14-29,
E-mail: tkvt_mz@kture.kharkov.ua

The given work is connected with research in the field of probabilistic models for service call processes and its management in information next generation networks. For their in this report are used probabilistic models such as control Markov's circuit in discrete time observation and semiMarkov's processes in continuous time observation. It is considered realization this models for the basic call management processes in intelligent network.

При внедрении услуг информационных сетей следующего поколения (NGN) в Украине актуальной проблемой является разработка систем управления вызовами, примером которых является программный коммутатор (Softswitch). Для этого необходим выбор адекватных моделей их объектов управления, которые оказывают существенное влияние на стратегии, структуры и параметры систем управления. Решение этих задач исследований усложняется ввиду таких неотъемлемых свойств процессов обслуживания вызовов в NGN, как их распределенный характер и сложные алгоритмы взаимодействия между ними. Модели таких объектов управления должны представлять собой комплекс взаимодействующих компонентов со сложными и случайными причинно-временными связями. Все эти особенности вызывают необходимость применения вероятностных моделей процессов обслуживания вызовов и управления ими в NGN.

В качестве класса таких конструктивных моделей в докладе рассматриваются управляемые марковские процессы (УМП) $\xi(t)$ с конечным числом состояний (фаз обслуживания вызовов), переход между которыми осуществляется под воздействием управлений. Обозначим состояния УМП через $x_1, x_2, \ldots$, их множество - через X, траектории - через $x(t)$, а пространство этих траекторий - через χ. Когда необходимо особо подчеркнуть, что траектория рассматривается на интервале времени $[s,t)$, будем использовать обозначение $x_s^t = \{x(\tau), s \le \tau < t\}$. На вероятностные характеристики УМП $\xi(t)$ влияют управления $u(t)$ из некоторого множества U. Если управления в разных состояниях различны, то через U_x обозначим множество управлений в состоянии x. Тогда $U = \bigcup_{x \in X} U_x$. Управление $u(t)$ может быть рандомизированным, когда в момент времени t оно принимается на основании наблюдений за траекторией до этого момента времени и не зависит от будущего течения процесса: $u(t) = u\lfloor t, x^t \rfloor \equiv u[t, x(\tau);\ 0 \le \tau < t]$, где $u\lfloor t, x^t \rfloor$ - вообще говоря, случайный функционал над пространством траекторий χ процесса $\xi(\tau)$ на участке $[0,t)$. Семейство управлений во времени образует стратегию $\delta = \{u\lfloor t, x^t \rfloor,\ 0 \le t < \infty\}$. Поэтому поведение УМП характеризуется парой (ξ, δ).

Пусть наблюдения над объектом управления производятся в дискретные детерминированные моменты времени $t_n = n \cdot \Delta t \quad (n = 0,1,2,\ldots)$. Множество наблюдаемых состояний X состоит из конечного или счетного числа точек $\{x_1, x_2, \ldots\}$, а управления u принимают конечное число значений. Пространство допустимых стратегий Δ состоит из множества различных последовательностей

$$\delta = \{u(0, x(0)), u(1, x(0), u(0), x(1)), \ldots\}.$$

Наряду с пространством всех допустимых стратегий Δ будем рассматривать пространство Δ' марковских стратегий $\delta \in \Delta'$: $\delta = \{u(0, x(0)), u(1, x(1)), \ldots\}$ и пространство ϑ однородных марковских стратегий $\delta \in \vartheta$: $\delta = \{u(x), x \in X\}$.

Предположим, что наблюдения над состояниями системы удовлетворяют условию

$$\mathrm{P}\{\xi(t+1)=x_j/\xi^t=x^t,\delta^t=u^t\}=\mathrm{P}\{\xi(t+1)=x_j/\xi(t)=x_i,u(t)=u\}=p_{x_ix_j}(u).$$

Тогда УМП представляет собой управляемую марковскую цепь (УМЦ), определяемую вероятностями переходов $p_{x_ix_j}(u)$.

Более широкий класс объектов управления описывается полумарковскими процессами. Одно из возможных определений полумарковского процесса $\xi(t)$ состоит в следующем. Пусть процесс может находиться в одном из состояний конечного или счетного множества $X=\{x_1,x_2,\ldots\}$, причем переходы из состояния x_i в состояние x_j происходят с вероятностями $p_{x_ix_j}$ независимо от предыдущей истории, а время пребывания в состоянии x_i до перехода в состояние x_j является случайной величиной $T_{x_ix_j}$ с заданной функцией распределения $F_{x_ix_j}(t)=P\{T_{x_ix_j}\le t\}$. Такой процесс $\xi(t)$, который в момент времени t находится в состоянии x, является управляемым полумарковским процессом (УПМП).

Обозначим через $N(t)$ число изменений состояний УПМП за время t; S_n - момент n-го изменения состояния УПМП, так, что $S_0=0$, $S_1=\tau_{x_0x_1},\ldots,S_n=\sum_{i=1}^{n}\tau_{x_{i-1},x_i,\ldots}$. $x_i=x(S_i-0)$ состояние УПМП непосредственно перед моментом i-го изменения.

Пусть теперь имеется управляющий параметр, принимающий значения u из некоторого конечного множества U, так что вероятностные характеристики УПМП зависят от значения управления. Семейство управлений во времени определяет стратегию

$$\delta=\{u[t,x^t]\,|\,0\le t<\infty\}.$$

Однородной марковской стратегией, как и ранее, называется стратегия, при которой управления в каждый момент времени зависят лишь от состояния процесса в этот момент времени $u[t,x^t]=u(x(t))$.

Если ограничиться лишь однородными марковскими стратегиями, то УПМП описываются наборами:

$p_{x_ix_j}(u)$ $(x_i,x_j\in X,u\in U)$ – вероятностей переходов;

$F_{x_ix_j}(t;u)$ $(x_i,x_j\in X,u\in U)$ – функций распределения вероятностей длительностей переходов.

В качестве примера практической реализации представленных научных результатов приводится описание УМП в виде вероятностного - временного графа для менеджера базового процесса обслуживания вызовов (BCM) при предоставлении набора услуг CS-1 интеллектуальной сети (IN). BCM является абстрактным представлением той части Softswitch, в которой реализованы функции управления вызовами (CCF) и функции коммутации услуг (SSF). Кроме того, в BCM реализована модель состояний базового процесса обслуживания вызовов (BCSM), которая представляет собой модель действий CCF, необходимых для установления и поддержания связи между пользователями. Она идентифицирует действия, относящиеся к базовому процессу обслуживания вызова, и показывает, как эти действия объединяются. Для построения модели соответствующего ей УМП предлагается использовать машины конечных состояний и диаграммы на языке спецификаций и описаний (SDL) в соответствии с Рекомендацией ITU-T Q.1214.

Приведенные в докладе новые научные и практические результаты позволят определить вероятность своевременного обслуживания вызова и среднее время его обслуживания, а также оптимизировать стратегии управления для Softswitch IN как неотъемлемой части NGN.

Секция № 4

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ПРОБЛЕМНІ ПИТАННЯ ТА ОСНОВНІ НАПРЯМИ УДОСКОНАЛЕННЯ ТА РОЗВИТКУ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ ВІДКРИТОГО КЛЮЧА

Горбенко Ю.І.[1],Чичмар С.В.[1], Тоцький О.С., Бондаренко В.І.[2], Горбенко І.Д.[3]
[1]АТ «Інститут інформаційних технологій»
[2]Адміністрація Держспецзвязку
[3]Харківський національний університет радіоелектроніки
61166, Харків, вул. Бакуліна, 12, ЗАТ»ІІТ», тел.(057) 714-22-05
E-mail: GorbenkoI@iit.kharkov.ua

An analysis of the development and use of public key infrastructure in Ukraine, are considered key issues for improvement and standardization of various applications, substantiated requirements for public key certification policies and perspective cryptographic conversions.

Загально визнаним та безумовним є той факт, що стан розвитку земної цивілізації в суттєвій мірі визначається станом розвитку та застосування інформаційних технологій та інформаційно – телекомунікаційних систем в різних сферах нашого буття, здійснення стосунків в межах земної цивілізації. Зважаючи на вказане в Україні значна увага приділяється створенню та розвитку різноманітних інформаційних технологій.

Прийнята науково – технічна програма впровадження і застосування грід - технологій на 2009-2013 роки. За задумкою національний грід – являє собою просторово-розподілена обчислювальну систему, яка на даний час уже складається з більше ніж 30 обчислювальних кластерів. Грід система може працювати як єдиний потужний комп'ютер і дозволяє розв'язувати наукові і науково-технічні задачі, що потребують надвеликих обчислювальних ресурсів.

Широкого розповсюдження набуло використання специфічно поданої інформації – електронних документів і здійснення на їх основі електронного документообігу[1-4]. Уже перші впровадження підтверджують, що електронний документообіг є найбільш результативним підходом до суттєвого підвищення ефективності в різних сферах нашого буття. Надзвичайно важливим є впровадження електронного документообігу в час розбудови інформаційного суспільства, функціонування технологій електронного управління для забезпечення прозорості відносин «громадянин – держава», «підприємство – держава» та високої якості надання ***державних, комерційних і банківських послуг***.

При інтеграції в Європейський Союз для України дуже актуальними є задачі створення та розвитку національної системи біометричної верифікації і ідентифікації громадян, а також систем виготовлення та обігу ICAO – сумісних на міжнародному рівні електронних документів, включаючи електронні біометричні паспорти.

При функціонуванні вказаних систем через доступ до інформаційних ресурсів здійснюється обробка інформації систем. Під обробкою інформації в системі розуміють виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Достатньо великий досвід застосування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем і різноманітних технологій підтверджує, що в них користувачам і власникам інформації та ресурсів послуги із забезпечення безпеки інформації, що обробляється, повинні надаватись з необхідною якістю. У подальшому під послугами криптографічної системи будемо розуміти послуги цілісності, автентичності (справжності), неспростовності (спостережливості), доступності, конфіденційності та надійності тощо. В суттєвій мірі якість надання вказаних послуг визначається інфраструктурою відкритих ключів (ІВК), тобто використанням асиметричних криптографічних перетворень та криптографічних протоколів, що на них засновуються..

1. Проблемні питання застосування асиметричних криптоперетворень

Серед особливо проблемних питань сьогодні необхідно виділити наступні[4-7] : 1) стандартизація та уніфікація криптографічних примітивів, криптографічних механізмів і

протоколів; 2) узгоджене стандартизоване впровадження ІВК в грід – системи, електронний документообіг, банківські платіжні та комерційні системи, різного призначення інформаційно – комунікаційні системи тощо; 3) подальше теоретичне обґрунтування вимог та умов надання користувачам послуг ІВК з різними рівнями гарантій, та уніфікації; 4) удосконалення та розробка нових методів, механізмів та алгоритмів криптографічних перетворень по критеріям стійкості та складності; 5) прогнозування розвитку, стандартизації, уніфікації та удосконалення міжнародних ІВК; 6) практичне створення та впровадження програмно – технічних комплексів ІВК для основних призначень та уніфікованих; 7) затвердження та введення в дію основних технічних специфікацій відносно форматів даних та протоколів взаємодії тощо.

Найбільшою особливістю асиметричних перетворень є використання асиметричної пари ключів, які містить відкритий ключ,що відомий всім, та особистого ключа, що пов'язаний з відкритим ключем за допомогою певного математичного перетворення. При цьому вважається що обчислення особистого ключа, при знанні загальносистемних параметрів та відкритого ключа, повинно мати в гіршому випадку субекспоненційну складність, за умови коли обчислення відкритого ключа при формуванні асиметричної ключової пари – поліноміальну. У таблиці 1 наведені основні криптографічні перетворення для електронного цифрового підпису(ЕЦП)[5]. У таблиці 2 наведено основні асиметричні крипто перетворення, що застосовуються або можуть застосовуватись для таких криптографічних перетворень як направлене шифрування, , узгодження ключів тощо .

Таблиця 1 - Асиметричні криптографічні перетворення для ЕЦП

Парам-ри перетв-ня / Вид перетв-ня	Особистий ключ	Відкритий ключ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри	Сертифікати	Складність крипто аналізу
Перетворення в кільці (RSA)	Di	Ei	(Ei, Di)	N = PQ	Ei	Субекспоненційна
Перетворення в полі Галуа F(P) (DSA)	Xi	$Yi= g^{Xi}(\text{mod } P)$	(Xi, Yi)	P, q, g	Yi	Субекспоненційна
Перетворення в групі точок еліптичних кривих E(F(q))	di	Qi= diG(modq)	(di, Qi)	a, b, G, n, f(x)(P), h	Qi	Експоненційна
Перетворення в гіпереліптичних кривих	C_i	$D_2= c_iD1$	(ci, D2)	f(x), g(x), q, D1, g, J	D_2	Експоненційна
Перетворення зі спарюванням точок еліптичних кривих	Di = s Q_{iD}	Q_{iD} = H1(ID)	(d_{iD}, Q_{iD})	G1, G2, e, H1, P, H2, H3, F^{2m}, Pp	Q_{iD}	Міжекспоненційна – субекспоненційна

Таблиця 2 - Асиметричні криптографічні перетворення для реалізації направленого шифрування.

Параметри НШ/ Математичний апарат	Особистий ключ НРШ	Відкритий ключ НЗШ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри крипто перетворення	Сертифікати	Складність крипто аналізу
НШ в кільці (RSA)	D_i	E_i	(D_i , E_i)	$N = P\ Q$	E_i	Субекспоненційна
НШ в полі Галуа$F(P)$	X_i	$Y_i=g^X{}_i(\mathrm{mod}\ P)$	(X_i, Y_i)	P, q, g	Y_i	Субекспоненційна
НШ в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i=d_iG(\mathrm{mod}q)$	(d_i, Q_i)	$a, b, G, n, f(x)(P), h$	Q_i	Експоненційна
НШ в гіпереліптичних кривих	C_i	$D_2= c_iD_1$	(c_i, D_2)	$f(x), g(x), q, D_1, g, J$	D_2	Експоненційна
НШ зі спарюванням точок еліптичних кривих	$d_{iD}=s\ Q_{iD}$	$Q_{iD}=H_1(ID)$	(d_{iD}, Q_{iD})	$G_1, G_2, e, H_1, P, H_2, H_3, F_2{}^m, P_p$	Q_{iD}	Експоненційна – субекспоненційна
НШ в кільці зрізаних поліномів (NTRU)	$f = 1+pF(\mathrm{mod}q)$	$h=f^{-1}*g*p(\mathrm{mod}q)$	(f,h)	N, q, p, f, g, df, dg, c		Експоненційна – субекспоненційна

Як випливає з таблиці 2, в якості (сертифіката) відкритого ключа направленого шифрування в RSA системі використовується відкритий Еі ключ із* асиметричної пари ключа (Di, Ei), а в якості особистого (таємного) ключ Di. Для асиметричного криптографічного перетворення в полі Галуа як (сертифікат) відкритого ключа направленого шифрування використовується елемент поля Yi, а як особистий ключ – ціле число Xi.Для асиметричного криптографічного перетворення в групі точок еліптичних кривих як сертифікат відкритого ключа направленого шифрування використовується точка еліптичної кривої Qi, а як особистий ключ електронного цифрового підпису – ціле число di. При застосуванні криптографічного перетворення на гіпереліптичних кривих як сертифікат відкритого ключа використовується якобіан D2, а як особистий ключ – *якобіан D1*. При застосуванні криптографічного перетворення зі спарюванням точок еліптичних кривих як сертифікат відкритого ключа направленого шифрування використовується ключ Q_{iD}, а як особистий ключ – d_{iD}. *Особливий інтерес нині мають ІВК, що ґрунтуються на криптографічних перетвореннях в кільці урізаних поліномів[6 -7].* Основною перевагою цього алгоритму є те, що він працює набагато швидше звичайних алгоритмів направленого шифрування з відкритим ключем, наприклад таких як RSA. Перевага у швидкості є особ-

ливо великою в генерації ключів, яке найчастіше є найбільш важливою частиною у криптографії з відкритим ключем. Для ЕЦП пряме перетворення виконується на особистому ключі, а зворотне на відкритому.

2. Стан створення та застосування ІВК для виготовлення та використання машиночитаємих документів.

В процесі інтеграції України на міжнародному рівні взагалі та в Європейський Союз для України дуже актуальними є задачі створення та розвитку національної системи біометричної верифікації і ідентифікації громадян, а також в цілому систем виготовлення та обігу ICAO – сумісних на міжнародному рівні електронних документів, включаючи електронні біометричні паспорти[8,11,12]. Безумовно важливою та необхідною цієї системи є інфраструктура відкритих ключів (ІВК). Україна в короткий час під загальним керівництвом EDAPS створила та практично ввела в експлуатацію вказану систему, що повністю сумісна на міжнародному рівні. Функціональна схема ІВК системи наведена на рис. 1. В процесі досліджень для ІВК, що наведена на рис. 1,визначено перелік основних загроз , до яких відносяться такі: компрометація змісту об'єкту захисту документу і логічної структури даних; точне копіювання або підміна чипу; скіммінг (зчитування без прямого доступу до паспорта); несанкціонований доступ до чипу паспорту та перехоплення інформації при обміні з терміналом.

Захист від вказаної множини загроз забезпечується засобом застосування таких механізмів захисту: пасивна автентифікація – для захисту від компрометації змісту об'єкту захисту документу і логічної структури даних; активна автентифікація – для захисту від точного копіювання або підміни чипу; розширений контроль даних – для захисту від несанкціонованого доступу; шифрування даних – для захисту додаткових біометричних параметрів.

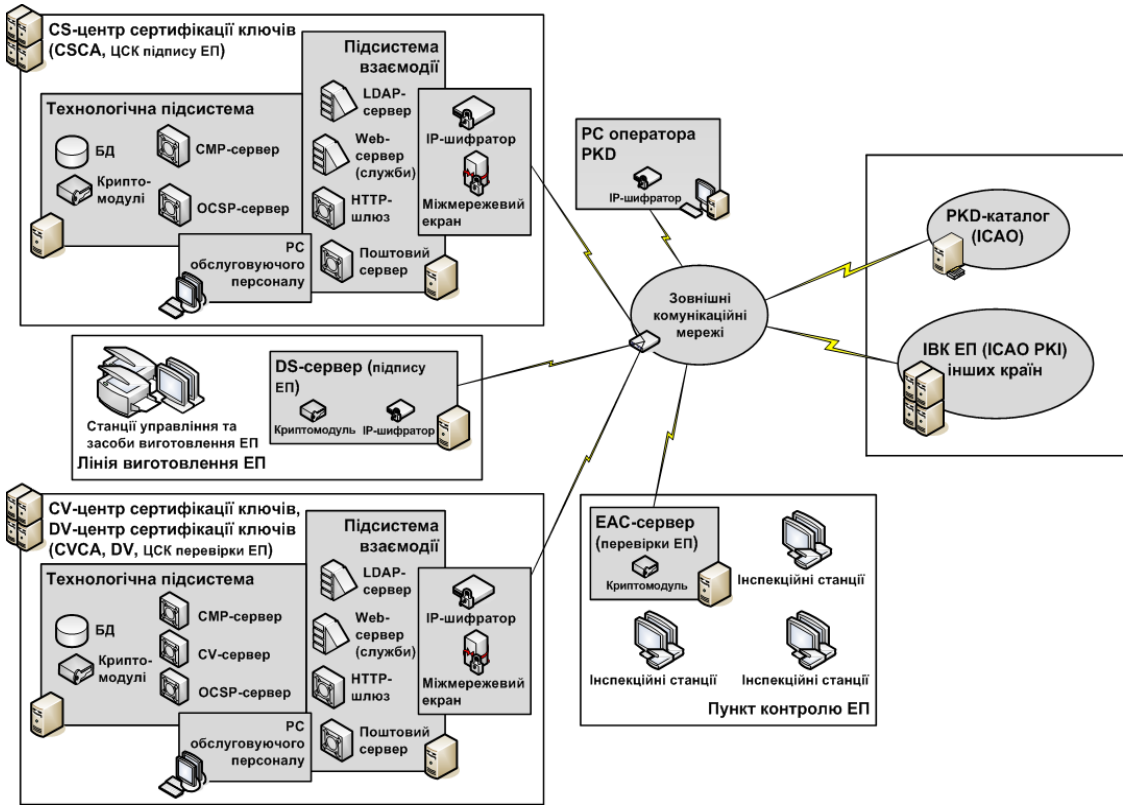


Рис. 1 - Функціональна схема ІВК для біометричного паспорту

Такий вибір не суперечить рекомендаціям та стандартам - ICAO рекомендує застосовувати два механізми перевірки біометричного електронного паспорту – пасивну та активну автентифікацію. Пасивна автентифікація є обов'язковою і призначена для автентифікації даних, які зчитані з електронного паспорту. Вона здійснюється шляхом перевірки підпису на зчитаних даних, використовуючи відповідний сертифікат ЦСК країни, що випустила паспорт. Активна автентифікація є необов'язковою і може використовуватися для перевірки чипу на справжність (автентичність).

Базовий контроль доступу є механізмом автентифікації та призначений для запобігання скіммінгу та перехоплення передачі повідомлень між машино зчитувальним проїзним документом і системою перевірки IS, його застосування є обов'язковою умовою для впровадження розширеного контролю доступу – механізму, що забезпечує захист від несанкціонованого доступу до додаткових біометричних даних.

Безпосередньо ІВК України створюється, як складова частина системи виготовлення та обігу біометричних паспортів у відповідності до технічних вимог ICAO. Її основою є програмно – технічний комплекс. Комплекс та його складові частини повинні відповідати технічним вимогам ICAO та правилам посиленої сертифікації. Він також повинен забезпечити реалізацію регламентних процедур та механізмів функціонування ІВК відносно обслуговування сертифікатів відкритих ключів; надання засобів КЗІ для використання у складових частинах інфраструктури під час виготовлення та перевірки біометричних

Функціональна схема діючого програмно – технічного комплексу наведена на рис. 1. Основними елементами комплексу є: CS-центр сертифікації ключів (CSCA, ЦСК підпису електронних паспортів); CV-центр сертифікації ключів (CVCA, ЦСК перевірки біометричних паспортів) , що суміщений з DV-центром сертифікації ключів (DV, що є версифікатором електронного паспорту; робоча станція (PC) оператора PKD (CIL); DS-сервер (сервер підпису електронних паспортів);EAC-сервер (сервер перевірки біометричних паспортів).

На основі аналізу в процесі розробки визначені вимоги до структури та призначення комплексу технічних засобів CS-ЦСК, вимоги до характеристик комплексу, що наведені у таблиці , вимоги до режимів функціонування комплексу, вимоги до режимів функціонування комплексу та до експлуатації комплексу.

Основні характеристики програмно - технічного комплексу наведені в таблиці 3.

Таблиця 3 – Основні характеристики комплексу.

Показник	Значення
Число одночасних підключень до серверів взаємодії CS-ЦСК та CV/DV-ЦСК – LDAP-каталогу та web-сторінки	не менше 1 000
Час обробки ЦСК запитів на формування, блокування, поновлення та скасування сертифікатів	не більше 1 с (не менше 20 запитів/с)
Час обробки ЦСК запитів на визначення статусу сертифіката	не більше 1 с (не менше 100 запитів/с)
Час формування ЕЦП при підписі даних паспорту	не більше 0.05 с (не менше 20 запитів/с)
Кількість одночасних підключень до серверів взаємодії CS-ЦСК та CV/DV-ЦСК – LDAP-каталогу та web-сторінки)	не менше 1 000
Час обробки ЦСК запитів на формування, блокування, поновлення та скасування сертифікатів	не більше 1 с (не менше 20 запитів/с)
Час обробки ЦСК запитів на визначення статусу сертифіката	не більше 1 с (не менше 100 запитів/с)
Час формування ЕЦП при підписі даних паспорту	не більше 0.05 с (не менше 20 запитів/с)

Для визначення степеню виконання ти функціональних вимог були використані у відповідності до стандарту ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation) [9,10] критерії оцінки електронних проїзних документів. Застосування стандарту ISO/IEC 15408 дозволяє забезпечити умови, в яких процес опису, розробки та перевірки продукту буде проведений з виконанням необхідних вимог. Функціональні вимоги безпеки для біометричних паспортів наведені в таблиці 4.

Таблиця 4 - Функціональні вимоги безпеки для електронних паспортів.

Функціональний клас безпеки	Функціональна складова безпеки
Криптографічна підтримка (FCS)	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1
Конфіденційність (FPR)	FPR_UNO.1
Захист даних користувача (FDP)	FDP_ACC.1, FDP_ACF.1, FDP_RIP.1, FDP_UCT.1, FDP_UIT.1
Ідентифікація та автентифікація (FIA)	FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.1
Менеджмент безпеки (FMT)	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.3, FMT_SMF.1, FMT_SMR.1
Захист TSF (FPT)	FPT_FLS.1, FPT_ITI.1, FPT_RVM.1, FPT_SEP.1, FPT_TST.1

Таким чином в цілому функціональні вимоги до електронного біометричного паспорту, в найбільш прийнятній формі можна задати при використанні стандарту ISO/IEC 15408.

3. Сутність та застосування ІВК в АБС банків.

ІВК є також основою для надання усіх вказаних вище послуг в банківських системах, перше за все в системах Клієнт – Сервер. Спосіб використання засобів реалізації ІВК для таких систем наведено на рис. 2. Функціональна схема ЦСК наведена на рис.3. Важливими є також питання, що пов’язані з використанням криптографічних систем та механізмів, а також криптографічних протоколів та технічних специфікацій. Вказані дані наводяться нижче.

