УДК 621.391

*А. В. ПЕРСИКОВ, Я. В. ДОРОШЕНКО*

# НЕКОТОРЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ФУНКЦИЙ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ НА ОСНОВЕ КОНЦЕПЦИИ AUTONOMIC COMPUTING

Современные телекоммуникационные системы (ТКС) являются нестационарными системами с динамически меняющейся структурой, управляющими информационными потоками за счет перераспределения ресурсов сети. Такие системы достаточно трудно разделить на независимые составляющие, так как процесс адаптации/реструктуризации структуры ТКС в целях оптимального перераспределения ресурсов сети приводит к стиранию четких границ между подсистемами [2, 4].

Новым подходом к построению систем, способных производить реструктуризацию телекоммуникационной сети для обеспечения возможности реализации оптимальных управляющих решений, является идея автономных систем (Autonomic Computing, AC). Они представляют собой совокупность сетевых элементов и программных модулей (ПМ), решающих локально в совокупности единую телекоммуникационную задачу, формируемую координационным центром. АС строятся на основе принципов самоконфигурируемости, самовосстанавливаемости, самозащищенности и самооптимизации; идея использования АС в управлении телекоммуникационными сетями есть решение проблемы продолжения предоставления услуг при частичном или полном разрушении связей внутри системы управления, вызванных отказами сетевых элементов или нарушениями политик безопасности в ТКС [1, 3].

АС представлена множеством пар агент–менеджер, выполняющих сходные или взаимосвязанные задачи без интенсивного информационного обмена с другими АС (рис. 1). АС формируются динамически непосредственно в той части ТКС, где решение сетевых задач (передача, обработка, хранение информации и др.) будет наиболее эффективным по критерию минимума необходимого сетевого ресурса. При правильной организации АС не требуется передачи больших объемов данных по каналам связи, уменьшается загрузка каналов и сетевого оборудования и отпадает потребность в шифровании данных и формировании безопасных каналов с заданными показателями качества обслуживания. АС способны по своей инициативе создавать или присоединять объекты для расширения функциональности, в результате чего возникают угрозы, связанные с загрузкой вредоносного кода, присоединения объектов, обладающих низким показателем надежности функционирования и утечки ресурсов вследствие потери связи АС с остальной частью системы управления.


Рис. 1

В таком случае дальнейшее поведение зависит от архитектуры: система либо перестает функционировать, либо распадается на множество АС, которые начинают независимо работать и противодействовать атаке [5, 7]. Нивелирование проблемы продолжения реализации сервисов в системе с некорректно работающими сетевыми элементами или разрушенными межэлементными связями требует решения следующих задач:

- преодоления проблем сложности безопасного сбора информации о состоянии агентов, менеджеров и сетевых элементов, управляемых ими;

- формирования точных оценок показателей надежности объектов, автономных систем и системы управления в целом без применения ресурсоемких процедур сбора информации;

- формирования интегральных оценок характеристик элемента, включающих безопасность, структурную целостность, надежность и отказоустойчивость;

- контроля изменения оценок во времени, когда АС ограничена в возможности обмена информацией с внешней по отношению к ней среде.

Решению этих и сопутствующих им задач посвящена данная работа.

**Использование архитектуры автономных систем для создания высоконадежных телекоммуникационных сервисов**

Одной из наиболее важных проблем, влияющих на возможность предоставления телекоммуникационных услуг с запрашиваемыми характеристиками качества обслуживания, является проблема обеспечения быстрой реакции ТКС на изменения трафика [4]. Очевидным адекватным решением, обеспечивающем своевременную обработку изменений, является задача динамического, в режиме реального времени, управления информационными потоками за счет перераспределения ресурсов сети. Данное решение находится на основе выборочной статистики и в общем случае обеспечивается при выполнении последовательности операций: наблюдение (измерение) – оценка – управление [4, 8].

