УДК004.75

МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ ПЕРЕДАЧІ ДАНИХ У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

ЯЦКІВ В.В.

Пропонується метод підвищення надійності передачі даних у безпровідних сенсорних мережах на основі системи залишкових класів та багатошляхової маршрутизації, який забезпечує можливість відновлення втрачених пакетів та характеризується меншою надлишковістю.

1. Вступ

Безпровідні сенсорні мережі (БСМ) є одним з сучасних перспективних напрямів розвитку відмовостійких розподілених, самоконфігурованих систем моніторингу і управління ресурсами та процесами [1, 2]. Разом з тим використання БСМ в ряді областей, зокрема, в системах керування технологічними процесами, пожежно-охоронних системах, системах безпеки, системах моніторингу реального часу ставить підвищені вимоги до надійності їх функціонування на всіх рівнях моделі OSI.

В загальному для підвищення надійності передачі даних використовують такі підходи: передавання даних на основі методів розширення спектра сигналів (DSSS, FHSS), коректуючі коди (циклічна перевірка парності, коди Ріда-Соломона, Боуза – Чоудхурі – Хоквінгхема та інші) [3, 4]. Крім того, в [5] розроблено модифікований метод, який базується на розширенні спектра сигналу методом стрибкоподібної зміни частоти та перетворенні системи залишкових класів, що дає змогу здійснювати завадостійке кодування та розпаралелювання обробки інформації без значного ускладнення обчислювальних засобів. Однак всі перелічені вище підходи підвищують надійність передавання даних тільки на фізичному рівні безпровідних мереж.

Разом з тим залишається актуальною задача забезпечення надійності та безпеки передавання даних на мережному рівні. Втрата пакетів на мережному рівні БСМ зумовлена перевантаженням вузлів, виходом з ладу або недоступністю вузлів при зміні топології мережі. В свою чергу повторне передавання пакета призводить до затримки доставки повідомлення, збільшення трафіка в мережі, а отже – до збільшення енергетичних затрат.

Одним з найбільш ефективних способів підвищення надійності передачі даних в БСМ на мережному рівні є використання багатошляхової маршрутизації [1, 2]. В алгоритмах багатошляхової маршрутизації для кожного адресата обчислюється декілька шляхів, що дозволяє оптимально використовувати канали зв'язку і підвищувати їх загальну пропускну здатність. Крім того, багатошляхова маршрутизація забезпечує простий механізм для збільшення ймовірності надійної доставки даних за рахунок відправлення декількох копій даних за різними маршрутами. Однак використання протоколів багатошляхової маршрутизації призводить до збільшення енергетичних затрат та підвищення трафіка мережі.

Більш ефективним алгоритмом є поділ повідомлення на частини та передавання частин різними маршрутами, при цьому для захисту від помилок до кожної частини повідомлення додається коректуючий код [6]. Недоліком даного алгоритму є неможливість відновлення повідомлення при відсутності хоча б однієї частини. Крім того, обмежені обчислювальні ресурси безпровідного сенсора ускладнюють вибір ефективних коректуючи кодів.

Як алгоритм поділу пакету даних на частини використовують методи розподілу секрету [1, 2]. В цих методах кількість частин, які необхідні для відновлення повідомлення, можуть відрізнятися від того, на скільки частин ми розділили повідомлення. Такі алгоритми називають ще пороговою схемою (t,n), де n – кількість частин, на які поділяється секрет, а t – кількість частин, необхідних для відновлення секрету. В криптографії для розподілу секрету використовується схеми: Шаміра, Бляклі, Міньотта, Асмута – Блума [7].

Однак слід зауважити, що використання відомих порогових схем розподілу секрету дозволяє відновити дані при наявності тільки t частин, тобто при втраті n-t частин повідомлення, в той же час використання спотвореної частини повідомлення може перешкодити відновленню пакета даних. Тому автором запропоновано покращений метод поділу пакетів даних у безпровідних сенсорних мережах на основі системи залишкових класів, описаний нижче.

Метою роботи є підвищення надійності та ефективності передачі даних в БСМ на основі багатошляхової маршрутизації та порогових схем поділу повідомлення на частини.

Задачі дослідження: а) розробка порогової схеми розділення даних у системі залишкових класів (СЗК); б) розробка алгоритму маршрутизації в БСМ; в) оцінка надлишковості порогових схем розділення секрету.

2. Метод багатошляхової маршрутизації на основі системи залишкових класів

В запропонованому методі поділу пакетів даних в БСМ на n частин використовується перетворення СЗК, причому передаються одержані частини (підпакети) різними маршрутами, підпакети утворюються в ре-

зультаті отримання залишку від ділення пакета на взаємопрості модулі p_i.