Рис. 2 - Використання засобів КЗІ

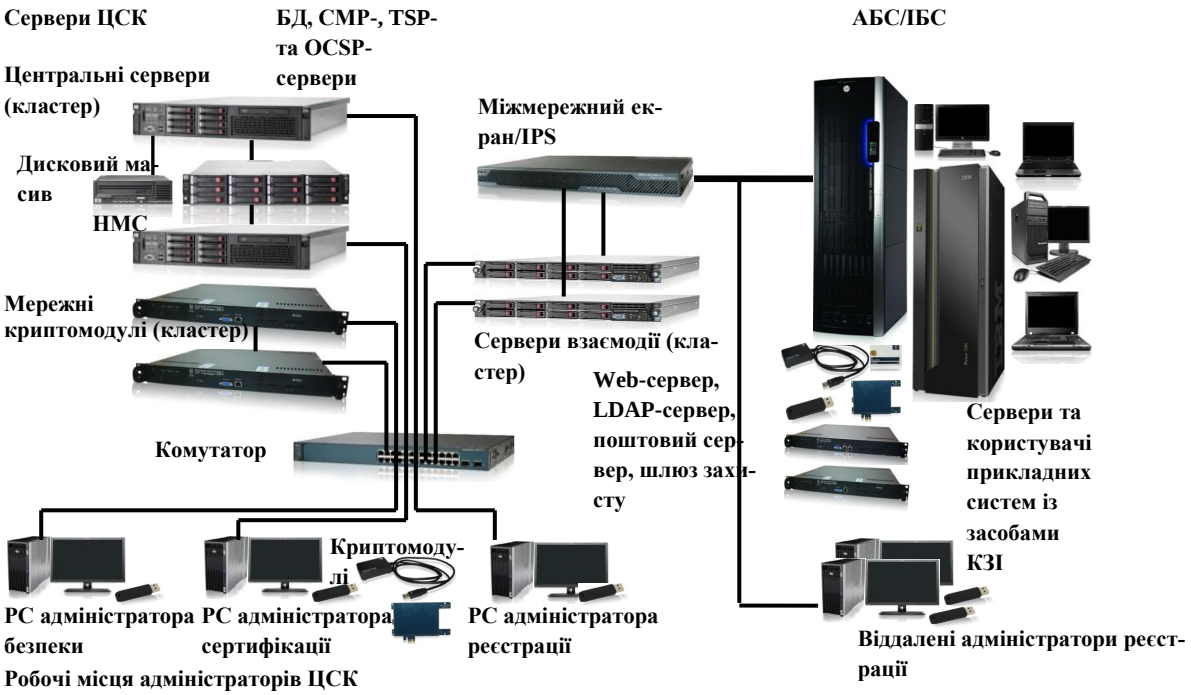


Рис. 3 - Функціональна схема ЦСК банку

Основними елементами центру сертифікації ключів є такі:

– Програмний комплекс ЦСК “ІІТ ЦСК-2” (програмні комплекси центрального сервера взаємодії, адміністраторів ЦСК та віддаленого адміністратора реєстрації).

– Програмний комплекс користувача ЦСК “ІІТ Користувач ЦСК-2” (засоби електронного цифрового підпису, шифрування та автентифікації, у т.ч. бібліотека користувача ЦСК).

– Апаратні криптомодулі “Гряда-52” та “Гряда-61”.
– Мережний криптомодуль “Гряда-301”.
– Електронний ключ “Кристал-1”.
– Старт-карта “Гряда-301”.

Криптографічні алгоритми та протоколи:
– Шифрування за ДСТУ ГОСТ 28147:2009.
– Електронний цифровий підпис (ЕЦП) за ДСТУ 4145-2002.
– Гешування за ГОСТ 34.311-95.
– Протокол розподілу ключових даних за ДСТУ ISO/IEC 15946-3 та державних технічних специфікацій.
– Протокол взаємної автентифікації за ДСТУ ISO/IEC 9798-3.
– Шифрування TDEA та AES за ISO/IEC 18033-3.
– ЕЦП RSA за ISO/IEC 14888-2:2008 та PKCS#1, DSA за ISO/IEC 14888-3 та ECDSA за ISO/IEC 15946-2.
– Протоколи розподілу ключових даних DH за ISO/IEC 11770-3:2008 та ECDH за ISO/IEC 15946-3.
– Гешування SHA за ISO/IEC 10118-3:2004.

Формати даних та протоколи взаємодії:
– Сертифікати та списки відкликаних сертифікатів (СВС) згідно ISO/IEC 9594-8 та державних технічних специфікацій.
– Протокол OCSP (визначення статусу сертифіката) згідно RFC 2560 та державних технічних специфікацій.
– Протокол TSP (фіксування часу) згідно RFC 3161 та державних технічних специфікацій.
– Підписані дані (дані з ЕЦП) згідно ETSI TS 101 733 (CAdES), RFC 5652 та державних технічних специфікацій.
– Захищені дані (зашифровані дані) згідно RFC 5652 та державних технічних специфікацій.
– Особисті ключі згідно PKCS#8 та PKCS#12.

Засоби захисту АБС на платформі SAP for banking.
Забезпечують у складі АБС:
– цілісність та неспростовність авторства електронних даних та документів, що циркулюють у системі;
– автентифікацію користувачів АБС та конфіденційність і цілісність даних, які передаються між користувачами та сервером системи.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у АБС, реалізуються шляхом формування та перевіряння ЕЦП від даних та документів, як на стороні користувача АБС (SAP-клієнта) так і на стороні сервера (SAP-сервера).

Аутентифікація користувачів АБС (SAP-клієнтів) на сервері (SAP-сервері) здійснюється під час підключення користувачів до сервера (встановлення з’єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером АБС під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Засоби захисту ІБС на платформі Oracle Flexcube.
Забезпечують у складі ІБС:

– цілісність та неспростовність авторства електронних даних та документів, що циркулюють у системі;

– автентифікацію користувачів ІБС та конфіденційність і цілісність даних, які передаються між користувачами та сервером системи.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у ІБС, реалізуються шляхом формування та перевіряння ЕЦП від даних та документів, як на стороні користувача ІБС (FlexCube-клієнта - web-оглядача) так і на стороні сервера (FlexCube-сервера).

Автентифікація користувачів ІБС (FlexCube-клієнтів - web-оглядачів) на сервері (FlexCube-сервері) здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером через шлюз захисту) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером ІБС (шлюзом захисту) під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум даних TCP-з'єднання.

4. Основні напрями розвитку та удосконалення ІВК.
Перспективна система шифрування на основі NTRU.

В середині 1990-х років групою математиків (ДжефріХовстейн, ДжиллПіфер та Джозеф Сильверман) було розроблено новий алгоритм який отримав назву NTRU[6,7]. В 1998 році було опубліковано повний опис алгоритму та його аналіз Основною перевагою цього алгоритму є те, що він працює набагато швидше звичайних алгоритмів з відкритим ключем, таких як RSA. Перевага у швидкості є особливо великою в генерації ключів, яке найчастіше є найбільш важливою частиною у криптографії з відкритим ключем. Розглянемо ідеї, що лежать в основі NTRU для застосування при направленому шифруванні та цифровому підписі.

У алгоритмі NTRU усі операції здійснюються в кільці усічених многочленів. Криптографічна стійкість алгоритму заснована на складності вирішення задачі знаходження короткого вектора у заданій решітці. NTRU працює, як вже згадувалось, швидше ніж криптосистеми з відкритим ключем, які застосовуються зараз. Для за шифрування та розшифрування повідомлення довжиною з N символів необхідно $O(N^2)$ операцій для крипто системи, в той час як для RSA потрібно $O(N^3)$ операцій. В таблиці 5 наведені основні параметри NTRU

Таблиця 5 - Параметри основного алгоритму

Параметр	Коротке пояснення параметру
N	Розмір усіченого кільця многочленів R. Елементи кільця представлені у вигляді поліномів ступеня N – 1(не секретний)
q	Великий модуль по якому приводиться кожний коефіцієнт многочлена у кільці R (не секретний)
p	Малий модуль по якому приводиться кожний многочлен (не секретний)
f	Многочлен, який є секретним ключем
g	Многочлен, який використовується для генерації публічного ключа h з f (секретний але відкидається після першого використання)
h	Публічний ключ, теж многочлен
r	Випадковий «забілюючий» многочлен (секретний але відкидається після першого використання)
df	f має df коефіцієнти еквівалентні 1 та df-1 коефіцієнти еквівалентні - 1
dg	g має dg коефіцієнти еквівалентні 1 та dg коефіцієнти еквівалентні - 1
dr	r має dr коефіцієнти еквівалентні 1 та dr коефіцієнти еквівалентні - 1

Основною перевагою, в тому числі і відносно криптосистем на еліптичних кривих, є можливість підвищення швидкодії на 2 – 3 порядки.

Основні проблемні питання розвитку системи ЕЦП України

В якості першочергових потрібно вирішити такі завдання:

- створення та застосування у існуючих та перспективних системах ІВК, сумісних з Європейськими та міжнародними;
- забезпеченням необхідних рівнів гарантій надання послуг з безпеки інформації;
- використанням досвіду технологічно розвинених держав, Європейської та міжнародної стандартизації, уніфікації тощо;
- поставка замовникам уніфікованих елементів ІВК та центрів сертифікації різного призначення та можливостей;
- надання користувачам послуг ІВК з вищим (апаратним) та середньо апаратним рівнями гарантій згідно ISO/IEC 15408;
- уніфікація та стандартизації національної ІВК, включаючи національну систему ЕЦП;
- удосконалення методів та алгоритмів криптографічних перетворень по критерію мінімізації складності операцій;
- розвиток математичних методів та систем крипто аналізу, прогнозування вимог і умов та обмежень відносно застосування стандартизованих криптографічних примітивів та криптографічних протоколів, їх удосконалення;
- дослідження та прогнозування розвитку та удосконалення міжнародних ІВК, врахування їх досвіду та результатів, гармонізація національної системи ЕЦП з міжнародними ІВК та ІВК технологічно розвинених держав.

При урахуванні вказаних пропозицій появиться можливість:

- вирішити низку наукових та практичних задач розвитку теорії та практики побудування ІВК, в тому числі система ЕЦП України як для внутрішньо державного так і міжнародного застосувань;
- отримати методики та засоби обґрунтування вимог, експериментального та практичного дослідження алгоритмів та засобів ЕЦП та порівняння існуючих стандартів ЕЦП;
- розробити методи та системи оцінки стійкості криптографічних перетворень в групах точок еліптичних та гіпереліптичних кривих, а також зі спарюванням точок еліптичних кривих;
- впровадити технічні специфікації відносно форматів даних та протоколів взаємодії в системі ЕЦП у відповідності з міжнародними вимогами;
- розробити апаратні засоби КЗІ, які будуть забезпечувати вищий рівень гарантій та можливість відображення політики на міжнародному та міждержавному рівнях;
- економічно обґрунтована ІВК, включаючи декілька засвідчувальних центрів та сукупності АЦСК та ЦСК , а також узгоджене впровадження системи відокремлених пунктів, включно до районних адміністративних одиниць;
- розробити та впровадити науково - обґрунтовану систему підготовки та перепідготовки спеціалістів, що задіяні в обслуговуванні, розробці, проведенні експертизи та експлуатації системи ІВК (ЕЦП);

Впровадження вказаних пропозицій дозволить створити в Україні конкурентоспроможні елементи і безпосередньо систему ІВК для усіх існуючих застосувань, яка за своїми характеристиками, в першу чергу рівнем гарантій надання послуг та криптографічної стійкості криптографічних примітивів, що будуть застосовуватись, що будуть відповідати міжнародним вимогам.

Література:

1.Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.

2.Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
3.Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.
4.ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8:2006»Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів. ».
5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010, 593с.
6. Joseph H. Silverman, Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem, NTRU Cryptosystems Technical Report 13, available at http://www.ntru.com.
7. J. H. Silverman and W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt. Technical Report #18
8. ICAO9303-pt1-vol2.
9. ISO/IEC 15408: 2000 – Information technology – Security techniques – Evaluation criteria for IT security. Part 1-3.
10. FIPS-186-3 - Information Technology Laboratory - National Institute of Standards and Technology - Digital Signature Standard (DSS), 2006.
11. Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents - Exended Access Control (EAC),Password Authenticated Connection Establishment (PACE)and Restricted Identification (RI), Version 2.05, TR-03110, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2010. 9
12. ePassport Protection Profile V1.0, National Intelligence ServiceIT Security Certification Center

СИСТЕМА ЗВ'ЯЗКУ З ШИФРУВАННЯМ ДАНИХ ПСЕВДОВИПАДКОВИМИ ПОСЛІДОВНОСТЯМИ ТА КОДУВАННЯМ КАНАЛУ КОДАМИ ХЕМІНГА

Політанський Р.Л., Політанський Л.Ф., Шпатар П.М, Іванюк П.В.
Чернівецький національний університет ім. Юрія Федьковича.
Кафедра радіотехніки та інформаційної безпеки
58000, Чернівці, вул.. Сторожинецька 101, +38(0372)24-24-36
E-mail: shpatar@ukr.net

A system of digital communication with encryption of pseudo-random sequences and coding channel of Hamming code is presents in this paper. The impact coding on synchronization of transmitting and receiving parts of the system for a channel with additive white Gaussian noise (AWGN-channel) has been investigated.

Перспективним напрямком розвитку засобів зв'язку є використання широкосмугових систем, функціонування яких базується на великих ансамблях малокорельованих між собою сигналів, формування яких здійснюється зокрема на основі псевдовипадкових послідовностей. Актуальним питанням залишається вплив завад у каналі зв'язку на процес синхронізації приймальних та передавальних частин системи.

Проблемам синхронізації присвячені актуальні роботи вітчизняних та зарубіжних авторів. Так у роботі [1] автор здійснює класифікацію методів синхронізації, виділяючи 2 основні види синхронізації: синхронізація в синхронних системах і старт-стопових системах. Розвиток сучасних систем супутникового зв'язку актуалізував проблему старт-стопової синхронізації. Це пов'язано з часовими вікнами прийому-передачі у роботі одного супутника.

Синхронізацію приймальних та передавальних частин системи можна здійснювати використовуючи властивість самосинхронізації псевдовипадкових послідовностей [2]. На тривалість часу синхронізації значний вплив проявляють шуми, притаманні каналам зв'язку [2]. Можна очікувати, що оброблення синхроімпульсів кодерами кодування каналу зменшуватиме тривалість часу синхронізації за рахунок зменшення ймовірності помилкових канальних бітів. Застосування завадостійкого кодування в цифрових системах передавання даних також дозволяє покращити інші важливі властивості систем передавання даних[1]: отримати енергетичний виграш кодування, підвищити швидкість передачі даних, досягти економії смуги пропускання.

Суть алгоритмів генерування псевдовипадкових послідовностей бітів, що називаються картами хаосу, полягає в наступному.

Нехай задана множина дійсних чисел X, на якій визначена міра належності, що розділяє її на дві підмножини X_0 та X_1 (у нашому випадку X_0=(0;1/2]; X_0=(1/2;1]), а також задана послідовність дійсних чисел $x_n \in (0;1)$ з алгоритмом отримання наступного біту послідовності, що описується співвідношенням:

$$b_n = \begin{cases} 0, \text{якщо } x_n \in X_0 \\ 1, \text{якщо } x_n \in X_1 \end{cases}. \quad (1)$$

Таким чином можливо отримати послідовність бітів необхідної довжини:

$$B(x_0) = \{b_1(x_1), b_2(x_2), \ldots, b_n(x_n)\}. \quad (2)$$

Приведемо рекурентне співвідношення, що описує послідовність x_n, і яке використовуються для генерування псевдовипадкової послідовності бітів з хорошими властивостями:

$$x_n = \sin^2\left(2^n * \arcsin\left(\sqrt{x_0}\right)\right), \quad (3)$$

де n – порядковий номер (n=0,1,2,…), x_0 – початковий елемент послідовності з проміжку дійсних чисел (0;1).

Як бачимо з рівняння (3), на з ростом n виникають ускладнення в зв'язку з обчисленням числа 2^n. Тому системах, які фізично можливо реалізувати необхідно визначити

верхнє значення порядкового номера послідовності N_{max}. Після досягнення цього значення починаємо визначення послідовності x_n з першого елемента послідовності. Таким чином отримаємо періодичну двійкову послідовність з періодом N_{max}.

Шифрування повідомлення здійснюватимемо співвідношеннями (1), (2), (3). Елементи інформаційного повідомлення сумуємо з елементами псевдовипадкової послідовності, використовуючи операцію XOR (4).

$$x_i = m_i \oplus b_i \,. \tag{4}$$

Далі повідомлення розділяємо на блоки по k біт ($x_i \rightarrow x_{(k)}$). Послідовність на виході кодера Хемінга (n,k), що передається у канал зв'язку, знаходиться за допомогою формули (5):

$$x_{(n)} = x_{(k)} * G_{(n,k)} \tag{5}$$

де $x_{(k)}$ – інформаційна послідовність довжиною k біт, $x_{(n)}$ – кодовий символ довжиною n біт, $G_{(n,k)}$ – генерувальна матриця коду (n,k).

Вплив на синхронізацію шуму в каналі з адитивним гаусовим шумом був досліджений у роботі [2]. Автори [2] дослідили залежність часу синхронізації від значення відносної величини шуму в каналі.

Робота запропонованої схеми була змодельована у середовищі MatLab. Аналіз роботи схеми показав, що додавання шифруючого сигналу не впливає на такий показник системи, як залежність ймовірності помилки у прийнятій послідовності від співвідношення сигнал/шум (рис. 1).

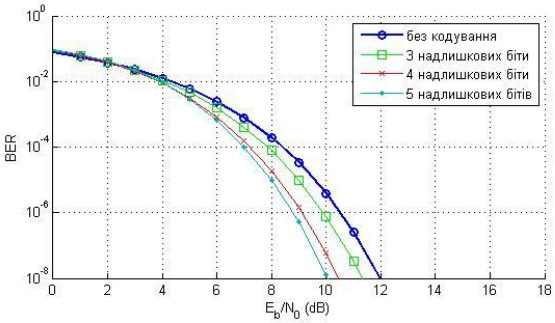


Рис. 1. Залежність бітової помилки в каналі для кодів різної довжини при різних відношеннях сигнал/шум

Провівши аналіз та дослідження схеми синхронізації за допомогою імпульсів, що відповідають псевдовипадковим послідовностям бітів, автори прийшли до висновку, що доцільно використовувати кодування Хемінга з метою покращення процесу синхронізації.

За основу визначення тривалості часу синхронізації ми вибрали час передавання такої кількості імпульсів, яка визначається мінімально необхідною кількістю біт відповідної ПВП для ідентифікації та визначення значення параметру генерування x_0 (на рис.3 цей час позначено T_1).

Якщо в каналі мають місце імпульсні завади, кількість імпульсів у синхронізуючому сигналі повинна бути збільшена на кількість інвертованих у каналі імпульсів.

Якщо в каналі є імпульсні завади, то ймовірність помилки канального біта дорівнює p. Для модуляції BPSK ця ймовірність [4] може бути виражена за допомогою формули (6):

$$p = Q\left(\sqrt{2 \cdot \frac{E_b}{N_0}}\right) \tag{6}$$

У формулі (6) Q-інтеграл помилок ($Q(x) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_x^{\infty} e^{-u^2/2} du$), E_b – енергія біта інформації, N_0 – потужність шуму в каналі.

Для оцінювання часу синхронізації потрібно крім довжини послідовності оперувати швидкістю передачі бітів. Для розрахунків приймемо значення R = 1 Мбіт/с [4]. Тоді зменшення часу синхронізації визначимо за формулою (7):

$$\Delta t_c = \left(\tilde{n}_0 - \tilde{n} \right) \Big/ R \qquad (7)$$

Графіки залежності мінімальної довжини послідовності, необхідної для синхронізації, приведені на рис. 2.

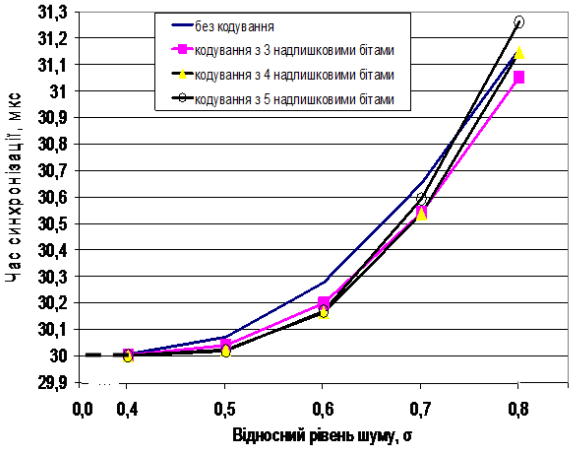


Рис. 2. Залежність часу синхронізації при використанні надлишкового кодування і без кодування.

Отримані результати дещо відрізняються від тих, що отримані в [2]. Так, у нашій роботі час синхронізації починає збільшуватися внаслідок шуму при σ = 0.4, тоді як у роботі [2] автори приводять значення 0.3.

З отриманих залежностей видно, що використання відносно простих схем лінійного блокового кодування призводить до зменшення часу синхронізації на рівні 0,2 мкс при значеннях σ, що знаходиться у межах від 0.4 до 0,7. Кількість надлишкових бітів при такому кодуванні не призводить до помітного підсилення ефекту.

Література:

1. Хома В. В. Основи збору, передачі та оброблення інформації / В.В. Хома. – Львів: Видавництво Львівської політехніки, 2007. – 312с.

2. Andreyev, Yu. CDMA communications using maps with stored information / V. Yu. V. Andreyev, A. S. Dmitriev, D. A. Kuminov, and S. O. Starkov // European Conference on Circuit Theory and Design. Budapest. – 1997.

3. Ємець, В Сучасна криптографія. Основні поняття / В. Ємець, А.Мельник, Р. Попович – Львів: БаК, 2003. – 144 с.

4. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом “ Вильямс” – 2007. – 1104с.

5. Мандзій, Б. А. Основи теорії сигналів / Б.А. Мандзій, Р.І. Желяк. –І Львів: Ініціатива, 2008.

ЗАХИСТ ПРИМІЩЕНЬ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

Медвідь М.О., Федюшин А.Ю.
Національний технічний університет України «Київський політехнічний інститут» Фізико-технічний інститут
Кафедра фізико-технічних засобів захисту інформації
03056, м. Київ, пр. Перемоги, 37 e-mail: antonio86@ukr.net

The main object of the thesis is the expansion of calculating of sound insulation method and calculation of sound insulation homogeneous wall at all the normalized frequency range.

As a result of sound insulation researching, acoustic resonances were detected which causing the effect of sound transparency.

Based on the results, it is necessary to execute additional calculations of sound insulation and measure one not only for the octave frequencies, but also at intermediate frequencies of the normalized frequency range.

Інформаційна безпека відіграє ключову роль у забезпеченні життєво важливих інтересів будь-якої країни. Створення розвиненого і захищеного інформаційного середовища є основною умовою розвитку сучасного суспільства, оскільки саме через неї реалізуються загрози національної безпеки в різних сферах діяльності держави.

Успішне функціонування й розвиток підприємств усе більше залежить від подальшого вдосконалення їхньої діяльності в області забезпечення інформаційної безпеки в сфері виробництва, бізнесу й підприємництва.

Необхідність і важливість проведення заходів щодо захисту приміщень від витоку мовної інформації по віброакустичним каналах надзвичайно актуальна не тільки при виконанні регламентованих вимог щодо захисту виділених приміщень, у яких обробляється інформація, яка є конфіденційною, або ведуться конфіденційні перемови [1, 2]. Залежно від режиму забезпечення границь контрольованої зони захист інформації від витоку акустичними і віброакустичними каналами має специфічні особливості й обмеження, які необхідно враховувати при реалізації методів ефективного захисту. Застосування активних методів захисту інформації від витоку акустичними каналами у більшості ситуацій пов'язане з виникненням акустичних шумів, які знижують комфортність роботи у приміщенні, що захищається та суміжних приміщеннях.

Для попередньої оцінки звукоізоляції приміщення частіше за все користуються нормативною документацією, а також параметрами звукоізоляції на октавних частотах. В той час немає гарантії, що на інших частотах звукоізоляція буде такою ж як і на октавних частотах.

Таким чином метою дослідження є розширення відомої методики розрахунку звукоізоляції [4] та розрахунок звукоізоляції однорідної стіни у всьому нормованому діапазоні частот.

Для дослідження була проведена модернізація методики [4], після чого розрахована звукоізоляція однорідної стінки для сучасних будівельних матеріалів (цегла, залізобетонна панель).

Розрахунок звукоізоляції стіни проводився за формулою 1.

$$Q = 10\lg[\cos^2(2\pi h\cos\theta/\lambda) + \frac{1}{4}(z/z_0 + z_0/z)^2\sin^2(2\pi h\cos\theta/\lambda)] \qquad (1)$$

де

$z = \rho c/\cos\theta$, $z_0 = \rho_0 c_0/\cos\theta_0$ – акустичний імпеданс матеріалу та навколишнього середовища відповідно,

ρ, ρ_0 – щільність матеріалу та навколишнього середовища відповідно,

c, c_0 – швидкість звуку у матеріалі та навколишньому середовищі відповідно,

h – товщина стіни,

θ – кут падіння акустичної хвилі на стіну до нормалі,

λ – довжина звукової хвилі.

На базі формули було отримано залежність власної звукоізоляції від частоти у нормованому діапазоні частот. Графік залежності звукоізоляції від частоти наведено на Рис.1.

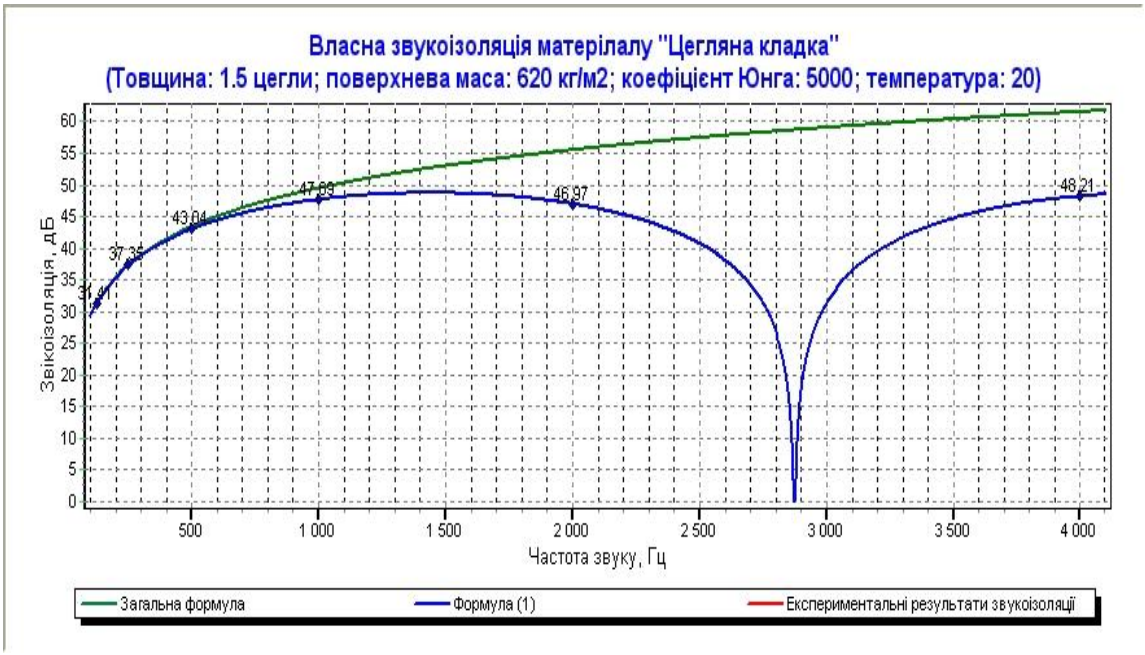


Рис.1 – Власна звукоізоляція цегляної кладки товщиною у 1.5 цеглини.