Все обозначенные операции эффективно решаются локально с использованием рекурсивных процедур [8], с исключением активного информационного обмена между агентами и менеджерами и нивелированием роли координационного центра, ответственного за выработку глобальных управляющих воздействий. Естественной концепцией разработки таких систем является концепция АС, предложенная Intel и внедряемая многими производителями телекоммуникационного оборудования.

В ТКС важную роль играют характеристики доступности, надежности и структурной целостности систем. Их обеспечение может быть просто реализовано на основе ядра системы управления, построенного по одноранговому принципу [9] и использования ПМ, функционирующих на выбираемых в зависимости от условий задачи и состояния сети серверах приложений или виртуальных машинах [10].

Формирование АС должно быть произведено безопасным образом. Проще всего это реализуется на основе самозащищающихся платформ [5] с использованием криптографических методов защиты – обеспечения конфиденциальности (путем шифрования данных) и целостности (применения электронных цифровых подписей, ЭЦП). При взаимодействии множества объектов общий используемый секрет эффективно вырабатывается из ЭЦП, которые формируются для объектов, входящих в АС, например, с помощью схемы Шамира [6].

При использовании схемы разделения секрета, общий секрет $s$ может формироваться на основе ЭЦП ПМ. Например, для схемы Шамира, где в качестве секрета $s$ выбирается некоторое целое число из диапазона $[0...p-1]$, $p$ – простое число, процедура формирования общего секрета сводится к следующему. Аппаратная платформа (АП) собирает $t$ ЭЦП ПМ $a_1, ..., a_t \mod p$, формирует и распределяет $i$ теней $s_i = f(i) \bmod p$, вычисленных для многочлена $f(X) = s + a_1 X + ... + a_t X^t$. Таким образом, $(t+1)$ ПМ могут восстановить секрет $s$, тогда как $t$ ПМ не могут этого сделать.

Общий секрет должен обновляться либо периодически (например, раз в 5 минут [12]) или по мере появления нового объекта в АС. Процедура обновления предполагает выполнение следующих действий. Каждый ПМ $i$ случайно разыгрывает коэффициенты многочлена $f_i(X)$ степени $t$, такого что $f_i(0) = 0$. Затем ПМ $i$ посылает АП $j$ значение $s_{ij} = f_i(j) \bmod p$. АП $j$ вычисляет новую тень $\hat{s}_j$:

$$\hat{s}_j = s_j + s_{1j} + ... + s_{nj} \bmod p$$

и затем стирает старую. Легко видеть, что новые тени удовлетворяют многочлену степени $\hat{f}(X) = f(X) + f_1(X) + ... + f_n(X)$ степени $t$, с секретом $s$ в качестве свободного члена. Процедура гарантирует эффективное противодействие атакам со стороны ПМ, имеющего доступ к памяти сервера приложений, но не способного влиять на его работу.

Отталкиваясь от задач реструктуризации и определения АС [4,5], можно прийти к возможности множественных реализаций АС и различным пространствам состояний моделей реализаций. Любая заданная временная система $S$ может иметь много различных реализаций, а две различные пары семейств реакций системы $(\overline{\rho})$ и функций перехода $(\overline{\varphi})$ $(\overline{\rho}, \overline{\varphi})$ и $(\overline{\hat{\rho}}, \overline{\hat{\varphi}})$, могут быть динамическими реализациями одной и той же АС. Поскольку динамика поведения системы описывается в терминах изменения ее состояний, т.е. выбор реализации системы должен подразумевать минимальность реализации, т.е. минимальность пространства состояний [11]. Рассмотрим этот момент с позиций алгоритмов реализации АС.