2.1. Кодування на основі системи залишкових класів

Нехай задана система з основами $(p_1, p_2, ..., p_n)$ і діапазоном [8]

$$\wp = \prod_{i=1}^{n} p_i .$$

Відомо, що будь-яке число із діапазону $[0, \wp)$ можна представити у вигляді залишків по вибраних взаємопростих основах $M = (b_1, b_2, ..., b_n)$.

Заданій системі основ однозначно відповідає система ортогональних базисів $B_1, B_2, ..., B_n$, таких, що число M в позиційній системі числення можна представити як

$$M \equiv \sum_{i=1}^{n} b_i \cdot B_i \,(\mathrm{mod}\,\wp) .$$

До переваг системи залишкових класів необхідно віднести:

– незалежність утворення розрядів, в результаті чого кожний розряд несе інформацію про все число;

– мала розрядність залишків, що представляють число.

В запропонованому методі багатошляхової маршрутизації на основі СЗК для поділу пакета даних M на частини (t, n) виберемо взаємопрості числа $p_i < p_{i+1}$, добуток яких $\prod_{i=1}^{t} p_i > M$ (рис.1).

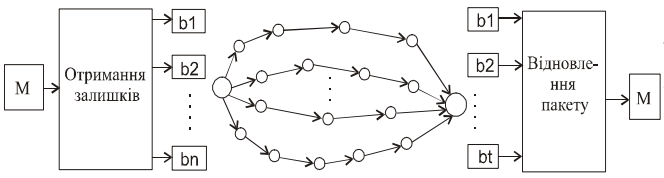

Рис. 1. Схема кодування на основі системи залишкових класів

Пакет даних M розділяємо на частини за формулою

$$b_i = M \bmod p_i .$$

В результаті поділу формується масив даних $\{\wp, p_i, b_i\}$.

Для реалізації можливості відновлення повідомлення по t частинах із n розглянемо систему з основами $p_1, p_2, \ldots, p_i, ..., p_t$ і діапазоном $P = p_1 \cdot p_2 \cdot \ldots \cdot p_t$. Діапазон P будемо називати робочим. Введемо основи $p_{t+1}, p_{t+2}, ..., p_n$ взаємопрості з будь-якою із прийнятих раніше основ і будемо представляти числа в системі із основами $p_1, ..., p_n$. Це означає, що будемо передавати і виконувати операції над числами, які знаходяться в діапазоні $[0, P)$, у більш широкому діапазоні $[0, \wp]$, де $\wp = P \cdot p_{t+1} \cdot ... \cdot p_n$.

Всі числа, з якими працює алгоритм кодування, повинні знаходитись в діапазоні $[0, P)$. Отже, якщо в результаті передавання одержано число M, більше P, це означає, що була допущена помилка.

Використання розширеної системи модулів СЗК забезпечує ефективне відновлення при спотворенні або втраті даних. Універсальність кодів системи залишкових класів пояснюється не лише їх високими коректуючими можливостями, арифметичністю і здатністю виправляти пакети помилок, але і їх адаптивністю до гнучкої зміни коректуючих властивостей без зміни способу кодування.

2.2. Алгоритм багатошляхової маршрутизації на основі системи залишкових класів

В розробленому алгоритмі маршрутизації (рис. 2) вузол БСМ, що ініціює передачу даних, визначає доступні маршрути, які не перетинаються (бл.1), та оцінює ефективність кожного маршруту (бл. 4).

Залежно від кількості доступних маршрутів вибирається кількість та значення взаємопростих модулів p_i (бл. 2), обчислюються робочий і загальний діапазони представлення даних.

В результаті поділу повідомлення на вибрану систему модулів (бл. 3) отримуємо залишки, які передаються по визначених маршрутах. Залишки більшої розрядності передаються по маршрутах з вищою оцінкою і навпаки (бл. 5), що дозволяє покращити коректуючі можливості кодів СЗК, а відповідно підвищити надійність передачі в цілому. Базова станція отримує підпакети (залишки по відповідних модулях) і відновлює початкові пакети (бл.7).

3. Порівняльна оцінка методів поділу повідомлення на частини

Порівняємо надлишковість кодування даних при поділі повідомлення на частини з використанням існуючих порогових схем розділення секрету (Шаміра, Асмута-Блума) та запропонованого алгоритму. Для цього обчислимо обсяг повідомлення при заданих значеннях: кількість частин (маршрутів) $n = 10$, $t = 8$, розмір пакета даних 24 біти.