Для цегляної кладки товщиною від 1.5 цеглини при використанні формули (1) на деяких частотах звукоізоляція знижується до 0. Даний ефект в акустиці має назву ефект звукопрозорості. Для цегляної кладки у 1.5 цеглини частота на якій виникає ефект звукопрозорості – $f = 2875\,\text{Гц}$; для кладки у 2 цеглини – $f = 2210\,\text{Гц}$.

Для залізобетонної стінки товщиною 30 см ефект звукопрозорості виникає на частоті $f = 5830\,\text{Гц}$. В результаті проведених досліджень можна зробити наступні висновки:

1. Значне зниження звукоізоляції на окремих частотах може бути використано як канал витоку інформації, що необхідно враховувати при проектуванні приміщення.

2. Так як ефект звукопрозорості виникає поза октавними частотами, а методики оцінки звукоізоляції використовують тільки октавні частоти, то розрахунок та вимірювання звукоізоляції реальних стін необхідно проводити не тільки на октавних частотах, а і на проміжних, з метою знаходження резонансних частот, на яких виникає необхідність додаткової звукоізоляції.

3. Представляється необхідним у діючу методику внести уточнення пов'язані з виявленням резонансів, пов'язаних з ефектом звукопрозорості.

Література:

1. Каргашин В. Л. Проблемы активной защиты виброакустических каналов//Специальная техника, 1999, № 6.

2. Хорев А. А., Макаров Ю. К. К оценке эффективности защиты акустической (речевой) информации//Специальная техника, 2000, № 5

3. Справочник по акустике/Иофе В.К., Корольков В.Г., Сапожков М.А./Под ред.. М.А. Сапожкова. – М: Связь, 1979. – 312 с.

4. СНиП 23-03-2003 «Защита от шума»

5. Нурумов Р.Б., Омаров С.С., Бегимов Т.Б. Расчет звукоизоляции от воздушного шума однослойными массивными железобетонными и пазогребневыми гипсовыми конструкциями //ҚАЗҰТУ ХАБАРШЫСЫ – ВЕСТНИК КАЗНТУ, 2009, №3 (73)

АНАЛИЗ ВОЗМОЖНОСТИ УТЕЧКИ ЗАКРЫТОЙ ИНФОРМАЦИИ ЧЕРЕЗ ИНТЕРФЕЙС D-SUB

Бовкун А.Н.
Центральный научно-исследовательский институт
вооружения и военной техники Вооруженных Сил Украины
03049 Киев, пр. Воздухофлотский, 28, тел (044) 520-12-84,
E-mail: a.n.bovkun@gmail.com, факс (044) 520-12-84

In the report possibility of leak of the confidential information on technical channels is considered. The basic attention is given collateral electromagnetic radiation at data transmission from the system block of the computer to the monitor on interface D-Sub.

Введение. На современном этапе широкое распространение находит экономический и промышленный шпионаж, не связанный непосредственно с межгосударственными, политическими и военными противоречиями. Главной причиной возникновения промышленного (экономического) шпионажа является конкуренция между фирмами, компаниями и предприятиями. Промышленный шпионаж охватывает сегодня все сферы рыночной экономики, и в современных условиях мировой экономики его масштабы резко возрастают.

Важнейшая роль в достижении информационного господства отводится виртуальному шпионажу — шпионажу, ведущемуся в информационных потоках, которые в гигантских количествах производятся предприятиями всех видов собственности и отдельными физическими лицами.

В настоящее время на подавляющем большинстве предприятий и организаций для обработки и хранения закрытой информации широко используются электронно-вычислительные машины (ЭВМ). В результате ЭВМ становятся носителями важной информации, а следовательно важным объектом для промышленного шпионажа. Существенную опасность с точки зрения утечки закрытой информации, циркулирующей в ЭВМ и локальных вычислительных сетях (ЛВС) представляют технические каналы, возникающие при функционировании средств как в составе ЛВС так и отдельных ЭВМ.

Наиболее уязвимыми элементами ЭВМ как объекта технической разведки являются:

- центральный процессор;
- запоминающие устройства;
- система ввода-вывода данных;
- аппаратура сопряжения;
- каналы связи;
- оконечные устройства.

Утечка информации возможна по следующим техническим каналам:

- побочное электромагнитное излучение ЭВМ и ЛВС;
- наводки информационных сигналов по цепям питания, заземления и т.д.;
- наводки на посторонние провода и кабели, проходящие в непосредственной близости от ЭВМ и ЛВС, но не связанные с ними;
- и другие.

На предприятиях и организациях для защиты информации от несанкционированного доступа разрабатывается ряд организационных, организационно-технических и технических мероприятий. Проведение этих мероприятий существенно затрудняет или исключает возможность снятия информации средствами разведки по техническим каналам утечки информации.

Однако непрерывное развитие и совершенствование средств и методов цифровой обработки сигналов расширяют возможности аппаратуры разведки.

В частности представляет интерес возможности снятия текстовой информации отображаемой на мониторе ЭВМ.

Основная часть. В настоящее время на категорированных объектах находятся средства обработки закрытой информации прошедшие сертификацию в специализированых лабораториях. В своей основе эти средства состоят из ЭВМ, так называемого, «офисного плана». Они характеризуются применением надежных, дешевых решений. В составе этих ЭВМ могут использоваться мониторы выполненные как по технологии CRT (только аналоговые интерфейсы передачи данных) так и LCD (аналоговые и цифровые интерфейсы передачи данных). Однако графические адаптеры этих компьютеров преимущественно встроенные и используют аналоговый интерфейс D-Sub.

Характерной особенностью интерфейса D-Sub является передача сигналов от системного блока к монитору в аналоговом виде по трем сигнальным каналам (RGB) и двум каналам синхронизации развертки.

Текстовая информация передаваемая на монитор характеризуется статичностью. Ее время обновления может достигать нескольких десятков минут. При этом информация на экране монитора отображается с использованием двух крайних уровней — уровня черного (текст) и уровня белого (фон). Следовательно, передаваемые по каналам RGB интерфейса D-Sub мгновенные значения сигналов практически идентичны. Сигналы синхронно и скачкообразно изменяются от своего минимального значения к максимальному и наоборот. Фактически в проводниках интерфейса от системного блока к монитору циркулирует периодический импульсный сигнал. Период повторения сигнала равен периоду кадровой развертки монитора (рис.1).

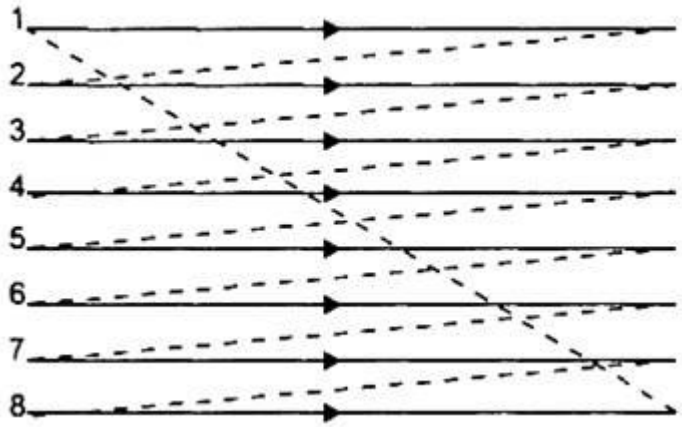


Рис. 1. Принцип формирования кадра на CRT – мониторе.

Таким образом, обнаружение побочных электромагнитных излучений CRT-монитора можно рассматривать как обнаружение пачки одинаковых по форме импульсов.

Особенностью такого подхода является возможность применения накопления сигнала в средствах разведки действующим по побочным каналам электромагнитного излучения.

При использовании стандартной частоты развертки монитора 60 Гц, и времени накопления сигнала 2,5 … 3 минуты на обработку поступает порядка 10000 кадров. В зависимости от частоты кадровой развертки монитора и времени статичного отображения текстовой информации на экране монитора, количество обрабатываемых (накапливаемых) кадров определяется соотношением $N = F \cdot T$, где F — частота кадровой развертки монитора, а T — время статичного отображения информации на экране монитора.
При этом выигрыш в энергетике для разных N приведен в таблице 1.

Таблица 1.

Выигрыш в энергетике принимаемого сигнала [дБ]
в зависимости от числа накапливаемых кадров

N	Когерентное накопление	Некогерентное накопление
10	10	8
100	20	15,5
10000	40	40

Вывод. Использование современной цифровой аппаратуры шпионажа для обработки сигналов принимаемых по побочным каналам электромагнитного излучения, позволяет реализовать время накопления сигнала от нескольких секунд до нескольких десятков минут. Это позволяет при определенных условиях произвести скрытое снятие закрытой информации передаваемой от системного блока компьютера к монитору по интерфейсу D-Sub даже при проведении стандартных мероприятий по защите от несанкционированного допуска организационного, организационно-технического и технического плана.

Литература:

1. Зверев В.А., Стромков А.А. Выделение сигналов из помех численными методами. – Нижний Новгород: ИПФ РАН, 2001. – 188 с.
2. Меньшаков Ю.К. Защита объектов и информации от технических средст разведки. М.: Российск.гос.гуманит.ун-т, 2002. – 399 с.
3. Теоретические основы радиолокации. Под ред. Ширмана Я.Д. Учебное пособие для вузов. М.: изд-во «Советское радио», 1970 – 560с.
4. Кузьмин С.З. Цифровая радиолокация. Введение в теорию. – К.: КВіЦ, 2000. – 428 с.
5. Бабак В.П. та ін. Обробка сигналів: Підручник. – 2-е вид., перероб. і доп. – К.: Либідь, 1999. – 496 с.

ПРАКТИЧЕСКИЕ ОСОБЕННОСТИ УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

А.О. Дугин
Украинский научно-исследовательский институт связи
03680, Киев, ул. Соломенская, 3
Email: andrew.dugin@gmail.com

There are practical aspects of intrusion detection and prevention systems infrastructure design and operation described in the article. The traffic analysis results may be used for information systems management. Methods described were used in the corporate environment with deep packet inspection of corporate traffic.

Введение

Одним из показателей работы инфраструктуры организации является сетевой трафик, вырабатываемый пользователями и серверами, а также служебный трафик активного сетевого оборудования. В крупных организациях общий объем передаваемых по сети данных настолько велик, что для проведения его анализа и использования результатов, в зависимости от целей, необходимо использование мощных анализаторов, систем определения сетевых аномалий, систем обнаружения и предотвращения вторжений и других типов сетевых сенсоров.

На этапе проектирования инфраструктуры анализа сетевого трафика, систем обнаружения вторжений необходимо правильно рассчитать пропускную способность интерфейсов коммутаторов, на которые «зеркалируется» трафик, с целью принятия решения об использовании на каждом участке сети сенсора определенной мощности и, соответственно, стоимости. На стадии внедрения определяется соответствие заявленных поставщиком характеристик сетевых сенсоров реальности с учетом специфики данной корпоративной сети, также может возникнуть необходимость реорганизации инфраструктуры в связи с ошибками проектирования. На этапе эксплуатации необходимо использование возможности анализа трафика для получения информации о текущем состоянии корпоративной сети, возможных произведенных без согласования реорганизациях инфраструктуры либо авариях, а также принятия решения о методах решения возможных ошибок проектирования и внедрения.

Определение пропускной способности

Глубокий анализ сетевого трафика системами обнаружения вторжений, как правило, производится без возможности потенциального влияния на сетевые сервисы. Это связано с тем, что специфичные бизнес-приложения могут генерировать трафик, который может быть распознан сенсорами как вредоносный. Реже используются системы предотвращения вторжений в режиме inline IPS (Intrusion Prevention Systems) либо с возможностью внедрения в TCP-сессию и принудительного ее разрыва. Необходимость установки сетевых сенсоров в режиме IDS (Intrusion Detection System) или IPS определяется корпоративной политикой защиты сети передачи данных. В зависимости от поставленных задач, применяется анализ полной копии всех пакетов либо информации о каждом установленном сетевом соединении/обмене. Полная копия пакетов, обрабатываемых управляемым коммутатором, направляется на выделенный «зеркалированный», или SPAN (Switched Port Analyzer) порт, к которому подключается сетевой сенсор. В зависимости от производителя, версии аппаратной платформы и программного обеспечения коммутатора, может применяться выборочное копирование трафика:

- определенных физических интерфейсов
- определенных логических интерфейсов
- соответствующего условиям списка доступа (Access Control List).

Для эффективного анализа пропускная способность SPAN-порта и, соответственно, сетевого сенсора, должна быть не менее пиковой суммарной нагрузки на анализируемые интерфейсы.

Предположим, существует коммутатор с n физических либо логических интерфейсов, сетевой трафик с m из которых необходимо анализировать. Независимо от того, будет SPAN-сессия терминироваться на данном коммутаторе или на удаленном, соблюдается условие $m \leq n - 1$, поскольку интерфейс, который дублирует пакеты на анализатор, не может подавать копию своей нагрузки на себя. В зависимости от поставленных задач и возможностей коммутатора по каждому из m интерфейсов анализируется входящий, исходящий, либо весь трафик. Обозначим за Rx пиковое значение загрузки (бит/с) интерфейса входящими данными, а за Tx – исходящими. Расчет пропускной способности SPAN-порта и, соответственно, сетевого сенсора (Bw), на который направляется весь трафик с m интерфейсов, производится по формуле:

$$Bw = \sum_{i=1}^{m} (Rx_i + Tx_i) \qquad (1)$$

Если же представляют интерес пакеты либо только входящие, либо только исходящие, в зависимости от порта коммутатора и подключенного к нему оборудования, то для вычисления введем дополнительные параметры: t – количество интерфейсов, с которых будет копироваться исходящий трафик, r – количество портов, у которых будут анализироваться входящие данные. В этом случае соблюдаются условия: $r \leq m$, $t \leq m$. Требования к соотношению значений r и t определяются либо поставленными задачами для исследования, либо программно-аппаратными ограничениями коммутатора. Таким образом, формула (1) для вычисления пропускной способности Bw приобретает следующий вид:

$$Bw = \sum_{i=1}^{r} Rx_i + \sum_{i=1}^{t} Tx_i \qquad (2)$$

Практическое применение результатов вышеописанных расчетов в Ethernet-сети предприятия, как правило, сводится к решению вопросов:

- Определение типа интерфейса на «зеркалированный» порт – FastEthernet, GigabitEthernet или TenGigabitEthernet.
- Выбор сетевого сенсора необходимой производительности и стоимости.

Использование статистики нагрузки агентов IDS

Применяя возможность сбора статистических данных с сенсоров IDS, при анализе загрузки процессоров, объеме и пакетности обрабатываемого трафика можно решить возникающие в ходе развития и эксплуатации инфраструктуры систем обнаружения вторжений проблемы:

- *рациональности использования ресурсов;*

Стоимость устройств напрямую зависит от их производительности. Необходимо четкое понимание того, какие требования должны предъявляться к программно-аппаратным комплексам, которые устанавливаются в разных сегментах сети.

- *соответствия реальных параметров официально заявленным производителем;*

Одна из наиболее важных и, соответственно, ценообразующих характеристик систем обнаружения вторжений – производительность. От возможности гарантированно обрабатывать сетевой трафик на определенной скорости зависит не только эффективность работы, но и стоимость. Официально заявленные производителем цифры могут не соответствовать реальности в связи со спецификой работы инфраструктуры и использования различных бизнес-приложений.

- рациональности распределения агентов IDS различной пропускной способности по разным участкам сети;

Если требования к производительности сенсоров не были учтены на этапе проектирования, возможно выявление несоответствий в процессе внедрения или эксплуатации благодаря анализу загрузки систем обнаружения вторжений.

- целесообразности снятия части нагрузки с агента IDS путем исключения из SPAN-сессии некоторых интерфейсов либо VLAN;

В сегментированных на виртуальные локальные сети (VLAN) корпоративных компьютерных сетях необходимо определить участки, которые требуется защищать в первую очередь (DMZ, бизнес-критичные сервера), в то время как защита других сегментов может быть не обязательна либо является второстепенной задачей.

- возможности наращивания инспектируемого трафика;

Подобная необходимость может возникнуть как при запланированном росте инфраструктурного сегмента, так и при постепенном увеличении трафика, который подается на сетевой сенсор.

- целесообразности подключения дополнительного сенсора IDS в коммутатор в случае перегрузок;

При отсутствии более мощных решений определенные реализации систем обнаружения вторжений позволяют объединять несколько устройств, суммируя их пропускную способность, для более эффективной обработки всего трафика. Рекомендуется использовать на сетевых сегментах, которые необходимо анализировать на наличие проникновений полностью.

- агрегации SPAN-сессий из разных коммутаторов для инспектирования на одном сенсоре любого производителя;

В случае наличия агента IDS с большим количеством интерфейсов либо агрегирующего ответвителя возможен анализ сетевого трафика, который подается с разных коммутаторов, одним сетевым сенсором.

- получения дополнительной информации об изменениях сетевой активности;

На основании информации об изменениях сетевого трафика можно контролировать появление аномалий либо использование несогласованных сетевых приложений

- получение информации о проведенных несогласованных работах по реорганизации сети либо о произошедшей аварии;

Зная среднестатистический уровень нагрузки каждого сетевого сегмента и сенсора в зависимости от времени, возможно определение проведенных работ по реорганизации инфраструктуры, реконфигурации активного сетевого оборудования. Также резкое изменение объема обрабатываемого трафика может свидетельствовать об аварии, отказе одного из элементов, перестроении таблиц маршрутизации, дерева коммутации и т. п.

- определение степени влияния работ на сервис для пользователей;

Резкое изменение показателей нагрузки, не характерное для данного временного интервала на определенном участке сети, может частично помочь в определении влияния проводимых работ либо произошедшей аварии на сервис для конечных пользователей.

- воздействие внешних факторов (температура, отключение штатного электропитания);

Если в программно-аппаратных средствах сенсоров реализована возможность получения информации о температуре окружающей среды и процессора, наличии штатного электропитания либо переходе на резервное – системы управления могут получать эту информацию и извещать соответствующие подразделения.

- программный/аппаратный сбой в работе сенсоров.

Учитывая то, что системы обнаружения вторжений в режиме IDS не влияют на работу корпоративной сети предприятия, сбой в работе агентов определяется в некоторых случаях по отсутствию возможности управления ими.

Заключение

Правильный расчет нагрузки, вызываемой копией трафика на «зеркалированный» порт коммутатора, может помочь выделить интерфейс необходимой пропускной способности и выбрать подходящий сетевой сенсор для каждого сегмента сети. Рекомендуемая пропускная способность не должна быть ниже суммарной пиковой нагрузки на интерфейсы, сетевой трафик с которых будет копироваться, во избежание потери пакетов. Анализируя загрузку сетевых сенсоров, существует возможность получения ряда дополнительных сведений, на основании которых можно сделать выводы о рациональности использования ресурсов, соответствия официальных параметров действительным данным, получать информацию об авариях, несогласованных работах либо появлении аномалий в сети и т. п.

ПРИМЕНЕНИЕ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ ОТБОРА КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРОГРАММНОГО КОМПЛЕКСА «СТИМУЛ»

Озарко Екатерина Сергеевна, директор НИИ инфокоммуникаций ОНАС им.А.С.Попова
Опотяк Юрий Владимирович, с.н.с. НИЦ телекоммуникационных систем и сетей связи ОНАС им.А.С.Попова
Научно-исследовательский институт инфокоммуникаций Одесской национальной академии связи им.А.С.Попова, г.Львов, Украина, 79000 ул. Троллейбусная,11
E-mail: ndii@i.ua; тел./факс: +38 (032) 261-63-14

Рассмотрена возможность использования разработанного НИИИ ОНАС им.А.С.Попова программного комплекса тестирования «Стимул» для решения задач подбора кадров в сфере управления информационной безопасностью. Использование инструментальных средств поможет объективно подойти к решению этой задачи.

The possibility of using of program testing complex ‘Stimul’, developed by Scientific and Research Institute of Infocommunication of Odessa National A.S. Popov Academy of Telecommunications, has been considered for solving tasks in personnel selection in the sphere of information security management. Making use of instrumental means will help to approach objectively to solving of this.

Введение

Подбор кадров в сфере информационной безопасности является одной из наиболее важных и актуальных задач. Несмотря на постоянное совершенствование специальной техники в сфере защиты информации, «человеческий фактор является определяющим как с точки зрения достижения в развитии производства, так и его упадка, совершения аварий и даже катастроф» [1]. Известно, что надежность систем защиты информации в значительной мере определяется организационными мероприятиями, что напрямую связано с личностными характеристиками и установками каждого отдельного специалиста, работающего в сфере информационной безопасности. Недостаточно иметь образование в области ИТ, знать и уметь работать со специальными программными и аппаратными средствами. Нужно обладать соответствующими свойствами характера. Недостаточное внимание к личностным качествам каждого отдельного специалиста в сфере информационной безопасности, может представлять для предприятия более значительную угрозу, чем утечка информации с использованием специальных технических средств. В то же время, к примеру, выявление лидеров и правильное использование их авторитета является одним из способов сокращения количества киберпреступлений [2].

Разработанный в НИИИ ОНАС им.А.С.Попова программный комплекс тестирования «Стимул» (ПКТ «Стимул») предназначен для определения личностных свойств анкетируемых (персонального профиля) с использованием валидных методик DISC, MBTI, Р. М. Белбина, В.И. Герчикова и др.[3-5]. Использование этих методик, их сопоставление и творческое переосмысливание, позволяют избавиться от субъективного фактора при определении свойств характера персонала и перейти к более определенным объективным характеристикам. Это, в свою очередь, делает возможным формирование на основе проведенного тестирования т.н. «профиля анкетируемого». Использование «профилей» позволяет с помощью ПКТ «Стимул» производить подбор наиболее предпочтительных для каждого анкетируемого профессий. Результаты применения ПКТ «Стимул» на ряде украинских и зарубежных предприятий, организаций и учебных заведений свидетельствуют о надежности и достоверности получаемых результатов тестирования. ПКТ «СТИМУЛ» апробирован в Одесской национальной академии связи им.А.С.Попова, Мореходном колледже технического флота ОНМА, Концерне Радиовещания, радиосвязи и телевидения, Производственном объединении «Азтелеком» (республика Азербайджан), Дочернем предприятии «Синергия» (Synergia SE), Керченском городском совете (автономная республика Крым), Научно-производственном предприятии «Квант-Эфир», Государствен-

ном предприятии «Украинский государственный центр радиочастот», учебных заведениях г.Львова (ЛСШ №4, школе-лицее «Орияна») и др.

В связи с выше изложенным представляется целесообразным проведение исследований, призванных сформулировать набор признаков и характеристик специалистов, работающих в сфере защиты информации, неких «шаблонов» специалиста по защите информации. Эти «профили» могут быть получены путем анализа и обработки результатов опроса целевых групп специалистов. Отбор по таким признакам целесообразно производить еще на этапе обучения в ВУЗе, а также, с целью корректировки в воспитательной работе.

Важными деталями эффективного и надежного функционирования системы безопасности на отдельном предприятии являются также психологическая совместимость персонала, индивидуальные мотивационные устремления и ролевые позиции. ПКТ «Стимул» позволяет, после получения профилей анкетируемых, провести оценку межличностных взаимоотношений, определить мотивы и стимулы, наименее и наиболее приемлемые роли, выявить возможные конфликтные или иные негативные взаимодействия между членами коллектива. Очевидно, что устранение негативных взаимодействий, а также формирование мотивационных программ с учетом личностных установок и предпочтений, оптимального ролевого распределения будет способствовать улучшению функционирования системы защиты информации в целом.

Выводы

1. Использование в процессе подбора кадров в сфере управления информационной безопасностью средств для объективного выявления личностных характеристик анкетируемых (например, ПКТ «Стимул») является чрезвычайно важным и необходимым.

2. Разработка «шаблонов» профессий позволит проводить отбор специалистов, наиболее пригодных по своим личностным качествам для работы в сфере защиты информации, производить на этапе обучения в ВУЗе соответствующую корректировку воспитательной работы.

3. Выявление возможных негативных взаимодействий в коллективе, определение индивидуальных мотивационных устремлений на основе сформированных «профилей» анкетируемых будет способствовать повышению эффективности мер по защите информации.

Литература:

1. Воробиенко П.П. Развитие человеческого капитала при принятии на работу и карьерном росте/П.П. Воробієнко//Наукові праці ОНАЗ ім. О.С. Попова.-2008.
2. Шиндер Д.Л. Киберпреступность. Перевод Тропиной Т. Источник:Crime.vl.ru.
3. Dr. Russell J. Watson, Wheaton College, "Statistical Comparison Between the TTI Style Analysis and the Performax Personal Profile System," 1989.
4. Sylvan J. Kaplan: A Study of the Validity of the Personal Profile System. Minneapolis, MN: Performax Systems, International, 1983
5. Schmidt, F.L., Hunter, J.E. Urry, V.W. (1976) Statistical power in criterion-related validation studies. Journal of applied Psychology, 61, 473-485.

УЧЕТ ВЛИЯНИЯ НА СКРЫТНОСТЬ Wi-Fi КАНАЛОВ СВЯЗИ ИХ ЭЛЕКТРОДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК И УСЛОВИЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН

Стрельницкий А.А., Шокало В.М., Ягудина Е.В., Абдул-Хуссейн М.К.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. основ радиотехники, тел. (057) 702-14-30
E-mail: stal.sivan@gmail.com

The safety of Wi-Fi channels is usually characterize by the probability of detection $P_{об}$, which depends on wave propagation (WP). The article sets out options for models of WP, which take into account the peculiarities of the Wi-Fi radio. These models are then used for numerical analysis of the safety of a local wireless radio link according to the criterion $P_{об} \le 0,7$.

A relation connecting the probability to detected the operation of wireless digital communication systems (DCS) depending on the size of the aperture and diverting legitimate channels and their mutual arrangement has been obtained. It has been displayed, that the main factors affecting the efficiency of detection is removal of the legitimate and side channel receiving aperture from the aperture of the emitters and scatterers source of information, as well as the value of the secret speed.

Введение

Проникновение Wi-Fi технологий в область конфиденциальной связи вызывает необходимость исследования скрытности Wi-Fi каналов передачи информации. Известным параметром, характеризующим скрытность, является вероятность обнаружения $P_{об}$ легитимного канала с помощью созданного злоумышленником отводного канала [1], при этом критерием безопасной работы легитимного канала считается величина $P_{об} \le 0,7$.

В [1] получено выражение, позволяющее определить значение $P_{об}$ от соотношений сигнал/шум в отводном $(S/N)_o$ и легитимном $(S/N)_л$ каналах, а также от величины секретной скорости R_s, при которой канал связи не обнаруживается.

Однако пока не получены соотношения для $P_{об}$, учитывающие влияние размеров апертур антенн легитимного и отводного каналов, а также специфику работы Wi-Fi канала – возможность взаимного расположения антенн легитимного и отводного каналов не только в дальней, но и в ближней и промежуточной зонах.

Цель данной работы состоит в разработке модели анализа величины $P_{об}$, учитывающей указанную специфику функционирования Wi-Fi канала связи.

Вывод основных соотношений

Представим цифровую систему передачи информации (ЦСПИ) с отводным каналом по аналогии с [2] в виде трех взаимодействующих апертур (рис. 1). Две из них образуют легитимный канал. Передающая апертура является сферой с диаметром a, внутри которой находятся как излучатели, так и рассеиватели. Наличие рассеивателей позволяет увеличить, как известно из [2], число каналов передачи информации в MIMO системах. Приемная апертура легитимного канала имеет размер $a_л$. Отводной канал располагается по отношению к оси легитимного канала под углом γ и имеет приемную апертуру с размером a_o. В легитимном канале апертуры удалены на расстояние $r_л$, а в отводном – на расстояние r_o.

Получим для такой системы формулу, определяющую вероятность обнаружения $P_{об}$, взяв за основу выражение известное из [1]

$$P_{об} = 1 - \frac{(S/N)_л}{(S/N)_л + 2^{R_s}(S/N)_o} \cdot e^{\left[-\frac{2^{R_s}-1}{(S/N)_л}\right]} = 1 - \frac{1}{1 + 2^{R_s}\dfrac{(S/N)_o}{(S/N)_л}} \cdot e^{\left[-\frac{2^{R_s}-1}{(S/N)_л}\right]}. \qquad (1)$$

Используя теоремы Найквиста и Шеннона [3], а также результаты работы [2] из формулы (1) получим:

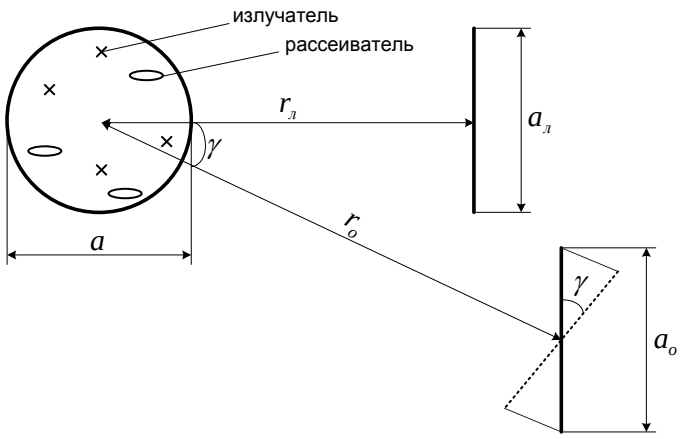


Рис. 1

$$P_{об} = 1 - \frac{1}{1 + 2^{R_s}\dfrac{\left(a \cdot a_o \cdot \cos\gamma / r_o \cdot \lambda\right)^2 - 1}{\left(a \cdot a_л / r_л \cdot \lambda\right)^2 - 1}} \cdot e^{\left[-\frac{2^{R_s}-1}{\left(a \cdot a_л / r_л \cdot \lambda\right)^2 - 1}\right]}. \qquad (2)$$

Формула (2) в явном виде отражают зависимость параметров S/N и $P_{об}$ от геометрических размеров апертур ЦСПИ a, $a_л$ и отводного канала a_o, а также их взаимного расположения (размеры $r_л$, r_o и угол γ). Анализируя выражение (2) нетрудно сделать такие рекомендации. Требуемое соотношения сигнал/шум в легитимном канале обеспечивается выбором соответствующих размеров приемной апертуры $a_л/\lambda$ и величины заполнения трассы радиоканала рассеивателями, т.е. зависит от отношения $a/r_л$. С точки зрения злоумышленника (см. выражение (2)) эффективная работа отводного канала также обеспечивается наличием большого числа рассеивателей вдоль трассы длиной r_o и значительными размерами апертуры отводного канала a_o/λ.

В приближении равенства температуры шума в легитимном и отводном каналах выражение (1) можно представить в виде

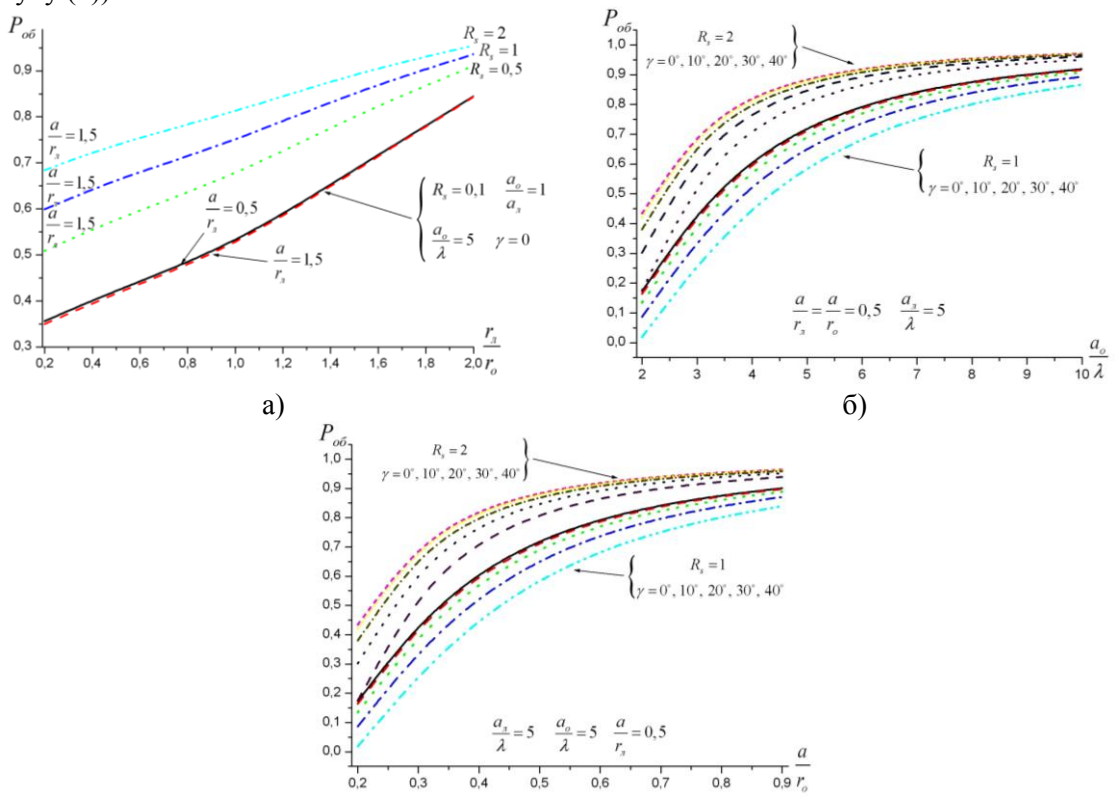
$$P_{об} = 1 - \frac{\exp\left[-\left(2^{R_s} - 1/(S/N)_л\right)\right]}{1 + 2^{R_s}\,\alpha_o/\alpha_л}, \qquad (3)$$

где α_o, $\alpha_л$ – величины затуханий в отводном и легитимном каналах соответственно.

Результаты расчетов и их анализ

Из анализа формулы (2) следует, что величина заполняемости рассеивателями трассы вдоль легитимного канала $a/r_л$ практически не сказывается на значении $P_{об}$ и одним из основных факторов, определяющим величину вероятности обнаружения, является отношение $r_л/r_o$. Этот вывод подтвержден результатами расчетов (рис. 2, а: две нижние кривые при $a/r_л = 0{,}5$ и $a/r_л = 1{,}5$). Второй важный фактор – секретная скорость

R_s. При ее росте увеличивается и вероятность обнаружения. Это также видно из рис. 2, а. Другие данные численных экспериментов по формуле (2) приведены на рис. 2 б, в. Они имеют ясный физический смысл. Так, с увеличением размера апертуры отводного канала a_o/λ растет и величина $P_{об}$ (рис. 2, б), что обусловлено увеличением $(S/N)_o$ (см. формулу (2)).



а) б)

в)

Рис. 2

При размещении апертуры a_o под некоторым углом γ к оси легитимного канала вероятность обнаружения падает, т.к. размер апертуры a_o уменьшается на значение $\cos\gamma$ (рис. 2, б).

Аналогичный характер имеют зависимости $P_{об}(a/r_o)$, приведенные на рис. 2, в. При изменении a/r_o от 0,2 до 0,5 происходит резкое увеличение вероятности обнаружения за счет роста значения $(S/N)_o$. В области, где $a/r_o > a/r_л = 0,5$ параметр $P_{об}$ слабо зависит от величины заполнения рассеивателями трассы отводного канала при больших значениях R_s и достигает максимума при $\gamma = 0^\circ$ (см., например, кривые при $R_s = 2$ бит/с).

Если принять, что уверенное обнаружение сигналов ЦСПИ возможно при $P_{об} \geq 0,7$, то можно провести такой анализ полученных результатов. Из рис. 2 следует, что сигналы ЦСПИ могут быть обнаружены при секретной скорости $R_s \geq 2$ практически при любых соотношениях $r_л/r_o$. При этом размеры апертуры излучателя отводного канала a_o должны быть не менее 4λ, а соотношение $a/r_o > 0,35$.

Рассмотрим теперь влияние условий распространения радиоволн (РРВ) на величину $P_{об}$. Формула (3) позволяет исследовать зависимость величины $P_{об}$ от значений α_o и $\alpha_л$, т.е. и от условий РРВ в легитимном и отводном каналах. С ее помощью были проведены расчеты, результаты которых представлены на рис. 3. Здесь показаны зависимости

$P_{об}(R_s)$ при $(S/N)_л = 20 дБ$ и различных значениях $r_л / r_o$ для открытого пространства (рис. 3, а – ближняя зона, рис. 3, б – промежуточная зона, рис. 3, в – дальняя зона) и помещения (рис. 3, г).

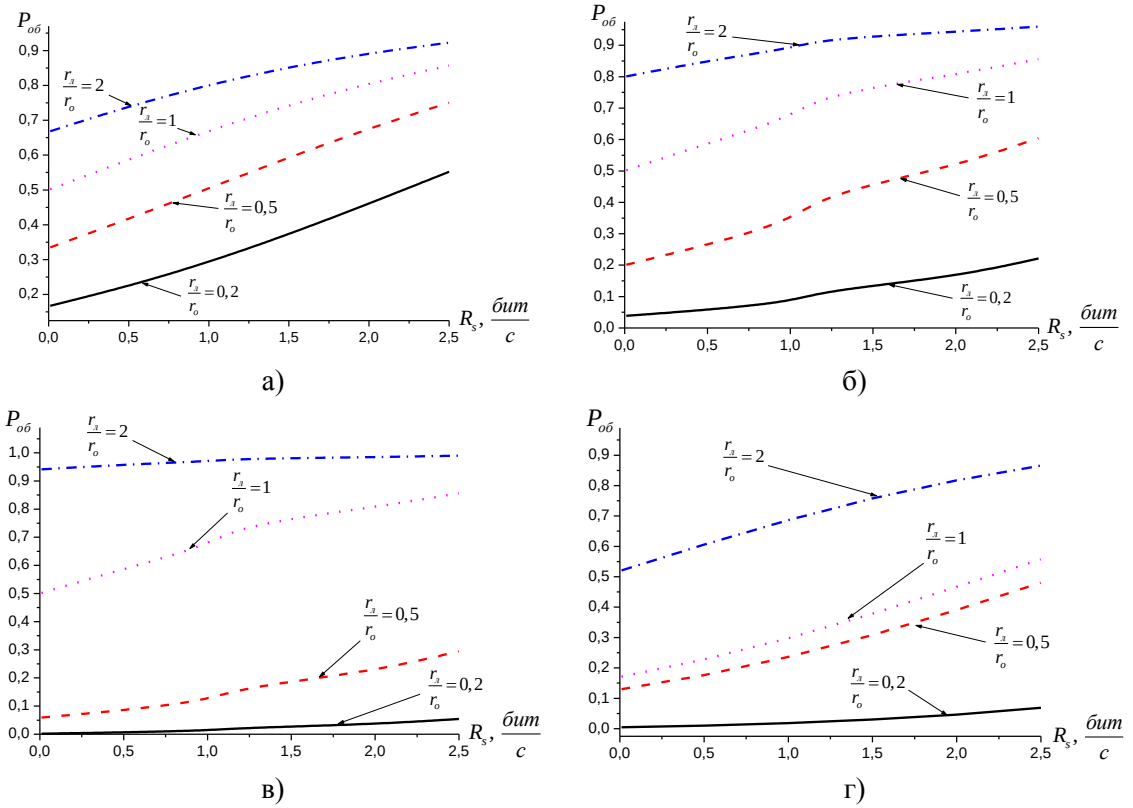


Рис. 3

При расчетах величин α_o и $\alpha_л$ для случаев открытого пространства и помещения вычислялись по формулам приведенным в [4].

Из приведенных данных следует, что в случае открытого пространства при размещении приемника легитимного канала сначала в ближней зоне передающей антенны, а затем в промежуточной и дальней зонах, вероятность обнаружений растет при $r_л < r_o$. Т.е. в ближней зоне условия обнаружения легитимного Wi-Fi канала более благоприятны.

В помещении условия обнаружения ухудшаются и критерий $P_{об} > 0,7$ реализуется при больших значениях $r_л / r_o$, чем в дальней зоне, при одних и тех же величинах R_s.

Литература:

1. *Chrysikos T., Dagiuklas T., Kotsopoulos S.* A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security // Proceedings of Security in Emerging Wireless Communication and Networking Systems (*SEWCN'09*). – Springer, 2010. – Vol. 42 of Lecture Notes in Computer Science. – pp. 3–12.

2. *Chakraborty K., Franceschetti M.* Maxwell meets Shannon: space-time duality in multiple antenna channels // Proc. 44-th Allerton Conf. Communication, Control and Computing. – Monticello, 2006. – pp. 761–770.

3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е издание. – М.: Издательский дом «Вильямс», 2003. – С. 1104.

4. *Shokalo V.M., Strelnitskiy O.O., Tsopa O.I.* Approximate Model for Estimation of Efficiency and Noise Immunity of Branched Street and Corridor Wi-Fi and WiMAX Communication Channels // International journal «Telecommunication and Radio Engineering». – Begell House, 2009. – Vol. 68(17). – pp. 1511–1528.

СТРУКТУРНАЯ СКРЫТНОСТЬ ЛИНЕЙНЫХ СИГНАЛОВ ШИРОКОПОЛОСНЫХ *xDSL* ТЕХНОЛОГИЙ

Шинкаренко И.В., Цопа А.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, кафедра ОРТ, тел. (057) 702-15-87,
E-mail: novagenoff@gmail.com.

This report presents assess of structural secrecy linear signals of digital communication's systems based on *xDSL* technology. We obtain formulas for calculating the structural secrecy of different options of linear signals and examined ways to improve the potential of structural secrecy.

При разработке защищенных ведомственных систем связи (ВСС) одним из важных требований к физическому уровню этих систем является обеспечение безопасной передачи информации, связанной, прежде всего, со скрытностью системы связи. Так как эта задача обычно решается на сигнальном уровне, то правильный выбор параметров линейных сигналов, которые являются переносчиками информации, является важным этапом при проектировании цифровых систем передачи информации (ЦСПИ) [1].

В проводном сегменте ВСС для передачи мультимедийной информации в основном применяются ЦСПИ с широкополосными *xDSL* технологиями, которые используют многоуровневые линейные сигналы [2].

Известен метод определения потенциальной структурной скрытности сигналов, не требующий знания алгоритмов обработки на станции несанкционированного доступа [3-4]. Однако анализ структурной скрытности сигналов, применяемых в проводных ЦСПИ, пока отсутствует, что не позволяет провести комплексную оценку защищенности интегрированных ВСС от перехвата информации.

Цель доклада представить результаты анализа потенциальной структурной скрытности широкополосных линейных сигналов, используемых в различных видах *xDSL* технологий и нахождение путей ее увеличения.

Структурная скрытность определяется числом двоичных измерений, которые необходимо осуществить для раскрытия структуры сигнала. Общее выражение для потенциальной скрытности S_P имеет вид [5]:

$$S_P = \log_2 A \ \text{[диз]}, \qquad (1)$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Так как в современных проводных ЦСПИ применяются составные сложные сигналы, то структурная скрытность S_Σ в этом случае будет суммой структурной скрытности отдельных элементов сигнала

$$S_\Sigma = S_1 + S_2 + .. + S_i = \log_2 A_1 + \log_2 A_2 + ... + \log_2 A_i \ \text{[диз]} \qquad (2)$$

где A_1, A_2, . . ., A_i – количество (арсенал, ансамбль) всех возможных значений каждого из *i*-параметров составного сигнала.

Используя выражение (2) и (1) для потенциальной скрытности отдельных параметров линейных сигналов, в работе проведена оценка скрытности основных *xDSL* технологий (*SHDSL, ADSL* и *VDSL)*, которые применяются при построении проводных ЦСПИ для ВСС.

Симметричная технология *SHDSL* использует сигналы с многоуровневой амплитудно-импульсной модуляцией *PAM-M* (*Pulse Amplitude Modulation*) с уровнем модуляции $M = 4,8,16,32,64,128$ ($S_{QAM} = \log_2(M!)$ и формированием формы

линейного сигнала с помощью фильтра приподнятого косинуса *RC* (*Raise Cosines*), имеющего арсенал состояний коэффициента сглаживания фильтра $A_{RS} = 128$.

Стабильность тактовых генераторов ЦСПИ обеспечивает потенциальную скрытность сигнала S_f, которая определяется числом возможных значений параметра частоты легитимного модема $f_{ЛК}$ в диапазоне частот разведки сигнала

$$S_f = \log_2\left(\sqrt{12}\cdot\sigma_f / \Delta f\right), \quad (3)$$

где Δf – шаг дискретизации по частоте в приемнике-обнаружителе; σ_f – среднеквадратическое отклонение (СКО) частоты.

Тогда потенциальная скрытность определяется выражением:

$$S_{SHDSL} = S_f + S_{QAM} + S_{RS} = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) + \log_2(M!) + \log_2(A_{RS}) \quad (4)$$

Высокоскоростная технология *VDSL* использует многочастотные *DMT* сигналы с модуляцией *QAM*. Потенциальная скрытность для сигналов *DMT* с N поднесущими частотами и дискретным изменением уровня мощности P_C линейного сигнала в пределах от *-17* до *+17 дБм* с шагом *1 дБм* (арсенал $A_P = 34$) имеет вид

$$S_{VDSL} = S_f + S_{DMT} + S_{QAM} + S_P = \log_2\left(\frac{\sqrt{12}\cdot\sigma_f}{\Delta f}\right) + \log_2(N) + \log_2(M!) + \log_2(A_P). \quad (5)$$

Используя полученные выражения (4) и (5), можно провести сравнительный анализ структурной скрытности линейных сигналов различных *xDSL* технологий.

Данные о потенциальной структурной скрытности *SHDSL, ADSL* и *VDSL* технологий при различных значениях отдельных параметров линейного сигнала представлены в таблице 1.

Таблица 1.

Вид технологии	Тип сигнала	Количество поднесущих, *N*	Уровень модуляции, *M*	Скрытность S, диз
HDSL	*PAM-16*	1	16	65
SHDSL	*PAM-128*	1	128	747
ADSL	*DMT QAM-256*	256	256	1720
ADSL2	*DMT QAM-1024*	512	1024	8839
VDSL	*DMT QAM-2048*	1024	2048	19700
VDSL2	*DMT QAM-4096*	2048	4096	43479

Приведенные результаты говорят о высокой потенциальной структурной скрытности сигналов, применяемых в современных цифровых технологиях передачи информации по кабельным каналам связи. Кроме того, из анализа табл. 1 следует, что *VDSL* технологии, использующие для передачи информации большое количество поднесущих частот и высокие уровни модуляции *QAM*, имеют значительное преимущество по сравнению с другими *xDSL* технологиями.

Исследования показывают, что для увеличения структурной скрытности ВСС необходимо не только расширять ансамбли применяемых сигналов, но и использовать оригинальные методы формирования линейных сигналов в ЦСПИ, что позволит применять *xDSL* технологии в проводных сегментах защищенных ВСС.

Заключение.

1) В докладе рассмотрены вопросы оценки потенциальной структурной скрытности линейных сигналов проводных ЦСПИ без учета особенностей алгоритма обработки сигнала в приемнике-обнаружителе.

2) Для увеличения структурной скрытности сигналов, используемых в *xDSL* технологиях, необходимо расширять ансамбли линейных сигналов.

3) Применение оригинальных алгоритмов взаимодействия модемов отечественных ЦСПИ позволит повысить защищенность проводных сегментов ВСС.

Литература:

1. *Хорошко В. А., Чекатков А. А.* Методы и средства защиты информации. – К.: ЮНИОР, 2003. – 504 с.

2. *Балашов В. А., Лашко А.Г., Ляховецкий Л. М.* Технологии широкополосного доступа *xDSL*. – М.: «Эко-Трендз», 2009. – 256 с.

3. *Захарченко Н. В.* Структурная скрытность таймерных сигналов в системах с кодовым разделением сигналов. / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-европейский журнал передовых технологий. – 2011. – №2/9(50). – С. 7-9.

4. *Кувшинов О. В., Вознюк Р. В.* Оцінка структурної критності широкосмугових сигналів. // Збірник наукових праць ВІТІ НТУ «КПІ». – 2011. – № 1. – С. 106-111.

5. *Каневский З. М.* Теория скрытности / З. М. Каневский, В. П. Литвиненко. – Воронеж: ВГУ, 1991. – 144 с.

СКРЫТАЯ ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ СЛОЖНЫХ ХАОТИЧЕСКИХ СИГНАЛОВ

Васюта К.С., Зоц Ф.Ф.
Харьковский университет Воздушных Сил им. Ивана Кожедуба
61045, Харьков, ул. Клочковская, 228, каф. боевого применения радиотехнического вооружения
E-mail: kohafish@yandex.ru

Solution of complex tasks increase of secrecy is in-process offered telecommunikations systems on the basis complication of attractors of the chaotic bearing. Linear and nonlinear transformations of chaotic sequence and their dynamic and statistical descriptions are investigational. The new method of the hidden transmission of binary report is offered by manipulation of Herst index arcwise-regenerate chaotic sequence. The new method of the hidden transmission of binary report is offered with the use of nonlinear operator interfusion elements of the chaotic bearing.

Проблема обеспечения скрытности радиотехнических систем передачи информации (РТС ПИ) и управления, признаком которой является их работа «под шум», является весьма острой и до сих пор не нашла своего решения в большинстве прикладных задач [1].

В настоящее время для скрытной передачи информации используют широкополосные сигналы (ШПС). Обеспечение конфиденциальности радиотехнических систем передачи информации с применением широкополосных сигналов позволяет ослабить воздействие многих видов помех и принимать сообщения при соотношении сигнал/шум много меньше единицы. Скрытность, которую называют энергетической, обеспечивается за счет передачи в эфир непрерывных во времени сложных широкополосных радиосигналов с очень низкой спектральной плотностью, при которой сигналы «прячутся» под шумом [1]. При этом без шума такие сигналы визуально не похожи на случайный процесс. Поэтому их скрытность обеспечивается лишь при наличии шума, уровень которого больше уровня сигнала. Сложные широкополосные сигналы не являются сигналами, работающими «под шум» и, следовательно, в полной мере не обеспечивают скрытность систем передачи информации, в которых они применяются.

Альтернативное решение проблемы обеспечения скрытности дает применение шумоподобных сигналов, формируемых нелинейными динамическими системами, демонстрирующими хаотическое поведение. Такие сигналы неотличимы от шума при визуальном анализе и обладают набором специфических свойств, делающих их привлекательными с точки зрения процессов обработки, построения схем скрытой передачи информации. Хаотические сигналы (процессы, последовательности) представляют собой нерегулярные колебания, обладающие сплошным спектром мощности и быстро спадающей автокорреляционной функцией. Это ставит их потенциально в один ряд с шумоподобными сигналами, широко применяемыми в современной технике связи.

В известных методах скрытой передачи информации декларируется их скрытность, не опирающаяся на численные оценки и в них рассматривается только структурная скрытность [2,3].

Скрытность для РТС, использующих хаотические сигналы более широкое понятие, в настоящее время еще не формализовано и поэтому под скрытностью косвенно понимают структурную скрытность. Так как в динамической системе (ДС) любое отклонение от начальных условий делает невозможным прогноз эволюции ее поведения, и получить структуру такого сигнала так же невозможно. Поэтому было принято под структурной скрытностью понимать набор параметров, определяющих состояние ДС.

Под скрытностью принято понимать способность противостоять мерам несанкционированного доступа обнаружению сигнала и определению его структуры на основе оценки ряда его параметров.

Изучение аттракторов сигналов, использующихся в известных методах скрытой передачи информации [2,3] показало, что они имеют простую структуру и при использовании метрического и визуального анализа позволяет их легко классифицировать (т.е. отличить от шума). А, следовательно, не обладают заявленной скрытностью.

Исходя из этого, в работе предлагается решение комплекса задач повышения скрытности РТС на основе усложнения аттракторов хаотической несущей.

Для этого исследованы линейные и нелинейные преобразования хаотической последовательности и их динамические и статистические характеристики. Показано, что линейное и нелинейное преобразования хаотической последовательности существенно изменяет ее статистические и динамические свойства. Увеличение числа элементов, участвующих в ее формировании, существенно влияет на плотность распределения, ковариационную функцию, энергетический спектр и поведение на фазовой плоскости. Применение специальных мер (линейное и нелинейное преобразования) усложнения эволюцию хаотического процесса в псевдофазовом пространстве (рис.1), разрушает связи в его значениях и позволяет значительно повысить скрытность коммуникационных систем и сетей, в целях передачи, приема и хранения конфиденциальной информации.