3.1. Порогова схема розділення секрету Шаміра

Щоб розділити пакет даних M, в схемі Шаміра вибирається просте число P, $P > M$, яке задає розмір кінцевого поля [7]. Над цим полем будується багаточлен розмірності $t - 1$:

$$F(x) = (a_t \cdot x^t + a_{t-1} \cdot x^{t-1} + ... + a_1 \cdot x + M) \bmod P$$

Рис.2. Блок – схема алгоритму багатошляхової маршрутизації на основі системи залишкових класів

Коефіцієнти багаточлена $a_t, a_{t-1} \ldots a_1$ вибираються випадково. Після цього обчислюються координати *n* точок:

$$t_i = F(i) = (a_t \cdot i^t + a_{t-1} \cdot i^{t-1} + \ldots + a_1 \cdot i + M) \bmod P$$

В результаті формується потік даних

$$\{P, t-1, t_i, j\},$$

де t_i – коефіцієнти, які обчислюються; j – номери коефіцієнтів; $t-1$ – розмір багаточлена; P – модуль.

Обсяг однієї частини повідомлення

$$v_1 =]\log_2 P[+]\log_2 (t-1)[+]\log_2 t_i[+]\log_2 j[,$$

тобто для простого числа $P > M$: $v_1 = 57$ біт.

Отже, для кожного з десяти маршрутів передачі формується пакет даних розміром 57 біт.

3.2. Порогова схема розділення секрету Асмута-Блума

Порогова схема розділення секрету Асмута-Блума побудована з використанням простих чисел [7]. Вибираємо просте число P з умови $P > M$ та n взаємопростих чисел $p_1, p_2, \ldots, p_n$ таких, що $p_i > P$; $p_i < p_{i+1}$, тобто

$$p_1 \cdot p_2 \cdot \ldots \cdot p_t > P \cdot p_{n-t+2} \cdot p_{n-t+3} \cdots p_n.$$

Обчислюємо $M' = M + r \cdot P$, де r – випадкове число, і знаходимо частини повідомлення

$$b_i = M' \bmod p_i.$$

В результаті формується масив даних $\{P, p_i, b_i\}$, а обсяг однієї частини повідомлення

$$v_2 =]\log_2 P[+]\log_2 p_i[+]\log_2 b_i[\text{ (біт)}.$$

Обчислимо обсяг даних, який формується в результаті поділу пакета на частини при заданих значеннях: $M = 16777216$; при $P > M$ розрядність P дорівнює 25 біт; розрядність взаємопростих чисел p_i згідно з умовою $p_i > P$ також дорівнює мінімум 25 біт; максимальне значення залишків рівне 25 біт.

Отже, обсяг однієї частини повідомлення при заданих значеннях дорівнює $v_2 = 75$ біт.

3.3. Схема кодування на основі СЗК

В результаті застосування перетворення СЗК обсяг однієї частини повідомлення

$$v_3 =]\log_2 \wp[+]\log_2 p_i[+]\log_2 b_i[\text{ (біт)}.$$

Для обчислення обсягу даних, який формується в результаті поділу пакета на частини (при заданих значеннях), вибираємо взаємопрості модулі:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,$$
$$p_6 = 17,\ p_7 = 19,\ p_8 = 23,\ p_9 = 29,\ p_{10} = 31,$$

$$\wp = \prod_{i=1}^{n} p_i = 17160990.$$

Оскільки розрядність залишків змінюється залежно від величини модулів p_i то доцільно визначити мінімальний і максимальний обсяг даних (рис.3):

$$v_{3\min} =]\log_2 17160990[+]\log_2 3[+]\log_2 2[= 28 \text{ біт},$$

$$v_{3\max} =]\log_2 17160990[+]\log_2 31[+]\log_2 30[= 35 \text{ біт}.$$

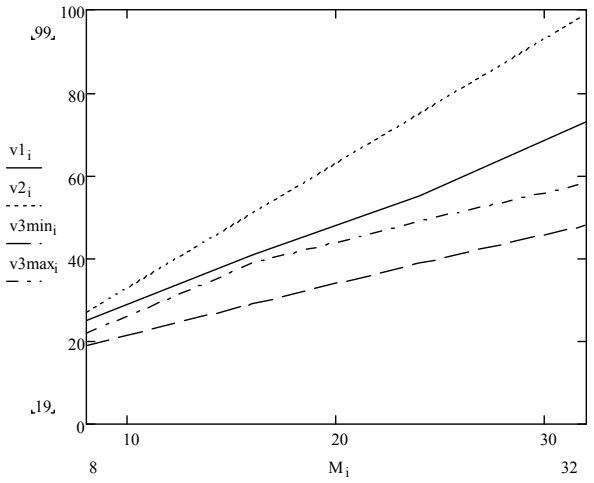

Рис. 3. Залежність обсягу даних v від розрядності пакета даних M для різних порогових схем поділу: v1 – схема Шаміра; v2 – схема Асмута-Блума; v3 – розділення на основі системи залишкових класів

Експериментально встановлено, що зменшити обсяги даних при використанні порогових схем для поділу повідомлення на частини можна передаючи лише пакети зі змінними складовими, при цьому постійні складові, необхідні для відновлення даних, передавати окремим пакетом (рис.4).