Получен новый метод скрытой передачи бинарного сообщения манипуляцией показателя Херста линейно-преобразованной хаотической последовательности (рис.2).

Метод передачи бинарных сообщений с использованием линейного преобразования хаотической последовательности с ядром Мандельброта за счет манипуляции показателя Херста позволяет осуществлять скрытую передачу бинарного сообщения. При этом сохраняется не только визуальное сходство сформированного процесса с белым шумом, но и его неразличимость в рамках спектрального, корреляционного и нелинейного анализа.

Получен новый метод скрытой передачи бинарного сообщения с использованием нелинейного оператора перемешивания элементов хаотической несущей (рис.3). Использование метода хаотического перемешивания хаотической несущей при формировании сигнала способствует увеличению его скрытности в 5 и более раз [4].

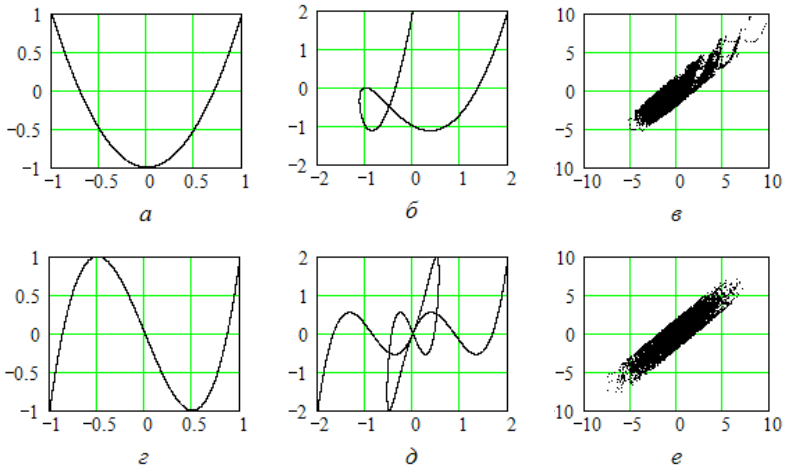


Рис.1. Поведение на фазовой плоскости линейно–преобразованной хаотической последовательности

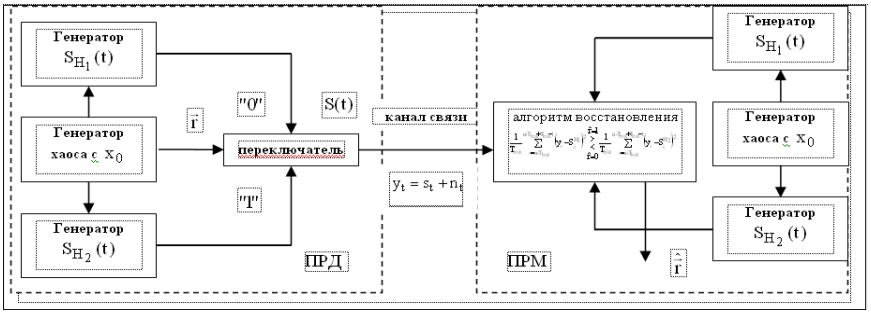


Рис.2. Схема скрытой передачи бинарного сообщения манипуляцией показателя Херста линейно-преобразованной хаотической последовательности

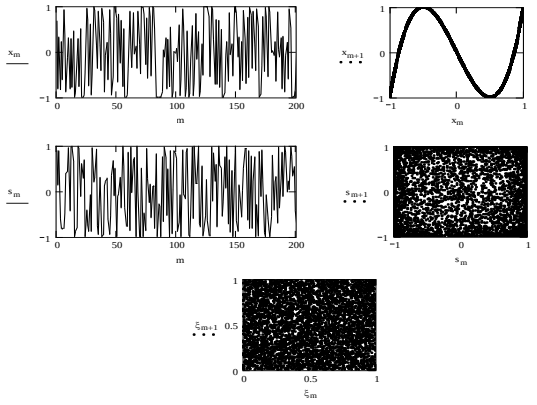


Рис.3. Поведение хаотического процесса до и после применения оператора перемешивания

Применение новых неклассических идей нелинейной динамики, методов нелинейного и статистического анализа, позволяют обеспечить работу современных РТС ПИ «под шум» и повысить их скрытность за счет использования при передаче цифровых сообщений хаотических сигналов со сложным аттрактором, которые неразличимы в рамках спектрального, корреляционного и нелинейного анализа.

Задачи обнаружения таких сигналов и оценка их параметров на фоне шумов для санкционированного наблюдателя с учетом их специальных свойств решены с привлечением BDS – статистики и технологии формирования суррогатных сигналов. При этом для рассмотренных классов сигналов, его характеристики обнаружения близки к характеристикам энергетического обнаружителя.

ЛИТЕРАТУРА

1. Помехозащищенность радиосистем со сложными сигналами / [Г. И. Тузов, В. А. Сивов, В. И. Прытков и др.]. — М.: Радио и связь, 1985. — 264 с.

2. Кроновский А. А. О применении хаотической синхронизации для скрытой передачи информации / А. А. Кроновский, О.И. Москаленко, А.Е. Храмов // Успехи физических наук. — 2009. — Т.179.— № 12. — С. 1281—1310.

3. Дмитриев А. С. Сверхширокополосная беспроводная связь на основе динамического хаоса / А. С. Дмитриев, А. В. Клецов, А. М. Лактюшкин [и др.] // Радиотехника и электроника. — 2006. — Т. 51, №10. — С. 1193—1242.

4. Использование BDS-статистики для оценки скрытности сигнала, полученного перемешиванием хаотической несущей / П. Ю. Костенко, К. С. Васюта, А. Н. Барсуков [и др.] // Известия вузов. Радиоэлектроника. — 2010. — № 5 (53). — С. 41—45.

АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В WINDOWS AZURE

Ганзенко В.В., Добрынин И.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. ТКС, тел. (057) 702- 55- 92 ,
E-mail: marunich.v.v@gmail.com

Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources .This may take the form of web-based tools or applications that users can access and use through a web browser as if they were programs installed locally on their own computers. Windows Azure, as an application hosting platform, must provide confidentiality, integrity, and availability of customer data. It must also provide transparent accountability to allow customers and their agents to track administration of services, by themselves and by Microsoft.

Отличительной особенностью облаков является: высокая пропускная способность, более дешевое хранение и надежная технология виртуализации, сделавшая идею программного обеспечения как службы реальностью. Облачные вычисления обеспечивает масштабируемые, гибкие системы с оплатой текущих расходов, соответствующие требованиям поколения «больших результатов с меньшими затратами», но безопасность остается критически важной проблемой. Обеспечение безопасности в Windows Azure состоит из трех основных компонентов: конфиденциальности, целостности и доступности, также как и в любой распределенной сети. В данном докладе подробно будут рассмотрены механизмы защиты информации для приложений и служб в Windows Azure.

Предложено несколько механизмов защиты информации для приложений и служб, размещенных в Windows Azure.

1. Владение учетной записью.

Портал для клиентов Майкрософт (MOCP) позволяет управлять учетными записями и биллингом в Windows Azure. На портале MOCP можно подписаться на службы Windows Azure, а также дополнительные службы, такие как SQL Azure, и создать новые экземпляры подписок. Подписки — это «граница биллинга» для служб Windows Azure. Для всех приложений, которым необходима особая структура биллинга, требуются отдельные подписки. Для каждой подписки определяются учетные записи «владельца учетной записи» и «администратора службы». Эти учетные записи связаны с учетными записями Windows Live ID. Владелец учетной записи самостоятельно отвечает за управление подпиской и биллингом на портале MOCP.

Акцентировано внимание на создании отдельных учетных записей для этих ролей. Эти учетные записи независимы от отдельных учетных записей. Для идентификации пользователя в системе необходимо использовать персональную учетную запись Windows Live ID в качестве учетной записи владельца или администратора учетной записи. Для создания уникальной учетной записи можно использовать схему именования (например, AO[уникальный идентификатор]@uib.ua для владельца учетной записи и AA[уникальный идентификатор]@uib.ua для администраторов учетной записи) с паролями, которыми можно управлять и восстанавливать при необходимости, на централизованном уровне. После создания подписи администраторы учетных записей могут управлять размещенными службами на портале управления Windows Azure. Для этого используются учетные данные учетной записи администратора службы.

2. Использование сертификатов.

Существует два вида сертификатов, использующихся в защите приложений и служб: сертификаты служб и сертификаты управления.

Сертификаты служб — это традиционные сертификаты SSL, используемые для защиты связи конечных точек. Сертификаты служб используются для рабочих развертыва-

ний сред, выпускаемых доверенным корневым центром сертификации (CA). Поэтому они отдельно приобретаются у стороннего поставщика.

Имя сертификата SSL должно соответствовать имени домена веб-сайта. Для этого нужна запись DNS CNAME для сопоставления app.cloud.net (имя домена для приложения, предоставленное Windows Azure) с www.yourcompany.com. Для целей обеспечения безопасности нельзя приобрести сопоставление сертификатов с app.cloud.net. Только корпорация Майкрософт может выпускать сертификаты для cloud.net, хотя для целей разработки можно создавать собственные само подписывающиеся сертификаты.

Сертификаты управления — другой тип сертификатов, использующихся Windows Azure. Средства Windows Azure для Microsoft Visual Studio используют сертификаты управления для проверки подлинности разработчиков для развертывания Windows Azure. Средство командной строки CSUpload также использует сертификаты управления для развертывания ролей образов виртуальных машин, выполняющих запросы Windows Azure Service Management REST API.

Одной из основных проблем организации является изменение учетной записи пользователя, например, когда сотрудник перестает работать на данном предприятии. Для того чтобы закрыть доступ пользователю к ресурсам или просто внести изменения в учетную запись сотрудника необходимо следовать следующим правилам.

Правило 1 — восстановление паролей для всех учетных записей администраторов служб, к которым имел доступ бывший сотрудник. Если установлены уникальные и независимые идентификаторы владельца учетной записи и администратора службы с возможностью централизованного управления, это упростит данный процесс. Если невозможно восстановить пароль для учетной записи администратора службы, можно войти в систему MOCP как владелец учетной записи, обновить учетную запись, указанную как запись администратора службы. Также необходимо удалить все учетные записи, указанные для дополнительных администраторов на портале управления Windows Azure.

Правило 2 — повторный выпуск всех необходимых сертификатов управления. Эти сертификаты предоставляют средства проверки подлинности для размещенной службы через API Visual Studio и Windows Azure. Поэтому им нельзя больше доверять после того, как сотрудник прекращает трудовые отношения.

Выше перечисленные механизмы защиты информации в Windows Azure, позволят предотвратить различные утечки информации, как от доверенных сотрудников, так и от лиц с которыми заключены деловые отношения. Также уменьшить риск зависимости бизнеса от ИТ - структуры.

Литература:

1. Cloud computing [Электронный ресурс] / En.wikipedia.org – Режим доступа URL: http://en.wikipedia.org/wiki/Cloud_computing – 20.08.2011 – Загл.с экрана.

2. Windows Azure. Общие сведения об управлении учетными записями безопасности в Windows Azure [Электронный ресурс] / Oszone.net. Джошуа Хоффман – Режим доступа URL: http://www.oszone.net/15725/Windows-Azure - 19.07.2011 – Загл. с экрана.

3.Windows Azure Security Overview [Электронный ресурс] / Globalfoundationservices.com. Charlie Kaufman and Ramanathan Venkatapathy – Режим доступа URL:http://www.globalfoundationservices.com/security/documents/WindowsAzureSecurityOverview1_0Aug2010.pdf - 01.08.2011 - Загл. с экрана.

АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ СТАНДАРТА ISO/IEC 27001

Дуравкин Е.В., Гладий Л.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем,
тел.(057) 702-55-92), E-mail: tcs@kture.kharkov.ua; факс: (057) 702-13-20

The information is one of the most important business resources who provides the organizations additional cost and thereof requires protection. ISO/IEC 27001 is the formal set of specifications against which organizations may seek independent certification of their Information Security Management System (ISMS). ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing an organization's information security risks. The standard covers all types of organizations such as commercial enterprises, government agencies and non-profit organizations.

На сегодняшний день информация является одним из наиболее ценных активов компаний. Следовательно, успешность бизнес процессов компании на прямую связанно с вопросами обеспечения безопасности информационных активов.

Правильная организация системы менеджмента информационной безопасности (СМИБ) позволяет минимизировать не только риски потерь информации, важной для компании, но и снижает общую стоимость владения системой безопасности. По статистике группы компьютерной безопасности по реагированию на инциденты (CERT) более 60% организаций регулярно терпят убытки, связанные с нарушением информационной безопасности и не способны оценить ущерб или хотя бы обнаружить многие из этих нарушений.

Отчет группы CERT за 2010 год показал, что киберпреступники начинают отказываются от традиционных методов массовой рассылки спама и переходят к персонализированным атакам. Главная цель этих атак – кража интеллектуальной собственности. Ежегодно такие атаки, организуемые с учетом особенностей того или иного объекта и содержащие вредоносные программные коды, нацеленные на конкретную группу пользователей и даже на отдельного пользователя, наносят ущерб в $1,29 млрд.

Успех целевых атак, как и других киберпреступлений, строится на технических уязвимостях и людской доверчивости.

Против таких атак труднее всего защищаться, тогда, как они могут нанести значительный ущерб. Одним из наиболее эффективных способов защиты от таких атак является построение единой системы информационной безопасности в компании, которая будет в себя включать и организационные и технические процедуры защиты информации.

Международный стандарт менеджмента информационной безопасности ISO/IEC 27001 предназначен для разработки системы управления информационной безопасностью организации [1].

Положения стандарта описывают такие аспекты:

- Политика безопасности;
- Организационные методы обеспечения информационной безопасности;
- Управление ресурсами;
- Пользователи информационной системы;
- Физическая безопасность;
- Управление коммуникациями и процессами;
- Контроль доступа;
- Приобретение, разработка и сопровождение информационных систем;
- Управление инцидентами информационной безопасности;
- Управление непрерывностью ведения бизнеса.

Внедрение СМИБ позволит:

- Выявить основные угрозы безопасности для существующих бизнес-процессов;

- Оценить риски информационной безопасности и принимать решения на основе бизнес-целей компании;
- Обеспечить эффективное управление системой в критичных ситуациях;
- Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности)
- Четко определить личную ответственность сотрудников компании за нарушения безопасности;
- Снизить стоимость владения системой безопасности компании;
- Продемонстрировать клиентам, партнерам свою приверженность к информационной безопасности;
- Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках;
- Подчеркнуть прозрачность и чистоту бизнеса перед законом.

Такая система менеджмента информационной безопасности, построенная в соответствии с требованиями стандарта ISO/IEC 27001, представляет собой гибкий инструмент, использование которого позволит выявить возможные угрозы информационной безопасности и уязвимости в системе защиты, разрабатывать и внедрять мероприятия организационного, технического, физического характера, нацеленные на снижение вероятностей возникновения таких угроз, а также проводить оценку эффективности подобных мероприятий.

Особенностью данного стандарта является то, что он касается не только вопросов управления в компьютерных сетях, но и вопросов разработки политики безопасности, работы с персоналом, обеспечения непрерывности процесса производства, а также юридических требований.

При построении СМИБ в соответствии с требованиями ISO/IEC 27001 за основу берется модель PDCA [2]:

- Plan (Планирование) — фаза создания системы управления информационной безопасностью, создание перечня активов, оценки рисков и выбора мер;
- Do (Действие) — этап реализации и внедрения соответствующих мер;
- Check (Проверка) — фаза оценки эффективности и производительности системы управления информационной безопасностью. Обычно выполняется внутренними аудиторами.
- Act (Улучшения) — выполнение превентивных и корректирующих действий

В связи с тем, что требования к данному стандарту имеют общий характер, его можно применять к широкому кругу организаций – малых, средних, больших – занимающихся деятельностью в различных областях, особенно в тех, где вопросы защиты информации особенно важны, например, в таких отраслях, как здравоохранение, работа с финансами, страхование, информационные технологии и госучреждения.

Данный стандарт хорошо согласовывается и с другими стандартами систем менеджмента информационной безопасности, таких как 9001:2000 и ISO 14001:2004, что связано с использованием общих принципов защиты информации.

Использование данного стандарта при организации СМИБ на предприятии позволит снизить и оптимизировать затраты на поддержку системы безопасности. Будут финансироваться только те направления безопасности, которые закроют самые опасные риски для определенного предприятия.

Литература:

1. ISO/IEC 27001 Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. – Взамен BS 7799-2:2002; Введ. 18.10.05. 2. Praveen Gubta, Beyond PDCA - A New Process Management Model // Quality Progress. – July 2006, Vol. 39, No. 7, – P. 45-52.

УНИВЕРСАЛЬНАЯ СРЕДА ИМИТАЦИИ ПРОЦЕССОВ, ПРОИСХОДЯЩИХ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ, ОРИЕНТИРОВАННАЯ НА ЗАДАЧИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ АТАКАМ

Персиков А.В., Еременко А.С.
Харьковский национальный университет радиоэлектроники
61166 Харьков, пр.Ленина,14, кафедра ТКС, т.702-13-20
E-mail: white_seal@mail.ru, alexere@ukr.net

The given work is handling an actual problem of development of the generic environment for processes simulation that occurred during the network attack performing in the telecommunication system. The widespread simulation environments are analyzed including its facilities and limitations identification, as well as the imperfections that forbid performing an effective intruder and defending sides' actions simulation. The integrated solution that allows consolidating the possibilities of the variety of the environments and forming the common methods library of intrusion detection and prevention system is proposed.

Введение

Важной проблемой в обеспечении информационной безопасности (ИБ) телекоммуникационных систем (ТКС) является создание эффективной системы защиты от кибератак [1]. Опытные злоумышленники способны реализовать продуманные стратегии атак, которые включают [2]:

- сбор информации о ТКС при реализации атаки, идентификацию уязвимостей и защитных механизмов;
- определение путей преодоления защитных механизмов (в том числе, путем моделирования их поведения);
- подавление, нахождение обходных путей, обман компонентов системы защиты, проведение проб уровня защиты незаметным для системы защиты образом или путем проведения распределенных (и разделенных на части) атак с нескольких хостов;
- формирование сложных многофазных атак, присутствие которых сложно определяется подсистемой защиты ТКС;
- получение доступа к ресурсам, повышение привилегий и внедрение несанкционированного кода в отдельных сегментах ТКС для нарушения конфиденциальности, целостности, доступности в сети в целом;
- скрытие внешних признаков атаки.

Реализация мер противодействия атакам выполняется с помощью системы обнаружения и противодействия атакам (intrusion detection and prevention system, IDPS), которая является многокомпонентной распределенной системой, включающей следующие физические компоненты [2]:

- сенсоры, предназначенные для сбора разнотипной информации;
- защищенные каналы для обмена информацией;
- распределенные компоненты обработки информации;
- единый центр или распределенные компоненты принятия и исполнения решения.

IDPS должна поддерживать работу в режиме реального времени для проведения следующих операций:

- реализации механизмов защиты, соответствующих политике безопасности;
- определения вторжения и предсказания намерений и действий злоумышленника;
- оценки потенциальных уязвимостей, сбора данных и анализа текущего состояния сети и системы защиты;
- проведения ответных действий, включая подавление действий злоумышленника и перераспределение нагрузки между критически важными защитными механизмами;

– уменьшения последствий вторжения и определения уязвимостей, адаптации системы ИБ для лучшего противодействия уже изученным атакам в будущем.

Организация защиты от атак с помощью IDPS строится по следующей схеме:

– воспроизведение ситуации в сети в определенной среде имитации процессов, происходящих в ТКС;
– оценка возможных действий злоумышленника относительно сетевых приложений, элементов и протоколов;
– выявление способов противодействия или направления действий злоумышленника и их документирование с помощью определенного языка программирования;
– инсталляция кода (сценария) нового способа противодействия в базе знаний IDPS.

Именно возможности среды имитации определяют качество нового способа противодействия и увеличения функциональных возможностей IDPS, что естественным образом приведет к улучшению показателей распознаваемости атак. Существующие на сегодняшний день среды имитации обладают своими уникальными возможностями, позволяющими реализовать тот или иной функционал, а также присущими им ограничениями и недостатками. Поэтому задачей работы видится анализ возможностей популярных сред имитации, формирование их рейтинга, а также выдвижение предложений по интеграции их возможностей в рамках единой среды имитации.

1 Обзор сред симуляции систем обнаружения и противодействия атакам

Наиболее популярными средами имитации, обладающими развитыми функциональными способностями, являются NetSim (http://www.nsnam.org/), OMNeT INET Framework (http://www.omnetpp.org/), J-Sim (http://www.j-sim.zcu.cz/), SSF Net (http://www.ssfnet.org/), GTNetS (http://www.ece.gatech.edu/). Функциональные возможности сред представлены в табл. 1.

Таблица 1 – Функциональные возможности сред имитации

Возможность	NetSim	OMNeT	J-Sim	SSF Net	GTNetS
Тип симуляции	время	события	время	события	события
Распределенные вычисления	да	да	нет	нет	да
Основной язык программирования	TCL	Eclipse/ C++	Java	Java, C++	C++
Многоплатформенность	эмулятор	да	java	да	да
Сопряжение с реальным оборудованием	да	нет	нет	нет	нет
Модификация коммуникационной платформы	да	да	нет	нет	нет
Протокольный инжиниринг	нет	нет	нет	нет	нет
Программирование агентов взаимодействия	нет	нет	нет	нет	нет
Определение топологических и функциональных компонентов	да	да	нет	да	да
Розыгрыш соревновательной ситуации между злоумышленником и защищающейся стороной	нет	нет	нет	нет	нет
Поддержка IDMEF [RFC 4765], IDXP [RFC 4767] и протоколов-сателлитов	огранич.	нет	нет	нет	нет

Под протокольным инжинирингом понимается возможность формирования сценария взаимодействия сетевых элементов по накопленным сетевым данным и статистике.

Рассмотрение возможностей сред имитации позволил выявить ряд недостатков, критических для проведения анализа сетевых атак:

- отсутствие возможности розыгрыша случайных ситуаций в сети (фиксированная топология сети и размещение сетевых элементов);
- сложность описания состояния сети при проведении множества атак различного вида или многофазовых распределенных атак;
- отсутствие поддержки функций совмещения действия (кооперации) сетевых элементов и программирования агентов взаимодействия, ответственных за координацию действий сетевых элементов (как для атакующей, так и для защищающейся стороны);
- ограниченность взаимодействия сред имитации (лишь на уровне поддерживаемых форматов данных, да и то не во всех случаях);
- поддержка мультиплатформенности за счет эмуляции платформы, что значительно снижает скорость и эффективность имитации (как правило, эмулятор платформы не позволяет задействовать средства распределенных вычислений, поддерживаемые имитатором).

В общем можно определить, что рассмотренные среды изначально не предназначены для анализа параметров сети в состоянии проведения атак и должны быть дополнены определенным интегрирующим элементы, который позволит формировать программные компоненты и накапливать знания относительно задач IDPS.

2 Построение универсальной среды имитации

Создание и отладка полноценной среды имитации «с нуля» является сложной задачей, что приводит к решению о том, что среда должна быть посредником между различными уже существующими средами имитации и библиотеками шаблонов сетевого взаимодействия (рис. 1).

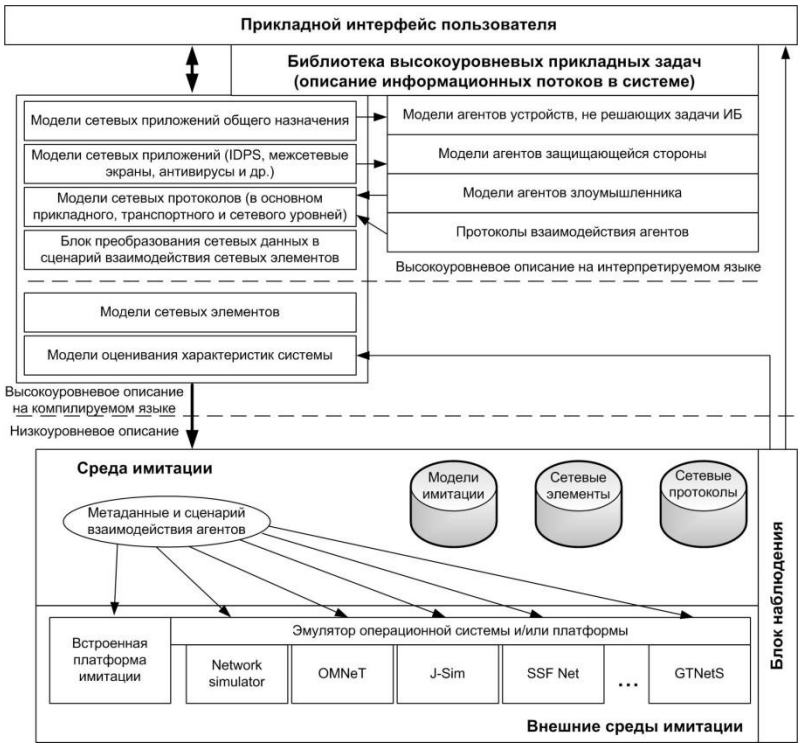


Рис. 1 – Структура среды имитации

Основной идеей универсальной среды имитации процессов (рис. 1) является применение специальной системы интерпретируемых команд, которая преобразуется в специфический для среды имитации и используемой программно-аппаратной платформы набор инструкций (на основе кросс-платформенных языков программирования, таких как C# или Java [3]). Ядром среды является множество моделей: сетевых элементов, протоколов и приложений, информация о которых может быть помещена в общую базу знаний с помощью UML-моделей и моделей конечных автоматов, предоставляемых разработчиками. Большинство современных сред разработки, такие как Visual Studio, Microsoft Visio и другие, позволяют генерировать шаблоны кода на основе диаграмм, формируя библиотеку компонентов на основе кросс-платформенного кода. Используя возможности программного обеспечения промежуточного уровня, такого как CORBA, J2EE, .NET Framework и других, становится возможным проведение прозрачных для разработчика распределенных вычислений и удаленной активации частей среды имитации. Применение агентных архитектур позволяет организовать ролевое управление задачами в имитаторе и логически связать телекоммуникационные процессы и действия атакующей и защищающейся стороны.

Недостатком такого решения является необходимость взаимодействия различных компонентов среды имитации (например, встроенной платформы симулирования и внешних средств имитации) с помощью компонентов-посредников, реализующих интерфейсы взаимодействия, что уменьшает скорость проведения имитации. Такое ограничение частично снимается за счет использования компилируемых языков программирования, поддерживаемых множеством платформ.

Выводы

На основе вышеперечисленного можно сделать вывод, что IDPS является системой с множеством сложных задач и проблем, требующих исследования связей между злоумышленником и подсистемой защиты ТКС. Возможности злоумышленника по проведению атак опираются на возможность анализа информационных потоков и эффективных манипуляций данными на сетевом уровне.

Моделирование и имитация процессов, которые происходят в ТКС во время проведения атак, являются сложными задачами, требующей инструментария с развитыми возможностями. Различные среды имитации предоставляют широкие возможности, однако они ориентированы на решение общесетевых задач и не предназначены для моделирования поведения сетевых элементов, которые управляются атакующей и защищающейся сторонами. Разработка универсальной среды моделирования атак и защитных действий позволит создать общую библиотеку сетевых элементов, протоколов и приложений, использовать распределенные вычисления с применением интерпретируемых языков программирования и сред моделирования параллельных процессов. Связывая среды, ориентированные на «чистое» математическое моделирование (OMNeT, J-Sim и др.) со средами, допускающими использование реального оборудования и высокую распараллеливаемость процесса имитации (например, NetSim), становится возможным масштабирование задачи анализа и управление оборудованием из программ, которые ранее этого не позволяли.

Литература:

1. Kotenko I. Agent-based modelling and simulation of network cyber-attacks and cooperative defence mechanisms. Discrete Event Simulations. Sciyo, In-teh. 2010. P.223-246.
2. Поповский В.В. Защита информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2006.
3. Troelsen A. Pro C# 2010 and the .NET 4 Platform. – NY.: Apress, 2010. – 1753 p.

АДМИНИСТРИРОВАНИЕ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ SQL AZURE

Скляренко С.Е., Быков П.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. Телекоммуникационных систем, тел. (057) 702-55-92
E-mail: discoveryid@gmail.com ; тел. +38(093) 8 121 77 5

Every day we have to increasingly deal with concepts such as cloud technology, computing power, as well as data centers.SQL Azure is a powerful storage infrastructure, data management and analysis. The work is based on SQL Azure component Cloud Fabric, which in turn controls the database instance and ensures their deployment, administration, updating, monitoring and supporting the entire lifecycle of the data. Users are provided with only such tasks as creating a scheme and its maintenance, query optimization, and security management. Understanding of administration and security arrangements SQL Server, is one of the most important and pressing issues in information technology. In this regard, this report focuses on the study of these issues.

С каждым днем нам приходиться все чаще сталкиваться с такими понятиями как облачные технологии, вычислительные мощности, а так же центры хранения данных. SQL Azure является мощной инфраструктурой хранения, управления и анализа данных. Работа SQL Azure базируется на компоненте Cloud Fabric, который в свою очередь управляет экземплярами базы данных и обеспечивает их развертывание, администрирование, обновление, мониторинг и поддерживает весь жизненный цикл работы с данными. Пользователям предоставляется лишь выполнение таких задач, как создание схемы и ее поддержание, оптимизация запросов и управление безопасностью. Понимание вопросов администрирования и механизмов обеспечения безопасности SQL Server, является одним из важнейших и актуальных вопросов в информационных технологиях. В связи с этим, данный доклад посвящен изучению этих вопросов.

SQL Azure является службой реляционных баз данных на платформе Windows Azure. Преимущества использования базы данных SQL Azure включают управляемость, высокий уровень доступности, масштабируемости, хранения, а так же управления и анализа данных.

База данных SQL Azure размещается на серверах, реализующих технологии SQL Server в центрах обработки данных Microsoft. С точки зрения архитектуры существует четыре разных уровня абстракции, которые работают совместно и обеспечивают реляционную базу данных, которой пользуются создаваемые приложения: уровень клиента, уровень служб, уровень платформы и уровень инфраструктуры.

В ходе анализа SQL Azure было показано, что при обеспечении безопасности баз данных SQL Azure необходимо рассматривать следующие вопросы:

- Брандмауэр;
- Шифрование и проверка сертификатов;
- Проверка подлинности;
- Имена входа и пользователи.

Первоначально весь доступ к серверам SQL Azure блокирован брандмауэром SQL Azure, попытки соединения с сервером SQL Azure, исходящие из Интернета или Windows Azure, будут неудачными. Чтобы начать использование сервера SQL Azure, необходимо подключиться к порталу управления и указать один или несколько параметров брандмауэра, разрешающих доступ к серверу SQL Azure. С помощью параметров брандмауэра указать область разрешенных IP-адресов из Интернета, а также то, разрешаются ли приложениям Windows Azure попытки подключения к серверу SQL Azure. Это можно осуществить с использованием портала управления платформой Windows Azure или программным путем с использованием средств «Операции с правилами брандмауэра», до-

ступ к которым предоставляет API REST управления базами данных API сервера SQL Azure. Кроме того, после организации доступа можно использовать базу данных **master** для просмотра и изменения настроек брандмауэра программным путем. Также, стоит отметить, что доступ к службе баз данных SQL Azure предоставляется только через порт 1433 протокола TCP. Для обеспечения доступа к базе данных SQL Azure следует убедиться в том, что применяемый брандмауэр разрешает исходящие соединения через порт 1433 протокола TCP.

Когда компьютер пытается подключиться к серверу SQL Azure из Интернета, брандмауэр SQL Azure проверяет исходный IP-адрес запроса, сравнивая его с полным набором параметров брандмауэра. Если IP-адрес запроса не принадлежит ни к одному из указанных диапазонов, попытка соединения блокируется и не достигает сервера SQL Azure.

Если приложение пытается выполнить подключение к серверу SQL Azure из Windows Azure, брандмауэр SQL Azure отыскивает определенный параметр брандмауэра, указывающий, разрешены ли соединения с Windows Azure.

Параметр брандмауэра с начальным и конечным адресом, равным 0.0.0.0, указывает, что соединения с Windows Azure разрешены. Если IP-адрес запроса не находится в пределах одного из указанных диапазонов, попытка соединения блокируется и не достигает сервера SQL Azure.

База данных SQL Azure обеспечивает полноценное многопользовательское обслуживание баз данных на основе общих источников.

Чтобы обеспечивались хорошие условия работы для всех клиентов базы данных SQL Azure, предложено соединение клиента со службой закрыть при возникновении следующих условий:

- Чрезмерное использование ресурсов;
- Соединения, неактивные в течение 30 минут и более;
- Отработка отказа в результате сбоя сервера.

Весь обмен данными между База данных SQL Azure и конкретным приложением (SSL) требует постоянного шифрования. SQL Azure не поддерживает незашифрованные подключения и имеет подписанный сертификат, выпущенный центром сертификации. Эти факторы также помогают обеспечить защиту передачи данных и предотвратить сетевые атаки с посредником (man-in-the-middle attacks).

Подтверждение шифрования происходит в потоке PRELOGIN протокола TDS. Это требуется для всей клиентский связи с SQL Azure, включая SQL Server Management Studio и приложения через ADO.NET.

Для обеспечения проверки сертификатов с помощью прикладного кода или специальных инструментов следует запрашивать зашифрованное соединение и не доверять сертификатам сервера. Если прикладной код или специальные инструменты не запрашивают зашифрованное соединение, то все равно получают зашифрованные соединения. Но эти программные средства могут не проверять сертификаты сервера, поэтому становятся восприимчивыми к атакам путем перехвата сообщений.

При соединении с базой данных в SQL Azure с помощью приложения ADO.NET следует учитывать следующие аспекты:

- Предотвращать атаки по принципу внедрения кода с применением класса Sql Connection String Builder. Он предоставляется в составе платформы .NET Framework в целях упрощения создания строки подключения;
- Тщательно защищать применяемую строку подключения. Строка подключения становится источником потенциальной уязвимости, если она не защищена;
- В целях полной защиты применяемого соединения, особенно при подключении к SQL Azure по Интернету, обязательно задать параметры соединения Encrypt и TrustServerCertificate платформы ADO.NET. Задать значение свойства соединения Encrypt, равное True (Encrypt = True), и значение свойства соединения

TrustServerCertificate, равное False (TrustServerCertificate = False). Это позволяет создать зашифрованное соединение и сделать невозможными какие-либо атаки путем перехвата сообщений.

Среда SQL Server Management Studio также поддерживает проверку сертификатов. В диалоговом окне «**Подключение к серверу**» следует выбрать параметр «**Шифровать соединение**» во вкладке «**Свойства**».

База данных SQL Azure поддерживает только проверку подлинности SQL Server. Проверка подлинности Windows (с помощью встроенных средств защиты) не поддерживается. Пользователи должны предоставлять учетные данные (имя входа и пароль) при каждом своем подключении к базе данных SQL Azure.

Для предотвращения снижения производительности повторная проверка подлинности в соединении не проводится сразу же после переустановки пароля базы данных SQL Azure, даже если это соединение переустанавливается в результате выполнения операций с пулом соединений. В этом состоит отличие от поведения локального экземпляра SQL Server. Вместо этого база данных SQL Azure прибегает к использованию механизма повторной проверки подлинности при разъединении просроченных сеансов. После того как в любом соединении по прошествии более 60 минут после последней повторной проверки подлинности выдается новый запрос, выполняется повторная проверка подлинности. Если пароль был изменен, попытка выполнения запроса окончится неудачей и произойдет разрыв соединения.

Администрирование безопасности в базе данных SQL Azure аналогично администрированию безопасности в локальном экземпляре SQL Server. Управление безопасностью на уровне базы данных практически полностью идентично, если не рассматривать различия в применимости нескольких параметров. Ключевой проблемой в администрирование баз данных SQL Azure является разграничение прав пользователей, это тот аспект, на который следует обратить особое внимание.

Сервер SQL Azure задает дополнительный уровень абстракции, на котором определяется группирование баз данных. Базы данных, связанные с конкретным сервером SQL Azure, могут размещаться на разных физических компьютерах в центре обработки данных Microsoft. Для администрирования на уровне сервера всеми этими базами данных используется отдельная база данных с именем **master.**

База данных **master** содержит имена входа и сведения о том, какие имена входа имеют разрешения на создание баз данных или других имен входа. Для выполнения операций CREATE, ALTER или DROP с именами входа или базами данных необходимо подключение к базе данных **master**. База данных **master** также содержит представления sys.sql_logins и sys.databases, которые можно использовать для просмотра соответственно имен входа и баз данных.

Для подключения к базе данных SQL Azure с использованием созданных имен входа сначала необходимо предоставить каждому из таких имен входа разрешения уровня базы данных, используя команду CREATE USER. В некоторых средствах поток табличных данных (TDS) реализован иначе, поэтому может потребоваться добавить имя сервера SQL Azure к имени входа в строке подключения с помощью нотации <login>@<server>.

Чтобы имена входа, которые не являются именем входа субъекта серверного уровня, могли управлять безопасностью уровня сервера, в базе данных SQL Azure реализованы две роли безопасности: loginmanager - для создания имен входа и dbmanager - для создания баз данных. Эти роли могут назначаться только пользователям в базе данных **master**.

Аналогично роли securityadmin в локальном экземпляре SQL Server, роль loginmanager в базе данных SQL Azure необходима для создания имен входа. Создавать другие имена входа могут только имена входа субъекта серверного уровня и имена входа, относящиеся к роли loginmanager.

Таким образом, в ходе анализа работы SQL Azure можно предложить ряд дополнений, которые будут повышать безопасность и стойкость работы с данными в облаках:

1. Ограничение количества передаваемых и принимаемых пакетов в определенный промежуток времени, после чего будет выполняться запрос на повторную аутентификацию;

2. Реализация алгоритма проверки подлинности Windows-Server-SQL Server$

3. Внедрение программ и алгоритмов генерации хэш-функций отправляемых данных аутентификации и сравнение полученных значений; проверка значений хэша полученных данных маркера доступа с хэшем отправленных данных;

4. Повышение безопасности передачи данных при работе клиента с севером Azure (дополнительный процесс шифрования данных передачи клиент-сервер);

5. Разграничение прав пользователей при работе с облаками (администраторы, пользователи, продвинутые пользователи – одни имеют право чтения и изменения любых данных и любых настроек, в том числе и политик доступа; вторые имеют право лишь чтения и записи данных, без возможности удаления; а последние чтения, изменения и удаления данных).

Литература:

1. http://msdn.microsoft.com/ru-ru/library/ee872418.aspx

2. http://msdn.microsoft.com/ru-ru/library/ee336243.aspx

3. http://msdn.microsoft.com/practices

4. Кейт Браун. Руководство по Microsoft .NET Access Control Service для разработчиков. 2009.

ПОДХОД К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ С УЧЕТОМ КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ СРЕДСТВ НАПАДЕНИЯ И ЗАЩИТЫ

Снегуров А.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-06,
E-mail: arksn@rambler.ru ; факс (057) 702-11-13

The report consider the approach to assessing information securitys risks in view of the conflict interaction of defense and attack

Постановка проблемы. Современные телекоммуникационные системы (ТКС) относятся к сложным территориально-распределенным организационно-техническим системам. Данные системы включают в себя как технические подсистемы и средства, так и персонал, их эксплуатирующий. Одним из основных требований к телекоммуникационным системам является обеспечение конфиденциальности, целостности и доступности информации, циркулирующей в них. Реализация данных требований осуществляется проведением комплекса организационных и технических мероприятий в рамках функционирования системы управления информационной безопасности (СУИБ) организации, эксплуатирующей телекоммуникационную систему.

Функционирование СУИБ ТКС на современном этапе происходит в следующих особенностях:

1. Активными темпами развиваются способы и средства нарушения информационной безопасности ТКС. При этом атаки могут осуществляться как с использованием сложных технических решений (DDOS-атаки, использование различного вредоносного программного обеспечения, съем информации через побочные излучения и наводки компьютерной техники, различные виды мошенничества, осуществление неправильной маршрутизации* и т.д.), так и простым стиранием информации или ее копированием на электронные и бумажные носители.

2. Особенностью функционирования СУИБ ТКС является неопределенность относительно атакующей стороны, характера и времени атаки. Осуществление атак на ТКС может подчиняться некоторым принципам. К ним можно отнести внезапность и активность атаки (для этого атакующая сторона может заблаговременно изучить слабые и уязвимые стороны СУИБ, оценить способы защиты, выбрать наиболее эффективные свои действия), комплексность нападения (атаки на разные подсистемы, проведения различных видов атак, согласование различных атак по времени). Атака может быть осуществлена в наиболее неблагоприятный для СУИБ временной промежуток: ночь, выходные, периоды наибольшей нагрузки на ТКС, периоды времени, когда ТКС решает важнейшие задачи.

В этих условиях эффективное функционирование СУИБ ТКС позволяет телекоммуникационной системе функционировать с заданными показателями качества обеспечивая тем самым бизнес-процесс организации, ее эксплуатирующей.

Согласно международному стандарту ISO/IEC 27001-2005, система управления информационной безопасностью - это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности».

Процессы оценки и управления рисками информационной безопасности являются одними основных процессов при проектировании и эксплуатации СУИБ. Именно реализация данных процессов позволяет ответить на четыре основных вопроса: Что защищать? От кого защищать? Почему это нужно защищать? И как защищать?

Подход к оценке риска ИБ в настоящее время основывается на учете вероятности угрозы (частоты реализации угрозы), степени ее опасности и ценности ресурса, на который может быть реализована угроза [1]. Определение данных показателей осуществляет-

ся в реальной практической деятельности, как правило, экспертным путем. Такой показатель, как степень опасности угрозы, определяет эффективность реализации угрозы при существующих средствах защиты (или эффективность средств защиты для определенных угроз).

Одним из проблемных вопросов, возникающих при оценке данных показателей, является необходимость учета конфликтного взаимодействия средств защиты и нападения. Рассмотрение такого конфликтного взаимодействия позволяет учесть возможность опережения в действиях противоборствующей стороны. Так время реакции СУИБ показывает возможность данной системы своевременно обнаружить и распознать угрозу, принять решение на использование адекватных способов и средств защиты, их активизировать. Своевременность реакции СУИБ означает, такие действия данной системы, при которых защитные мероприятия запускаются до того, как произошло нарушение конфиденциальности, целостности и доступности информации при возникновении угрозы (атаки). Кроме того, актуальность такого подхода для организационно-технических систем обусловлено тем, что он позволяет учесть выбор нападающей и защищающейся сторонами разных стратегий поведения и вариантов своих действий в различных условиях обстановки, наличие или отсутствие информации о действии противоборствующей стороны. Такой подход также позволяет учесть человеческий фактор в обеспечении информационной безопасности в организации.

Цель исследования – рассмотрение подхода к оценке рисков информационной безопасности телекоммуникационных систем с использованием аппарата конфликтного взаимодействия атакующей стороны и системы управления информационной безопасностью.

Оценка риска информационной безопасности ТКС с учетом вышеуказанного подхода, на наш взгляд, должна быть многоуровневой, при котором каждый из уровней определяется масштабом рассматриваемых процессов (рис.1). Такой подход позволяет осуществить декомпозицию конфликта высокого иерархического уровня на составляющие его более «простые» конфликты.

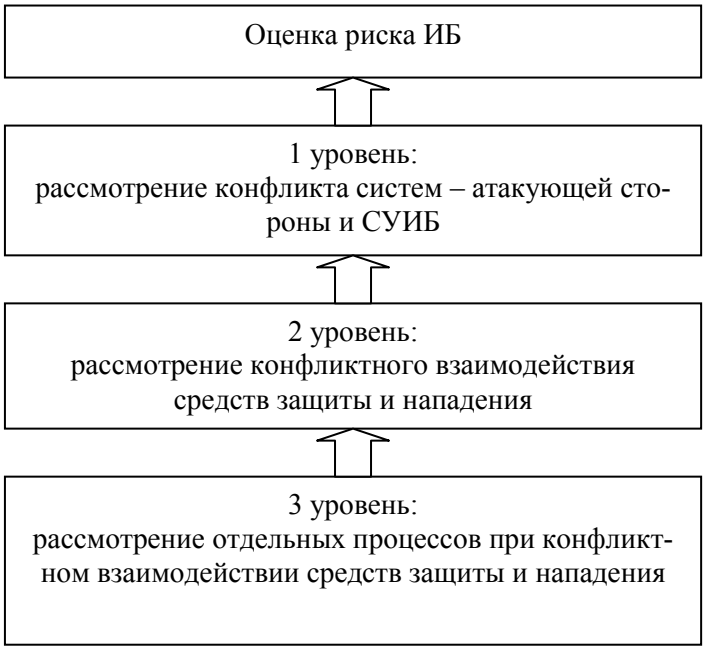
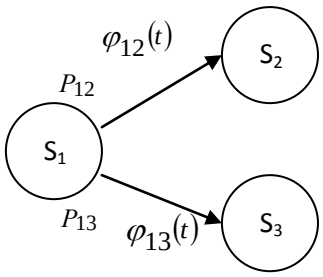


Рис. 1 – Уровни рассмотрения конфликтного взаимодействия атакующей стороны и СУИБ

На 1 уровне детализации конфликта осуществляется учет стратегии и тактики действия конфликтующих сторон, выбор ими рефлексии различного уровня, использование атакующей стороной комплексной атаки через разные каналы, возможность ведения раз-

ведки и имитирующих действий атакующей стороной и т.д. На данном этапе анализируются все уязвимые места в СУИБ ТКС, все возможные средства нападения, которые может выбрать атакующая сторона.

На 2 уровне осуществляется рассмотрение конфликта конкретных средств нападения и защиты, например, вредоносное программное обеспечение – антивирусные пакеты, средства проникновения в ТКС – системы обнаружения вторжения и т.д. Существующий подход к учету конфликтной обусловленности функционирования противоборствующих средств основывается на использовании теории полумарковских процессов [2,3]. Данный подход предполагает представление действий атакующей стороны и средств защиты в виде графа состояний.



Где S_1 – начальное состояние – начало конфликта, S_2 и S_3 – состояния выигрыша конфликтующих средств.

Переход из одного состояния в другое описывался в виде двух типов показателей: вероятностей перехода P_{12}, P_{13} и плотностей вероятности времени перехода $\varphi_{12}(t)$ и $\varphi_{13}(t)$. Решение системы интегральных уравнений (1) позволяет определить вероятность достижения конечного состояния конфликта – выигрыш нападающего или выигрыш средства защиты в зависимости от всех характеристик конфликтующих сторон, в том числе и временных.

$$P_2(t) = P_{12}\int_0^t \varphi_{12}(t)\left[1 - F_{13}(t)\right]d\tau,$$

$$P_3(t) = P_{13}\int_0^t \varphi_{13}(t)\left[1 - F_{12}(t)\right]d\tau, \qquad (1)$$

где $P_2(t), P_3(t)$ - вероятность достижения выигрыша в конфликте с учетом упреждения противоборствующей стороны;

$F_{12}(t), F_{13}(t)$ - вероятности выполнения бесконфликтных действий при отсутствии противодействия.

На 3 уровне детализации конфликта осуществляется углубленное рассмотрение отдельных процессов конфликтного взаимодействия средств нападения и защиты, например, процесс обнаружения зловредным ПО нужной атакующему информации в базе данных, процесс обнаружения атаки системами обнаружения вторжений, процесс физического проникновения через систему охрану злоумышленника к ресурсам ТКС и т.д. На данном этапе необходимо определить показатели конфликтного взаимодействия средств нападения и защиты, необходимые для 2 уровня детализации конфликта: плотность вероятности длительности процесса, вероятности обнаружения, распознавания, уничтожения и т.д.

Такой подход к оценке риска позволяет учесть все особенности конфликта сложных систем, которыми являются СУИБ и нападающая сторона, учесть возможность опережения в действиях противоборствующей стороны, предъявить требования к основным характеристикам как отдельных средств обеспечения информационной безопасности, так и всей системы управления информационной безопасностью в целом.

Литература:

1. Астахов А.М. Искусство управления информационными рисками [Текст] – М.: ДМК Пресс, 2010. – 312 с.

2. Будников С.А., Барсуков О.М., Сербов Д.А. Федукович З.Б. Анализ требуемого качества конфликтного функционирования информационных радиоэлектронных средств [Текст] / С.А. Будников, О.М. Барсуков, Д.А.Сербов, З.Б. Федукович // Радиотехника. – 2009. - № 5. – С. 88 – 91.

ПОДХОД К ВЫЯВЛЕНИЮ ИНСАЙДЕРОВ НА ОСНОВЕ МЕТОДОВ ВИЗУАЛЬНОЙ ПСИХОДИАГНОСТИКИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

Снегуров А.В., Романчук Е.Ю.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-06,
E-mail: arksn@rambler.ru ; факс (057) 702-11-13

In this report the issue of fighting with insiders is considered, and the method of assessment of employees emotional condition is offered, which is based on the mathematic apparatus of the fuzzy logic.

Постановка проблемы. В настоящее время одной из ключевых угроз информационной безопасности продолжает оставаться инсайдерская деятельность. Так, например, в результате опроса, проведенного корпорацией Symantec и сообществом Профессионалы.ru. выяснилось [1], что 70% сотрудников российских компаний выносят с работы конфиденциальные данные. 68% опрошенных допустили утечку через социальные сети, 56% сознались, что выносили секреты на флешке. По результатам онлайн-опроса, проведенного компанией SailPoint [2] 29% американцев и 23% британцев, меняя место работы, готовы украсть у предыдущих работодателей базы данных клиентов. 15% американцев и 17% британцев могут взять с собой внутреннюю документацию, планы компании и дизайн продуктов. Опрос с участием 500 айтишников, проведенный Government Technology [3] показал, что примерно 40% IT-специалистов в случае чего могут взять в заложники сеть работодателя. Исследование, проведенное компанией Venafi, также показало, что треть респондентов уверена в том, что их знаний и полномочий достаточно, чтобы парализовать работу компании.

По ряду проводимых исследований [1] причины утечек кроются в небрежности (у 37% опрошенных корпоративные ноутбуки лежали без присмотра в общественных местах), беспечности (50% используют простые пароли, а 10% и вовсе приклеивают их возле компьютера), излишней доверчивости (68% не гнушаются попросить друзей помочь с особо трудным корпоративным файлом). Около 9% сознались, что подумывали продать конфиденциальную информацию на сторону, 6% так и сделали, а 45% отправляли данные по запросу клиентов.

В настоящее время существует следующая классификация инсайдеров в зависимости от механизма реализации ими зловредных действий и мотивации на нарушение информационной безопасности [4]. Халатные - сотрудники, которые по своей халатности допустили нарушение конфиденциальности, целостности или доступности информации (КЦД). Манипулируемые - сотрудники, подвергшиеся атакам методами социальной инженерии. Обиженные - сотрудники, которые по личным мотивам стремятся нанести вред компании. Нелояльные - сотрудники, как правило, меняющие место работы и уносящие всю информацию, до которой были доступны. Завербованные - сотрудник изначально лояльный, а затем подкупленный либо запуганный. Внедрённые - сотрудники специально устроенный в организацию для похищения информации.

Решение проблемы борьбы с инсайдерами имеет несколько направлений:

1. Выявление предрасположенности к инсайдерству. Данные механизмы позволяют определить возможность сотрудников стать халатными, манипулируемыми, обиженными, нелояльными инсайдерами.

2. Определение того факта, что сотрудник стал инсайдером. Механизмы, реализующие данное направление, должны позволять выявлять все типы инсайдеров. При этом наиболее сложно выявить внедренного инсайдера, который может быть специально подготовлен к такой деятельности.

3. Реализация организационно-технических мероприятий по защите информации от инсайдеров.

Одним из перспективных механизмов борьбы с инсайдерством является использование методов визуальной психодиагностики как для выявления предрасположенности анализируемого сотрудника к инсайдерской деятельности, так и для выявления инсайдера. Следует заметить, что результаты визуальной психодиагностики должны использоваться в рамках комплекса организационно-технических мероприятий борьбы с инсайдерами. Определение психологических характеристик человека по его телесным (внешним), подсознательным проявлениям позволяет повысить адекватность принятия решения руководителей, особенно при допуске сотрудников к критической для организации информации.

Целью исследования является рассмотрение проблемы борьбы с инсайдерством, разработка методов визуальной психодиагностики для повышения эффективности обеспечения информационной безопасности организаций.