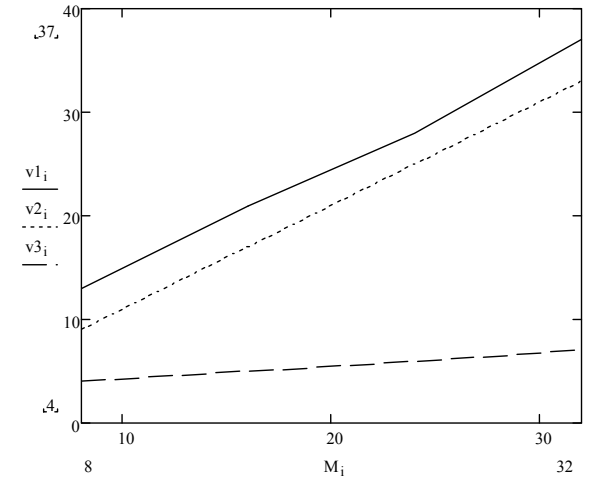

Рис.4. Залежність обсягу даних v від розрядності пакета даних M без врахування постійних складових: v1 – схема Шаміра; v2 – схема Асмута-Блума; v3 – розділення на основі системи залишкових класів

Висновки

Науковою новизною роботи є розроблений метод передачі даних на основі перетворення системи залишкових класів та багатошляхової маршрутизації, який забезпечує можливість відновлення втрачених пакетів даних та характеризується меншою надлишковістю порівняно з пороговими схемами поділу секрету:

– в 1,5 рази при передачі службових даних з кожною частиною пакета;

– в 5 разів при передачі службових даних окремим пакетом.

Ще однією перевагою запропонованого підходу є те, що в результаті поділу повідомлення на частини формуються підпакети (залишки) різної розрядності – це дає можливість розподіляти їх залежно від інтегральної оцінки якості маршруту, тим самим збільшити можливості схеми виявлення помилок.

Практичне значення одержаних результатів. Запропонований алгоритм передачі даних на основі системи залишкових класів може бути використаний при розробці протоколів маршрутизації в безпровідних сенсорних мережах.

Перспективи дослідження. Планується провести оцінку захищеності передачі даних на основі запропонованого підходу.

Література: 1. *Lou W.* An efficient N-to-1 mutlipath routing protocol in wireless sensor networks // Proc. of IEEE international Conference on Mobile Ad-hoc and Sensor Systems (MASS), Washington, DC, November 2005. **2.** *Жуков И.А., Дрововозов В.И.* Способы повышения надежности и безопасности сбора информации в системах управления реального времени // Проблеми інформатизації та управління. 2008. 1(23). С. 262– 276. **3.** *Столлингс В.* Беспроводные линии связи и сети: Пер. с англ. М.: Издательський дом «Вильямс», 2003. 640 с. **4.** *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение, 2-е издание: Пер. с англ. М.: Издательський дом "Вильямс», 2003. 1104 с. **5.** *Sachenko A., Yatskiv V., Krepych R.* Modified Method of Noise-Immune Data Transmission in Wireless Sensors Networks // International Conference on Networks Security, Wireless Communications and Trusted Computing, "NSWCTC 2009", 25-26 April 2009, Wuhan, Hubei, China, Volume 2. P.847–850. **6.** *Lou W., Liu W., Fang Y.* SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004. **7.** *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с. **8.** *Червяков Н. И., Сахнюк П. А., Шапошников А. В., Рядов С. А.* Модулярные параллельные вычислительные структуры нейро-процессорных систем / Под. ред. Н.И. Червякова. М.: Физматлит, 2003. 288 с.

Надійшла до редколегії 20.05.2010

Рецензент: д-р техн. наук, проф. Крилов В.М.

Яцків Василь Васильович, канд. техн. наук, доцент кафедри спеціалізованих комп'ютерних систем Тернопільського національного економічного університету. Наукові інтереси: кодування та передача даних в безпровідних сенсорних мережах, модулярна арифметика. Адреса: Україна, 46004, Тернопіль, вул. Львівська, 11, тел. (0352) 43-01-46. E-mail jazkiv@ukr.net