Согласно исследованиям учёных в данной области, широко известны данные о том, что в течение первых 12 секунд общения, при знакомстве, на долю невербальных сигналов приходится примерно 92 % всего объема принимаемой информации. Кинесические исследования Ф. Селже говорят о том, что при разговоре значимость слов составляет лишь 7%, интонация — 38%, а на жесты и мимику приходится 55% [5]. Жесты могут рассказать: о характере, о темпераменте, об отношении к партнеру, об эмоциональном состоянии человека, о попытке обмана и т.д. Невербальные движения, используемые человеком, трудно им контролируются, что позволяет использовать их для оценки ситуаций в сфере информационной безопасности.

В исследовании были рассмотрены и классифицированы наиболее часто используемые основные жесты и позы. Рассмотрены следующие виды жестов: жесты-симптомы, выполняющие функцию самовыражения: выражают состояние, процессы, модальные (выражают оценку субъектом чего-либо); жесты-регуляторы, которые выполняют регулятивно-коммуникативную функцию воздействия на партнера; жесты-информаторы, выполняющие информативно-коммуникативную функцию. В ходе исследования были рассмотрены шесть основных эмоциональных состояний (гнев, радость, страх, печаль, удивление и отвращение) универсальных для всех людей. Для каждого эмоционального состояния были приведены их основные мимические проявления. В исследовании предложен способ описания эмоциональных состояний человека и их распознавания на основе математического аппарата нечеткой логики.

Направлениями дальнейших исследований является выявление всех особенностей поведения инсайдеров, автоматизация процессов съема информации при осуществлении визуальной психодиагностики, автоматизация процессов комплексной обработки информации при выявлении инсайдеров.

Литература:

1. Ульянов В.В. Динамика безопасности: от внешних угроз – к внутренним [Текст] / В.В.Ульянов // Защита информации. INSIDE. – 2008. - № 4. – С. 34 – 38.

2. 70% сотрудников крадут корпоративные секреты [Электронный ресурс] / Securitylab - Режим доступа: URL: http://www.securitylab.ru/news/405499.php. - 27 апреля, 2011. - Загл. с экрана.

3. Уволенные офисные сотрудники чаще воруют данные, чем вещи [Электронный ресурс] / Securitylab - Режим доступа: URL:http://www.securitylab.ru/news/396974.php. - 23 августа, 2010. - Загл. с экрана.

4. 40% IT-специалистов готовы взять в заложники сеть работодателя [Электронный ресурс] / Securitylab - Режим доступа: URL:http://www.securitylab.ru/news/405783.php. - 01 июня, 2011. - Загл. с экрана.

5. Петрова Е.А. Жесты в педагогическом процессе. [Текст] / Е. А. Петрова. - М.: Педагогическое общество России , 1998. – 222 с.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ, ПОСТРОЕННЫХ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ»

Снегуров А.В., Ткаченко Е.А., Кравченко А.Д.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-06,
E-mail: arksn@rambler.ru ; факс (057) 702-11-13

The report considered the problem of information security systems based on technology of "smart house", discussed the threats of information security for such systems.

Постановка проблемы. Технология «Умный дом» является одной из наиболее перспективных для управления сервисом офисных и производственных помещений, жилых зданий. Автоматизация управления всеми процессами жизнеобеспечения является настолько привлекательной, что приводит к огромному предложению на рынке данных услуг различными компаниями. По данным экспертов компании YORK International [1], прогнозируется ежегодный рост рынка систем, использующих данную технологию, на 20-25% в год. Автоматизированное управление электро-, водо-, газо-, теплоснабжением, кондиционированием, мониторинг различных процессов позволяют не только уменьшить эксплуатационные затраты, но и повысить безопасность персонала (жильцов).

Однако внедрение данной технологии влечет за собой появление новых проблем, связанных информационной безопасностью. Так уже в мире произошло ряд атак на информационные системы энергогенерирующих, промышленных компаний, управления транспортом, системы управления водоснабжением [2-4]. Следует ожидать увеличение подобных атак в будущем.

Учитывая экономическую подоплеку большинства атак на информационные ресурсы организаций можно отменить, что подобные атаки на систему «Умный дом» могут иметь целью шантаж с дальнейшим вымоганием денег, дезорганизация работы конкурирующей организации, получение конфиденциальной информации о деятельности конкурирующей организации (VIP-жильцов) и т.д.

Целью доклада является рассмотрение проблемы обеспечения информационной безопасности интеллектуальных систем, построенных по технологии «Умный дом», выделение основных угроз информационной безопасности, возникающих при эксплуатации систем, построенных с использованием данной технологии.

Рассмотрим угрозы информационной безопасности систем, построенных по технологии «Умный дом». Считаем, что базовыми классическими угрозами информационной безопасности являются нарушение конфиденциальности, целостности и доступности (КЦД) информации.

Под конфиденциальностью информации в данном исследовании мы понимаем невозможность утечки конфиденциальной информации организаций (лиц), эксплуатирующих «Умный дом», через его подсистемы (например, через телекоммуникационную сеть).

Под доступностью информации мы понимаем такое состояние системы, при котором легальные пользователи (и сама система), используя элементы «Умного дома», имеют доступ к информации о состоянии системы и могут реализовывать разрешенные в системе действия (открывать двери, включать кондиционирование или систему пожаротушения, отключать газ или воду в случае утечки, мониторить ситуацию и т.д.). Нарушение доступности информации может привести к невозможности системы реагировать на различные ситуации, в том числе и аварийные. Примером может быть ситуация утечки газа при которой система не может провести необходимые отключения, запустить вентиляцию вследствие нарушения доступности информации.

Под целостностью информации мы понимаем такое состояние системы, при котором легальные пользователи (и сама система) получают достоверную информацию о состоянии подсистем «Умного дома». Получение системой недостоверной информации о температуре в помещениях, наличии пожара, утечки газа и воды, физическом проникно-

вении нарушителя в здание и т.п. приведет к неадекватным ее действиям (например, к включению системы пожаротушения, перекрытию воды и т.д.).

Из примеров видно, что нарушение конфиденциальности, целостности и доступности информации в системе, построенной по технологии «Умный дом», может привести как к дезорганизации работы организаций (лиц), ее эксплуатирующих, так и к катастрофическим последствиям.

Выделим наиболее вероятные угрозы, через которые может произойти нарушение информационной безопасности анализируемой системы. При этом будем учитывать, что данная система построена по централизованной схеме, где управление осуществляется через центральный сервер.

Таблица1 – Вероятные угрозы информационной безопасности систем, построенных по технологии «Умный дом»

№ п/п	Тип атаки	Уязвимость	Возможные последствия
1	Хакерские атаки на центральный сервер, влияние вредоносного программного обеспечения (ПО) на функционирование системы	Подключение сети «Умного дома» к Интернет. Отсутствие (неэффективность) механизмов защиты периметра сети	Нарушение работы, либо выход из строя центрального сервера, а следовательно и всей системы. Нарушение КЦД информации
2	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам или к зоне устойчивого перехвата радиосигналов сети. Отсутствие (неэффективность) механизмов защиты трафика	Нарушение конфиденциальности информации передаваемой по каналу. Возможен захват управления системой
3.	Радиоэлектронное подавление беспроводных каналов передачи информации	Возможность доступа злоумышленника к зоне, где возможно радиоэлектронное подавление беспроводных каналов передачи информации	Нарушение доступности и целостности информации
4	Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
5	Доступ к сети неавторизованных пользователей.	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
6	Наличие нарушителей в числе обслуживающего персонала (охранники, наладчики, уборщики и др.)	Отсутствие (неэффективность) организационных мероприятий по отбору и контролю за персоналом	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного обслуживания оборудования. Уровень опасности зависит от степени доступа инсайдера к системе

7	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Отсутствие (неэффективность) – физической охраны объекта	Нарушение КЦД информации
8	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
9	Стихийные бедствия (пожар и др.)	Отсутствие (неэффективность) механизмов защиты	Дезорганизация работы системы
10	Поломка аппаратуры системы	Низкая надежность оборудования, низкая квалификация персонала	Нарушение КЦД информации
11	Ошибки программного обеспечения	Использование нелицензионного ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КЦД информации
12	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Наличие ПЭМИ компьютерной техники. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны	Нарушение конфиденциальности информации, обрабатываемой на ЭВМ
13	Утечка информации по акусто-электрическому каналу	Наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	Нарушение конфиденциальности информации

Исходя из результатов оценки самыми опасными являются те угрозы, при которых злоумышленник может брать под контроль всю систему. Поэтому крайне необходимым является проведение мероприятий по защите телекоммуникационной сети, разграничение прав доступа пользователей, защита от инсайдеров. Опасными являются угрозы потери электропитания, пожар в серверной, поломки оборудования и отказ программного обеспечения, отвечающего за централизованное управление системой. Реализация данных угроз может привести к катастрофическим последствиям для всей системы.

В настоящее время на кафедре телекоммуникационных систем ХНУРЭ проводятся исследования, посвященные анализу всех потенциальных угроз и уязвимостей систем, построенных по технологии «Умный дом», разрабатываются методики оценки результатов воздействия различных угроз на уязвимые элементы данных систем, разрабатываются предложения по повышению их информационной безопасности.

Литература:

6.Перспективы рынка систем "Умный дом" [Электронный ресурс] / Центр инженерных технологий CENTEC. — Режим доступа: \www/ URL: http://www.centecgroup.ru/press/articles/18/ — 02.03.2011 г. — Загл. с экрана.

2. Хакеры оставили без электричества 3 млн бразильцев [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/387521.php: - 10.11.2009 г. — Загл. с экрана.

3. Энергосистема Австралии спасена благодаря Linux [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/386273.php: 06.11. 2009 г. — Загл. с экрана.

4. McAfee сообщила о росте числа ИТ-атак на промышленные объекты [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/405455.php: 10.11.2009г. — Загл. с экрана.

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ СИСТЕМАХ

Шаповалов И.В., Добрынин И.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. ТКС, тел. (057) 702-55-92
E-mail: Shapovalovstd@gmail.com

Cloud computing is a fast developing technology in which information is stored and processed on the remote servers. Security of the information, which is stored and processed in cloud systems, is important part of this new technology. According to social analysis, security of the information and trusting to the service providers are the most important problems of cloud computing. This work represents methods of securing data, which is stored in the cloud.

В связи с тем, что в облачных системах вся информация хранится и обрабатывается на стороне провайдера услуг, необходимо обеспечить ее конфиденциальность, целостность и доступность. Очень остро на данный момент стоит вопрос доверия провайдерам облачных услуг, что, в свою очередь, отстраняет многих потенциальных пользователей от использования облачных технологий. В данной работе представлены методы обеспечения конфиденциальности информации, обрабатываемой центром обработки данных (далее ЦОД), а так же управление доступом к данной информации.

На данный момент для защиты информации в ЦОД применяется шифрование, при этом информация шифруется на стороне провайдера. Однако для работы с ней необходимо проихводить обратную операцию – расшифрование. При этом доступ к информации может быть получен посторонними лицами, так как от ЦОД информация передается уже в открытом виде, хотя и с использованием различных протоколов защиты информации. Так же возможены злоумышленные действия со стороны ЦОД. В таком случае злумышленнику не придется проводить сложную атаку, так как вся ключевая информация хранится в датацентрах.

Для предотвращения подобных атак в данной работе предлагается использование посредника. Под посредником будем подразумевать сервер, установленный на стороне клиента, который будет производить шифрование и расшифрование данных.

Принцип работы представленной модели заключается в следующем:

1. Клиент проходит аутентификацию на сервере-посреднике.
2. Клиент при помощи посредника обращается к провайдеру услуг для загрузки информации на виртуальный сервер, расположенний на стороне провайдера.
3. Посредник производит шифрование передаваемых данных. При этом ключевая информация может как храниться на сервере-посреднике, так и выделяться при аутентификации клиента на сервере-посреднике..
4. Зашифрованная информация отправляется на сервер провайдера.

При применении данной модели провайдеру передается уже зашифрованная информация, что предотвращет атаки инсайдеров на хранящуюся в датацентрах информацию. Однако при этом нарушается клиент-серверная модель, от клиента требуются затраты на сервер-посредник Так же, для работы с посредником удаленно, необходима организация защищенного канала между клиентом и сервером-посредником. Применение данной модели целесообразно в случае использования облачных серверов организациями с большим числом пользователей. Однако необходимо помнить, что при увеличении числа пользователей возрастает нагрузка на сервер-посредник. Стоит заметить, что аутентификация производится два раза, первый раз – клиент аутентифицируется на сервере-посреднике, и второй раз – сервер-посредник аутентифицируется на сервере услуг.

Второй метод отличается от первого отсутствием сервера-посредника. При этом используется приложение, встраеваемое в браузер. При этом так же происходит аутентификация в приложении. Принцип работы данной модели практически не отличается от принципа работы предыдущей, за исключением того, что клиент через приложение производит обращения к серверу провайдера. При использовании данной модели отсутствует

необходимость в сервере-посреднике и, соответственно, и в установлении защищенного канала между клиентом и посредником. Однако при использовании данной модели нагрузка ложится на локальные машины клиента. К тому же из-за необходимости аутентификации в приложении необходимо обеспечить репликацию учетных записей с разных клиентских машин. Так же, в отличии от предыдущей модели, в которой аутентификация была централизованной, в данной модели она децентрализованна.

Оба этих метода объеденяет то, что инициатива обеспечения защиты информации исходит со стороны клиента, и провайдер в этом никакого участия не принимает.

Третий метод требует инициативы как от клиента, так и от провайдера услуг. В нем так же используется приложение. Только в данной модели оно не просто производит аутентификацию и шифрование и расшифрование данных. Данное приложение представляет собой API виртуального сервера, с помощью которого происходит аутентификация на самом сервере, а не в приложении, как в предыдущем случае. Шифрование и расшифрование происходит на машине клиента, что позволяет исключить возможность раскрытия конфиденциальной информации злоумышленниками.

Для шифрования информации, передаваемой в ЦОД, в данной модели рекомендуется использование потоковых шифров или блочных шифров в режиме OFB. Эти шифры обеспечивают должную защиту и при этом возможность изменения данных клиентом. При этом ключи шифрования хранятся на машине клиента или, в случае использования сервера-посредника, выделяются из аутентификационных данных. Однако при этом следует учесть, что преобразования аутентификационных данных для выделения ключей должны отличаться от преобразований для проведения аутентификации, а именно – для выделения хэшей для проведения аутентификации, так как в этом случае злоумышленник может получить ключ сразу, не проводя криптоанализа.

Аутентификация в приложении, за исключением API, может выполнятся по принципу простого объявления аутентификационных данных. Для API аутентификация выполняется по протоколу CHAP, Kerberos или другому протоколу, в котором аутентификационные данные не передаются в открытой форме. Метод аутентификации в данном случае выбирает провыйдер услуг. При аутентификации на сервере-посреднике возможна аутентификация при помощи протокола PAP, в том случае, если аутентификация происходит внутри локальной сети организации и не допускает удаленного соединения. В случае удаленного доступа необходима аутентификация, исключающая передачу аутентификационных данных в открытом виде.

Предложенные в работе методы позволяют обеспечить конфиденциальность инфрмации, хранящейся и обрабатываемой в ЦОД. Данные методы предполагают частичный перенос нагрузки с серверов провайдера на сервер-посредник или на рабочие машины клиента. Данные методы слегка отступают от концепции облачных вычислений, которая предполагает, что вся обработка информации происходит на стороне провайдера, однако обеспечиваемая защита данных превосходит появившуюся нагрузку. Использование предложенных методов позволит защитить информацию не только от злоумышленников в сети, но и от самих провайдеров, которые так же могут использовать ее в своих целях. При применении данных методов отпадает вопрос о доверии провайдерам ценной информации, что повысит спрос на их услуги и даст толчек дальнейшему развитию концепции облачных вычислений, так как, обратившись к социальным исследованиям на тему проблем облачных вычислений, можно увидеть, что безопасность и доверие провайдеру облачных услуг стоит там на первых местах.

Литература:

1. Защита и контроль доступа к информации. [Электронный ресурс] / Techdays.com. Онлайн семинары по современным технологиям. – Режим доступа: URL: http://www.techdays.ru/videos/3157.html/ - 08.12.2010г. – Загл. с экрана.

2. Are these your files? I found them on my cloud. [Электронный ресурс] / Stage.vambenepe.com. Блог архитектора приложений. – Режим доступа: URL: http://stage.vambenepe.com/archives/922/ - 02.09.2009г. – Загл. с экрана.

3. Сетевая инфраструктура как услуга. [Электронный ресурс] / Bytemag.ru. Электронный журнал о современных технологиях. – Режим доступа: URL: http://www.bytemag.ru/articles/detail.php?ID=16083/ - 17.12.2009г. – Загл. с экрана.

АЛФАВИТНЫЙ СПИСОК АВТОРОВ ДОКЛАДОВ

Bezruk V.M. 361
Bukhanko O.M. 361
H.Al Janabii 237
Loshakov V. 233, 237
Vadia Z. 233, 237

А

Абдуллах Икрам Кадир 253
Абдул-Хуссейн М.К. 404
Агеев Д.В. 88, 139, 143
Аджемов А.С. 29
Алексеев Н.А. 43
Алексейцев К.Ф. 220
Али С. Али. 85
Андрушко Ю.В. 161
Антонников Д.О. 29
Асланов Т.Г. 187
Ахмед Хассан Абед 156

Б

Бабаков М.Ф. 109
Баев А.Д. 207
Балан Н.М. 36
Барба І.Б. 64
Безрук В.М. 365, 369
Беликова Е.С. 373
Белокуров А.А. 196
Беркман Л.Н. 9
Бидный Ю.М. 375
Бобкова А.А. 357
Бовкун А.Н. 395
Бойко Е.В. 271
Бондаренко В.І. 379
Бондаренко М.Ф. 167
Бубырь А.П. 291
Бугиль Б.А. 315
Быков П.И. 422

В

Вавенко Т.В. 98
Валковой В.С. 220
Варич В.В. 365
Васюта К.С. 411
Вдовичено Е.И. 220, 222
Величко Д.А. 222
Воробиенко П.П. 54
Воробьев А.В. 83
Воронов Д.М. 81
Вотяков О.И. 196

Г

Галюк С.Д. 58
Ганзенко В.В. 414
Гаркуша С.В. 257
Гладий Л.В. 279,416
Глоба Л.С. 43
Голубова О.В. 54
Горбенко И.Д. 295, 298, 323, 339
Горбенко І.Д. 379
Горбенко Ю.І. 379
Горюнов А.А. 145, 149
Гріненко Т.О. 302

Д

Дагаев Э.Х. 344
Дворжакова И.О. 180, 183
Добришкін Ю.М. 81
Добрынин И.С. 414,434
Дугин А.О. 398
Дудник Л.А. 220
Дуравкин Е.В. 153,416

Е

Евдокименко М.А. 156
Евлаш Д.В. 88
Евсеева О.Ю. 67
Ельченко С.В. 226
Еременко А.С. 418

Ж

Жартовский Д.Н. 220

З

Загайнов В.И. 369
Замула А.А. 295, 298, 305, 307
Заргано Г.Ф. 171
Зарицкий В.И. 109
Заросилова М.Г. 291, 373
Здоренко Ю.М. 113
Зеленский А.А. 32, 311, 319
Земляков В.В. 171
Земляченко А.Н. 311
Зинченко А.А. 212
Зоц Ф.Ф. 411

И, І

Иваненко В.А. 275
Иванов К.И. 305
Ивженко А.В. 268
Игнатенко А.А. 143
Искандар С.А. 117
Искендерзаде Ш.Г. 36
Іванюк П.В. 61,390

К

Кадацкая О.И. 91
Казимиренко В.Я. 229
Калугин В.Д. 200
Кальной С.Е. 200
Карпенко А.О. 210
Карпин Н.Б. 159
Килячков К.П. 102
Киянчук Р.И. 295, 327
Климаш М.М. 315
Кобрин А.В. 105
Коваленко І.Г 204
Коваленко Т.Н. 94
Коляденко Ю.Ю. 271
Копытова Е.А. 153
Корниенко С.А. 176
Коровченко Е.Б. 283
Кочкин М.И. 369
Кравченко А.Д. 431
Кривенко С.С. 311
Кривуца В.Г. 9
Кричко Д.І. 261
Крук О.Я. 167
Кузниченко В.С. 196, 220
Куркин Д.А. 319
Куценко В.В. 81
Кушнір М.Я. 58

Л

Лабунько О.С. 171
Лаврів О.А. 121, 315
Лемешко А.В. 85, 125
Лепіх Я.І. 210
Лосев Ю.И. 46
Лукин В.В. 311, 319
Луценко В.И. 109
Лю Цзяньфен 109
Ляховец В.А. 369

М

Максимюк Т.А. 261
Мальцев В.С. 369
Малютин А.А. 180, 183
Мартынчук А.А. 242,248,253
Марчук А.В. 274
Медвідь М.О. 393
Минаков А.Г. 331
Митяева И.А. 323
Мишенков С.Л. 29
Мордвінов Р.І. 302

Н

Назмутдинов А.А. 248
Нарытник Т.Н. 229
Нестеров Л.А. 220
Нечаев Ю.Б. 180, 183, 207

О

Овчинников К.А. 145, 149
Озарко Е.С. 402
Олейников Р.В. 327, 331
Олешко И.В. 335
Омельченко А.В. 352
Онищенко В.О. 167
Опотяк Ю.В. 402
Орєшков В.І. 64

П

Павленко М.А. 73
Паршина Д.А. 339
Пастушенко А.Н. 265
Пастушенко Н.С. 265
Пашинцев В.П. 344
Переверзев А.А. 139
Персиков А.В. 418
Петров В.Л. 196
Писаренок Г.Г 196
Підченко С.К. 32
Поздняков П.В. 348
Покотило О.О. 12
Політанський Л.Ф. 58, 61,390
Політанський Р.Л. 61,390
Поліщук А.В. 121
Польщиков К.А. 71, 113
Пономаренко Н.Н. 311
Поповская Е.О. 130
Поповский В.В. 20, 105, 117
Прусский А.В. 200

Р
Радько П.Н. 180, 183
Разруцький Т.Ю. 12
Рвачева Н.В. 71
Роздымаха Е.А. 352
Ролік О.І. 12
Романчук В.І. 121
Романчук Е.Ю. 429
Романюк В.А. 204
Руккас К.М. 46, 145,149
С
Сабурова С.А. 91
Семенець В.В. 167
Семеняка М.В. 125
Сенокосова А.В. 344
Серков А.А. 40
Симоненко А.В. 76
Скляренко С.Е. 422
Скороход А.Н. 242
Слюсар В.И. 212, 215, 218
Слюсар Д.В. 215
Слюсар І.І. 355
Смирнов Н.И. 29
Снегуров А.В. 426,429,431
Снігур П.О. 210
Сокол Г.В. 128
Старкова Е.В. 136
Стрелковская И.В. 36
Стрельницкий А.А. 404
Стромов А.В. 207
Стрюк О.Ю. 132
Сырцов С.Л. 369
Т
Твердохлеб В.И. 369
Теленик С.Ф. 12
Теплицкая С.Н. 287
Тиртишніков О.І. 167
Тихонов В.И. 54
Ткаченко В.М. 159
Ткаченко Е.А. 431
Торба А.А. 357
Тоцький О.С. 379
Тулла Е.Н. 94
Тур Б.С. 117
Тютюник В.В. 200
У
Уткін Ю.В. 355
Ф
Федоров А.В. 352
Федюшин А.Ю. 393
Х
Хайдара Абдалла 143
Халава Саид Фауаз 279
Хафиз Мухаммад И. 271
Хуссейн Я.Т. 287
Ц
Цопа А.И. 268,408
Цыбулев Р.А. 218
Ч
Черныш В.И. 305
Чипига А.Ф. 344
Чичмар С.В. 379
Ш
Шаповалов И.В. 434
Шахтарин Б.И. 187
Шинкаренко И.В. 408
Шматков С.И. 46, 50
Шокало В.М. 404
Шостко И.С. 240
Шпатар П.М 390
Щ
Щебенюк В.С. 46
Ю
Юпиков О.А. 191
Я
Ягудина Е.В. 404
Янко А.С. 355
Яремко О.М. 261
Ярыгина Т.Е. 307

СОДЕРЖАНИЕ

Пленарное заседание конференции 7

Кривуца В.Г., Беркман Л.Н.
ПИТАННЯ ДОСЛІДЖЕННЯ МЕРЕЖ МАЙБУТНЬОГО FN (Future Networks) 9

Теленик С.Ф., Ролік О.І., Покотило О.О., Разруцький Т.Ю.
МУЛЬТИАГЕНТНІ ТЕХНОЛОГІЇ, МОДЕЛІ Й МЕТОДИ УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПРОВАЙДЕРІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ПОСЛУГ 12

Поповский В.В.
К РАЗВИТИЮ ТЕОРИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 20

Секция № 1
ОСНОВЫ ТЕОРИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 27

Аджемов А.С., Мишенков С.Л., Смирнов Н.И., Антонников Д.О.
ГЛОБАЛЬНАЯ СИСТЕМА РАСПРЕДЕЛЕНИЯ СИГНАЛОВ ТОЧНОГО ВРЕМЕНИ НА ОСНОВЕ СПУТНИКОВОЙ НАВИГАЦИОНОЙ СИСТЕМЫ ГЛОНАСС 29

Зеленський О.О., Підченко С.К.
ПРИНЦИПИ ПОБУДОВИ ІНВАРІАНТНИХ П'ЄЗОРЕЗОНАНСНИХ КОЛИВАЛЬНИХ СИСТЕМ 32

Балан Н.М., Стрелковская И.В., Искендерзаде Ш.Г
ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ГИБРИДНОЙ СИСТЕМЫ ЗВУКОВОГО ВЕЩАНИЯ В ДИАПАЗОНЕ ОВЧ 36

Серков А.А.
МЕТОДЫ ОЦЕНКИ ПОМЕХОЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 40

Алексеев Н.А., Глоба Л.С.
ПОДХОД К СОЗДАНИЮ КОМПЛЕКСНЫХ MDE–МОДЕЛЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 43

Лосев Ю.И., Шматков С.И., Руккас К.М., Щебенюк В.С.
ОЦЕНКА ЭФФЕКТИВНОСТИ ОДНОМАРШРУТНОГО И МУЛЬТИМАРШРУТНОГО МЕТОДОВ ПЕРЕДАЧИ СООБЩЕНИЙ 46

Шматков С.И.
МОДЕЛЬ ВЫСОКОУРОВНЕВОЙ ВРЕМЕННОЙ ФРАГМЕНТАЦИИ ЦИКЛИЧЕСКИХ ЗАДАЧ 50

Воробиенко П.П., Тихонов В.И., Голубова О.В.
ПРИНЦИПЫ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ ПО ТЕХНОЛОГИИ UA-ITT .. 54

Галюк С.Д., Політанський Л.Ф., Кушнір М.Я.
СИНХРОНІЗАЦІЯ ХАОСУ ЧЕРЕЗ КАНАЛ ЗВ'ЯЗКУ З ОБМЕЖЕНОЮ ПРОПУСКНОЮ ЗДАТНІСТЮ 58

Іванюк П.В., Політанський Л.Ф., Політанський Р.Л.
СИНХРОНІЗАЦІЯ ГІПЕРХАОТИЧНИХ СИСТЕМ ЛЮ ОБЕРНЕНИМ ЛІНІЙНИМ ЗВ'ЯЗКОМ 61

Барба І.Б., Орєшков В.І.
ПРОЕКТУВАННЯ МЕРЕЖІ АБОНЕНТСЬКОГО ШИРОКОСМУГОВОГО ДОСТУПУ 64

Евсеева О.Ю.
МЕТОДИКА ТЕНЗОРНОГО ОБОБЩЕНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 67

Польщиков К.А., Рвачева Н.В.
МЕТОД ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ДОСТАВКИ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ С КОММУТАЦИЕЙ ПАКЕТОВ..... 71

Павленко М.А.
ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ПРИ МОДЕЛИРОВАНИЕ ПРОЦЕССА МАРШРУТИЗАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ..... 73

Симоненко А.В.
ПОТОКОВАЯ МОДЕЛЬ ДИНАМИЧЕСКОЙ БАЛАНСИРОВКИ ЗАГРУЖЕННОСТИ ОЧЕРЕДЕЙ В MPLS-СЕТИ С ПОДДЕРЖКОЙ TRAFFIC ENGINEERING QUEUES..... 76

Добришкін Ю.М., Воронов Д.М., Куценко В.В.
МОДЕЛЬ УПРАВЛІННЯ ТРАФІКОМ З ГАРАНТІЯМИ НА ЯКІСТЬ ОБСЛУГОВУВАННЯ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ..... 81

Воробьев А.В.
ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ БАЛАНСИРОВКИ НАГРУЗКИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ УРОВНЯ ДОСТУПА..... 83

Лемешко А.В., Али С. Али.
МЕТОД ДИНАМИЧЕСКОГО УПРАВЛЕНИЯ ОЧЕРЕДЯМИ В СЕТИ MPLS-TE 85

Евлаш Д.В., Агеев Д.В.
МЕТОД ОЦЕНКИ ПАРАМЕТРОВ ИНФОРМАЦИОННЫХ ПОТОКОВ, ПЕРЕДАВАЕМЫХ ПО КАНАЛАМ СВЯЗИ МУЛЬТИСЕРВИСНОЙ СЕТИ ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГИ IPTV 88

Кадацкая О.И., Сабурова С.А.
УЛУЧШЕНИЕ ПАРАМЕТРОВ КАЧЕСТВА ТЕСТИРОВАНИЯ РАДИОТРАКТА НА АБОНЕНТСКОМ УЧАСТКЕ..... 91

Коваленко Т.Н., Тулла Е.Н.
МЕТОДИКА АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ РАСПРЕДЛЕННЫХ СИСТЕМ С СЕРВИС - ОРИЕНТИРОВАННОЙ АРХИТЕКТУРОЙ..... 94

Вавенко Т.В.
ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ С УЧЕТОМ ТЕХНОЛОГИИ TRAFFIC ENGINEERING ДЛЯ СЕТЕЙ, ПРЕДСТАВЛЕННЫХ СОЕДИНЕННЫМ ГРАФОМ..... 98

Килячков К.П.
МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 102

Поповский В.В., Кобрин А.В.
ИСПОЛЬЗОВАНИЕ ПОТОКОВЫХ АГЕНТОВ ДЛЯ МОНИТОРИНГА И УПРАВЛЕНИЯ КАЧЕСТВОМ ПОТОКОВОГО ВИДЕО В СЕТЯХ WIMAX..... 105

Луценко В.И., Лю Цзяньфен, Бабаков М.Ф., Зарицкий В.И.
СТОХАСТИЧЕСКАЯ СОТОВАЯ ПОДВИЖНАЯ СВЯЗЬ ИЛИ ЗАДАЧА О ПРЫГАЮЩЕЙ ОБЕЗЬЯНЕ И ЕЕ ПРИМЕНЕНИЯ В ТЕОРИИ СВЯЗИ..... 109

Польщиков К.О., Здоренко Ю.М.
МЕТОД НЕЙРО-НЕЧІТКОГО АКТИВНОГО УПРАВЛІННЯ ПАКЕТНИМИ ЧЕРГАМИ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ..... 113

Поповский В.В., Тур Б.С., Искандар С.А.
МЕТОДЫ ПОСЛЕДОВАТЕЛЬНОЙ КОМПЕНСАЦИИ ИСКАЖЕНИЙ В ДРЕВОВИДНЫХ АЛГОРИТМАХ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУП..... 117

Романчук В.І., Лаврів О.А., Поліщук А.В.
ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТРАФІКУ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ 121

Семеняка М.В., Лемешко А.В.
ИССЛЕДОВАНИЕ ОДНОПУТЕВОЙ МАРШРУТИЗАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ БАЛАНСИРОВКИ НАГРУЗКИ НА СЕТЬ 125

Сокол Г.В.
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЧУТЛИВОСТІ ФІЛЬТРУ КАЛМАНА-Б'ЮСІ ПРИ НЕСТАЦІОНАРНОМУ ТРАФІКУ 128

Поповская Е.О.
АНАЛИЗ МОДЕЛИ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ И ДАННЫХ 130

Стрюк О.Ю.
МЕТОД МАКСИМІЗАЦІЇ КОРИСНОСТІ МОБІЛЬНОЇ РАДІОМЕРЕЖІ НА ОСНОВІ ПОКАЗНИКІВ СПРИЙНЯТТЯ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ 132

Старкова Е.В.
ТРЕБОВАНИЯ К ПЕРСПЕКТИВНЫМ СРЕДСТВАМ КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ ПЕРЕГРУЗОК В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 136

Агеев Д.В., Переверзев А.А.
УПРАВЛЕНИЕ НАЗНАЧЕНИЕМ ДЛИН ВОЛН СВЕТОВЫМ МАРШРУТАМ В СЕТЯХ DWDM 139

Игнатенко А.А., Агеев Д.В., Хайдара Абдалла
ПОСТРОЕНИЕ МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ МЕТОДОВ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ И УЧЕТОМ ТРЕБОВАНИЙ СПЕЦИФИКАЦИЙ MUSE 143

Овчинников К.А, Руккас К.М., Горюнов А.А.
РЕКУРСИВНАЯ ПОТОКОВАЯ МОДЕЛЬ MPLS 145

Горюнов А.А., Руккас К.М., Овчинников К.А.
АНАЛИЗ ВОЗМОЖНОСТЕЙ ТЕХНОЛОГИЙ MPLS И GMPLS 149

Дуравкин Е.В., Копытова Е.А.
ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ СИСТЕМ УПРАВЛЕНИЯ МУЛЬТИСЕВИСНЫМИ СЕТЯМИ 153

Евдокименко М.А., Ахмед Хассан Абед.
ОБЗОР И КЛАССИФИКАЦИЯ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ 156

Карпин Н.Б, Ткаченко В.М.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПОТОКОВОЙ МАРШРУТИЗАЦИИ 159

Андрушко Ю.В.
ПРОЦЕДУРА ОЦЕНКИ RTT СЕГМЕНТА В СЕТИ НА ОСНОВЕ ЗАШУМЛЕННЫХ НАБЛЮДЕНИЙ 161

Секция № 2
БЕСПРОВОДНЫЕ СЕТИ И ТЕХНОЛОГИИ 165

Бондаренко М.Ф., Онищенко В.О., Семенець В.В., Тиртишніков О.І., Крук О.Я.
НАВЧАЛЬНО – ЛАБОРАТОРНИЙ КОМПЛЕКС ДЛЯ ВИВЧЕННЯ АНАЛОГОВИХ ЕЛЕКТРОНІКИ ТА СХЕМОТЕХНІКИ 167

Заргано Г.Ф., Земляков В.В., Лабунько О.С.
КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ СЕЛЕКТИВНЫХ УСТРОЙСТВ НА ВОЛНОВОДАХ СЛОЖНОГО СЕЧЕНИЯ ДЛЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 171

Корниенко С.А.
ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПРИМЕНЯЕМЫЕ ДЛЯ ОПИСАНИЯ ОСНОВНЫХ СВОЙСТВ СЛОЖНЫХ СИСТЕМ РАДИОКОНТРОЛЯ 176

Нечаев Ю.Б., Дворжакова И.О., Малютин А.А., Радько П.Н.
ПОМЕХОУСТОЙЧИВОСТЬ СИСТЕМ ДКМВ СВЯЗИ С MIMO 180

Нечаев Ю.Б., Дворжакова И.О., Малютин А.А., Радько П.Н.
ПОСТРОЕНИЕ СИГНАЛЬНЫХ СОЗВЕЗДИЙ ДЛЯ СИСТЕМ ДКМВ СВЯЗИ С MIMO 183

Шахтарин Б.И., Асланов Т.Г.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАРАКТЕРИСТИК ВОЗДЕЙСТВИЯ ПОМЕХ НА СИСТЕМЫ СИНХРОНИЗАЦИИ 187

Юпиков О.А.
МНОГОЛУЧЕВОСТЬ В ЗЕРКАЛЬНЫХ РАДИОТЕЛЕСКОПАХ: ЧУВСТВИТЕЛЬНОСТЬ В ШИРОКОМ ПОЛЕ ОБЗОРА 191

Белокуров А.А., Вотяков О.И., Кузниченко В.С., Петров В.Л., Писаренок Г.Г.
МЕТОДЫ АНАЛИЗА OFDM СИГНАЛОВ В СИСТЕМАХ АВТОМАТИЧЕСКОГО РАДИОМОНИТОРИНГА 196

Прусский А.В., Калугин В.Д., Кальной С.Е., Тютюник В.В.
ФОРМИРОВАНИЕ ЭФФЕКТА ПРОВОДИМОСТИ В МНОГОКОМПОНЕНТНЫХ ПОЛУПРОВОДНИКОВЫХ ПЛЕНОЧНЫХ СЕНСОРНЫХ СТРУКТУРАХ В ГАЗОВЫХ СРЕДАХ 200

Коваленко І.Г, Романюк В.А.
МЕТОД ЗБЕРЕЖЕННЯ ЕНЕРГОРЕСУРСУ НЕОДНОРІДНИХ СЕНСОРНИХ РАДІОМЕРЕЖ З НАДЛИШКОВОЮ КІЛЬКІСТЮ ВУЗЛІВ ПРИ ЗАБЕЗПЕЧЕННІ ЗАДАНОЇ ЯКОСТІ ПОКРИТТЯ РАЙОНУ МОНІТОРИНГУ 204

Нечаев Ю.Б., Баев А.Д., Стромов А.В.
МОДЕЛИРОВАНИЕ МАРШРУТИЗАЦИИ В СВЕРХБОЛЬШОЙ СЕНСОРНОЙ СЕТИ С ОЦЕНКОЙ ЭНЕРГОПОТРЕБЛЕНИЯ 207

Лепіх Я.І., Карпенко А.О., Снігур П.О.
ВИМІРЮВАЛЬНИЙ СТЕНД ДЛЯ ДОСЛІДЖЕНЬ АКУСТОЕЛЕКТРОННИХ ДАТЧИКІВ КУТА ПОВОРОТУ 210

Зинченко А.А., Слюсар В.И.
РАДИОЛОКАЦИОННЫЙ И СВЯЗНОЙ РЕЖИМЫ МОБИЛЬНЫХ СТАНЦИЙ СВЯЗИ И РАДИОЛОКАЦИИ С ЦИФРОВЫМИ АНТЕННЫМИ РЕШЕТКАМИ 212

Слюсар Д.В., Слюсар В.І.
МАТРИЧНА МОДЕЛЬ ВІДГУКУ БАГАТОСЕКЦІЙНОЇ ЦАР У СКЛАДІ ПІРАМІДАЛЬНОЇ НАНОСХЕМИ 215

Цыбулев Р.А., Слюсар В.И.
МЕТОД КОРРЕКЦИИ КВАДРАТУРНОГО РОЗБАЛАНСА 218

Алексейцев К.Ф., Валковой В.С., Вдовичено Е.И., Дудник Л.А., Жартовский Д.Н., Кузниченко В.С., Нестеров Л.А.
СИНХРОНИЗАЦИЯ СИГНАЛОВ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ НА ОСНОВЕ СИГНАЛЬНОГО ПРОЦЕССОРА 220

Величко Д.А., Вдовичено Е.И.
ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ВХОДНОГО СИГНАЛА РЕТРАНСЛЯЦИОННОГО ИЗМЕРИТЕЛЯ ЦИФРОВЫМИ МЕТОДАМИ 222

Ельченко С.В.
ТЕСТИРОВАНИЕ XPD – CPA МОДЕЛЕЙ 226

Казимиренко В.Я., Нарытник Т.Н.
СИСТЕМА БЕСПРОВОДНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ УСЛУГАМ 229

Loshakov V., Vadia Z.
USING KALMAN FILTERING IN SOLVING ADAPTIVE MODULATION PROBLEMS IN MIMO CHANNELS 233

Loshakov V., Vadia Z., Al Janabii H.
RESULTS OF EXPERIMENTAL RESEARCH QUALITY OF COMMUNICATIONS IN WiMAX SYSTEM, ... 237

Шостко И.С.
МЕТОД УВЕЛИЧЕНИЯ БЫСТРОДЕЙСТВИЯ УСТРОЙСТВА ГРОЗОЗАЩИТЫ ПРИЁМНИКОВ РАДИОТЕХНИЧЕСКИХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ... 240

Мартынчук А.А., Скороход А.Н.
ВЛИЯНИЕ ИНДЕКСА ПОЛЯРИЗАЦИИ СИГНАЛА НА ПРОПУСКНУЮ СПОСОБНОСТЬ ПРИЕМНОГО КАНАЛА SISO СИСТЕМ..... 242

Мартынчук А.А., Назмутдинов А.А.
ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ MIMO СИСТЕМЫ ПУТЕМ ИСПОЛЬЗОВАНИЯ ПОЛЯРИЗАЦИОННО-ОРТОГОНАЛЬНЫХ АНТЕНН 248

Мартынчук А.А., Абдуллах Икрам Кадир.
ANALYSIS FEATURES PARAMETERS OF POLARIZATION-ORTOGONAL ANTENNAE FOR MIMO SYSTEM 253

Гаркуша С.В.
КЛАСИФІКАЦІЯ ТА АНАЛІЗ МЕТОДІВ РОЗПОДІЛУ ЧАСТОТНИХ КАНАЛІВ В БАГАТОКАНАЛЬНИХ MESH-МЕРЕЖАХ 257

Яремко О.М., Максимюк Т.А., Кричко Д.І.
ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РАДІОІНТЕРФЕЙСУ БЕЗПРОВІДНИХ СИСТЕМ НАСТУПНОГО ПОКОЛІННЯ 261

Пастушенко Н.С., Пастушенко А.Н.
К ВОПРОСУ ПОВЫШЕНИЯ КАЧЕСТВА ОБРАБОТКИ АКУСТИЧЕСКИХ СИГНАЛОВ 265

Ивженко А.В., Цопа А.И.
ИСПОЛЬЗОВАНИЕ КРИТЕРИЯ PSNR ДЛЯ ОЦЕНКИ КАЧЕСТВА ПЕРЕДАЧИ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИ В СИСТЕМЕ БЕСПРОВОДНОГО ДОСТУПА WiMAX..... 268

Коляденко Ю.Ю., Бойко Е.В., Хафиз Мухаммад И.
АНАЛИЗ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК РАДИОКАНАЛОВ СИСТЕМ WI-MAX 271

Марчук А.В.
ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ MIMO В ОТКРЫТЫХ ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ..... 274

Иваненко В.А.
МЕТОД ПОЗИЦИОНИРОВАНИЯ УЗЛОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ..... 275

Гладий Л.В., Халава Саид Фауаз.
МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫМ ГОРОДОМ..... 279

Коровченко Е.Б.
МЕТОДИКА АНАЛИЗА И ВЕРИФИКАЦИИ ТЕЛЕКОММУНИКАЦИОННЫХ ПРОТОКОЛОВ С ПОМОЩЬЮ Е-СЕТЕЙ И ФОРМАЛЬНЫХ ГРАММАТИК 283

Теплицкая С.Н., Хуссейн Я.Т.
ИМИТАЦИОННАЯ МОДЕЛЬ САМООРГАНИЗАЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ 287

Секция № 3
ИНФОРМАЦИОННЫЕ СЕТИ СВЯЗИ 289

Бубырь А.П., Заросилова М.Г.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ АСИММЕТРИЧНЫХ АЛГОРИТМОВ NTRU, RSA И ECC 291

Горбенко И.Д., Киянчук Р.И., Замула А.А.
МЕТОД ПОСТРОЕНИЯ МНОГОФАЗНЫХ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ 295

Горбенко И.Д., Замула А.А.
ЗАЩИТА РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СЛОЖНЫХ СИГНАЛОВ, ... 298

Гріненко Т.О., Мордвінов Р.І.
ОБГРУНТУВАННЯ ВИМОГ ДО МЕТОДІВ ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ 302

Замула А.А., Черныш В.И., Иванов К.И.
МЕТОД СТРУКТУРИРОВАННОЙ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 305

Замула А.А., Ярыгина Т.Е.
МЕТОД ФОРМИРОВАНИЯ МНОЖЕСТВА ДИСКРЕТНЫХ СИГНАЛОВ С ЗАДАННЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ 307

Зеленский А.А., Земляченко А.Н., Кривенко С.С., Лукин В.В., Пономаренко Н.Н.
СЖАТИЕ ИЗОБРАЖЕНИЙ С ПОТЕРЯМИ БЕЗ ВИЗУАЛЬНО ЗАМЕТНЫХ ИСКАЖЕНИЙ: ПРИМЕНЕНИЯ, ПРОГРЕСС, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ 311

Климаш М.М., Лаврів О.А., Бугиль Б.А.
ВПЛИВ ВЛАСТИВОСТЕЙ ТРАФІКУ НА ПАРАМЕТРИ ЯКОСТІ ОБСЛУГОВУВАННЯ ВУЗЛА МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ 315

Куркин Д.А., Зеленский А.А., Лукин В.В.
ОЦЕНИВАНИЕ ВЗАИМНОЙ ЗАДЕРЖКИ ШИРОКОПОЛОСНЫХ СИГНАЛОВ ПРИ НЕГАУССОВЫХ ПОМЕХАХ 319

Митяева И.А., Горбенко И.Д.
АНАЛИЗ УЯЗВИМОСТИ КРИПТОАЛГОРИТМОВ В ГРУППАХ КОС 323

Олейников Р.В., Киянчук Р.И.
ПЕРСПЕКТИВНЫЙ БЛОЧНЫЙ СИММЕТРИЧНЫЙ ШИФР, ОПТИМИЗИРОВАННЫЙ ДЛЯ АППАРАТНОЙ РЕАЛИЗАЦИИ 327

Олейников Р.В., Минаков А.Г.
КРИПТОАНАЛИЗ НА ОСНОВЕ АТАК ПО ПОБОЧНЫМ КАНАЛАМ 331

Олешко И.В.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ ПО ОТПЕЧАТКУ ПАЛЬЦА 335

Паршина Д.А., Горбенко И.Д.
ОБЗОР КРИПТОГРАФИЧЕСКИХ СИСТЕМ В ГРУППАХ КОС 339

Пашинцев В.П., Чипига А.Ф., Сенокосова А.В., Дагаев Э.Х.
ОЦЕНКА ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С ПОНИЖЕННОЙ ЧАСТОТОЙ 344

Поздняков П.В.
КРИПТОГРАФІЧНИЙ ПРОТОКОЛ НА ОСНОВІ КІНЦЕВИХ АВТОМАТІВ У РАДІОЛІНІЇ ОБМІНУ ІНФОРМАЦІЄЮ З БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ 348

Роздымаха Е.А., Омельченко А.В., Федоров А.В.
МОДЕЛЬ ТРАФИКА ETHERNET В ВИДЕ ON/OFF ПРОЦЕССА 352

Слюсар І.І., Уткін Ю.В., Янко А.С.
МОДЕЛЬ СТЕНДУ ДЛЯ ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ VOIP 355

Торба А.А., Бобкова А.А.
УЛУЧШЕНИЕ СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ БИТ 357

Bezruk V.M., Bukhanko O.M.
MULTICRITERIA OPTIMIZATION IN TELECOMMUNICATION NETWORKS PLANNING, DESIGNING AND CONTROLLING 361

Безрук В.М., Варич В.В.
РЕШЕНИЕ ЗАДАЧИ ВЫБОРА МАРШРУТОВ С ПРИМЕНЕНИЕМ МНОГОКРИТЕРИАЛЬНОГО ПОДХОДА 365

Безрук В.М., Загайнов В.И., Кочкин М.И., Ляховец В.А., Мальцев В.С., Сырцов С.Л., Твердохлеб В.И.
ИНФОРМАЦИОННАЯ СИСТЕМА КОМПЬЮТЕРНОЙ ТЕЛЕФОНИИ ДЛЯ АВТОМАТИЗАЦИИ ДИСПЕТЧЕРСКИХ СЛУЖБ СВЯЗИ 369

Беликова Е.С., Заросилова М.Г.
АНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ NTRU СОГЛАСНО СТАНДАРТА ANSI X9.98 373

Бидный Ю.М.
ВЕРОЯТНОСТНЫЕ МОДЕЛИ ПРОЦЕССОВ ОБСЛУЖИВАНИЯ ВЫЗОВОВ И УПРАВЛЕНИЯ ИМИ В ИНФОРМАЦИОННЫХ СЕТЯХ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ 375

Секция № 4
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 377

Горбенко Ю.І.,Чичмар С.В., Тоцький О.С., Бондаренко В.І., Горбенко І.Д.
ПРОБЛЕМНІ ПИТАННЯ ТА ОСНОВНІ НАПРЯМИ УДОСКОНАЛЕННЯ ТА РОЗВИТКУ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ ВІДКРИТОГО КЛЮЧА 379

Політанський Р.Л., Політанський Л.Ф., Шпатар П.М, Іванюк П.В.
СИСТЕМА ЗВ'ЯЗКУ З ШИФРУВАННЯМ ДАНИХ ПСЕВДОВИПАДКОВИМИ ПОСЛІДОВНОСТЯМИ ТА КОДУВАННЯМ КАНАЛУ КОДАМИ ХЕМІНГА 390

Медвідь М.О., Федюшин А.Ю.
ЗАХИСТ ПРИМІЩЕНЬ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ 393

Бовкун А.Н.
АНАЛИЗ ВОЗМОЖНОСТИ УТЕЧКИ ЗАКРЫТОЙ ИНФОРМАЦИИ ЧЕРЕЗ ИНТЕРФЕЙС D-SUB 395

Дугин А.О.
ПРАКТИЧЕСКИЕ ОСОБЕННОСТИ УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ 398

Озарко Е.С., Опотяк Ю.В.
ПРИМЕНЕНИЕ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ ОТБОРА КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРОГРАММНОГО КОМПЛЕКСА «СТИМУЛ» 402

Стрельницкий А.А., Шокало В.М., Ягудина Е.В., Абдул-Хуссейн М.К.
УЧЕТ ВЛИЯНИЯ НА СКРЫТНОСТЬ WI-FI КАНАЛОВ СВЯЗИ ИХ ЭЛЕКТРОДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК И УСЛОВИЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН 404

Шинкаренко И.В., Цопа А.И.
СТРУКТУРНАЯ СКРЫТНОСТЬ ЛИНЕЙНЫХ СИГНАЛОВ ШИРОКОПОЛОСНЫХ XDSL ТЕХНОЛОГИЙ 408

Васюта К.С., Зоц Ф.Ф.
СКРЫТАЯ ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ СЛОЖНЫХ ХАОТИЧЕСКИХ СИГНАЛОВ 411

Ганзенко В.В., Добрынин И.С.
АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В WINDOWS AZURE 414

Дуравкин Е.В., Гладий Л.В.
АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ СТАНДАРТА ISO/IEC 27001 416

Персиков А.В., Еременко А.С.
УНИВЕРСАЛЬНАЯ СРЕДА ИМИТАЦИИ ПРОЦЕССОВ, ПРОИСХОДЯЩИХ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ, ОРИЕНТИРОВАННАЯ НА ЗАДАЧИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ АТАКАМ 418

Скляренко С.Е., Быков П.И.
АДМИНИСТРИРОВАНИЕ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ SQL AZURE 422

Снегуров А.В.
ПОДХОД К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ С УЧЕТОМ КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ СРЕДСТВ НАПАДЕНИЯ И ЗАЩИТЫ 426

Снегуров А.В., Романчук Е.Ю.
ПОДХОД К ВЫЯВЛЕНИЮ ИНСАЙДЕРОВ НА ОСНОВЕ МЕТОДОВ ВИЗУАЛЬНОЙ ПСИХОДИАГНОСТИКИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ 429

Снегуров А.В., Ткаченко Е.А., Кравченко А.Д.
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ, ПОСТРОЕННЫХ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ» 431

Шаповалов И.В., Добрынин И.С.
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ СИСТЕМАХ 434

Алфавитный список авторов докладов 437

СБОРНИК НАУЧНЫХ ТРУДОВ

4-го Международного радиоэлектронного форума

«Прикладная радиоэлектроника. Состояние и перспективы развития»

(МРФ’2011)

Том II

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

«ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

(МКТСТ’2011)

Ответственные за выпуск

Дохов А.И.
Поповский В.В.
Булавина Е.С.

Материалы сборника публикуются в авторском варианте
без редактирования

Подписано к печати 06.10.2011. Формат 60 × 84 1/8. Бумага офсетная.
Усл. печ. л. 51,6. Тираж 180 экз. Зак. 2-816. Цена договорная.

61166 Украина, Харьков, просп. Ленина, 14

Отпечатано в учебно-научном издательско-полиграфическом центре ХНУРЭ
61166 Украина, Харьков, просп. Ленина, 14