Алгоритм реализации АС $S$ и выбора реализации должен учитывать критерий вероятности работы ТКС в нескомпрометированном состоянии (одно из условий структурной целостности). Критерий вводится одновременно с решением задачи оптимизации, которая формулируется следующим образом [17]: в системе имеется $n$ АС; каждая $j$-я АС $j \in J = \{1, 2, ..., n\}$ может находиться в одном из двух состояний: доступности $s_j$ и недоступности $\overline{s_j}$. В произвольный фиксированный момент времени $t \in T$ система может находиться в одном из $2^n$ состояний $(s_1, ..., s_{j_1-1}, \overline{s}_{j_1}, s_{j_1+1}, ..., \overline{s}_{j_i-1}, s_{j_i}, s_{j_i+1}, ..., s_n)$. Каждое состояние системы характеризуется показателем условной вероятности $P_{i_1,...,i_j}$ функционирования системы в данном состоянии. Показатель условной вероятности функционировния системы, когда все подсистемы не скомпрометированы и доступны, обозначим $P_0$. Задача может формулироваться следующим образом: найти такую реализацию АС, которая удовлетворив ограничениям, могла бы обладать наивысшей доступностью.

Объекты $u_{jk}$ АС характеризуют доступностью функций АС, которая может быть задана множеством вероятностей $p_j(u_{jk})$, $k \in K_j$ ($K_j = \{1, 2, ..., K_j^*\}$ – множество индексов типов элементов) и технико-экономическими характеристиками $g_{ij}(u_{jk})$ и могут резервироваться с кратностью резервирования $\nu_{jk} \in [\alpha_{jk}, \beta_{jk}]$, где $\alpha_{jk}$ и $\beta_{jk}$ – минимальная и максимальная кратности резервирования. Значения вероятностей $p_j(v_j)$ и ресурсов $g_{ij}(v_j)$ на варианте реализации $v_j \in V_j$ $j$-й АС определяются элементным составом варианта реализации, кратностями резервирования и числом различных типов входящих в него элементов.

Исследовав конструктивные возможности формирования вариантов АС, сформируем возможные решения

$$\Re_{K_j}^{r_j} = \{k_{l_j}(r_j) = \{k_1^{l_j}, ..., k_p^{l_j}, ..., k_{r_j}^{l_j}\},\ k_p^{l_j} \in K_j, l_j = 1, 2, ..., C_{|K_j|}^{r_j},\ r_j \in R_j\}, \quad (1)$$

где $R_j = \{1, 2, ..., r_j, ..., k_j^*\}$ – множество длин вариантов реализации $j$-й подсистемы ($r_j \in R_j$ – длина, т.е. число различных типов элементов, используемых при резервировании). $\Re_{K_j}^{r_j}$ – множество сочетаний по $r_j$ индексов из множества $K_j$. Для каждого сочетания $k(r_j) \in \Re_{K_j}^{r_j}$ длины $r_j$ определим множество $V_{jk(r_j)} = \{v_{jk(r_j)}^{\nu_j}\}$ возможных вариантов $v_{jk(r_j)}^{\nu_j} = (\nu_{jk_1} u_{jk_1}, ..., \nu_{jk_p} u_{jk_p}, ..., \nu_{jk_{r_j}} u_{jk_{r_j}})$ длины $r_j$. Обозначим $V_j^{r_j} = \bigcup_{k(r_j) \in \Re_{K_j}^{r_j}} V_{jk(r_j)}$ – множество вариантов $v_{jk(r_j)}^{\nu_j}$ длины $r_j$. Тогда $V_j = \bigcup_{r_j \in R_j} V_j^{r_j}$.

Вероятность нахождения в нескомпрометированном состоянии и значения показателей (определяющих структурную целостность) ресурсов $j$-й подсистемы на варианте $v^{v_j}_{jk(r_j)}$ определяются по формулам:

$$p_j(v^{v_j}_{jk(r_j)}) = 1 - \prod_{k_p \in k(r_j)} (1 - p_j(u_{jk_p}))^{v_{jk_p}}, \quad (2)$$

$$g_{ij}(v^{v_j}_{jk(r_j)}) = \sum_{k_p \in k(r_j)} v_{jk_p g_{ij}}(u_{jk_p}),\ i \in I,\ j \in J. \quad (3)$$

Выбор из возможных вариантов $\Re$ производится из условия (3) методами нелинейной оптимизации.

Задача формирования АС может решаться как вне объектов, которые в будущем сформируют АС (внешнее управляющее воздействие, инициируемое координационным центром), так и самими объектами (процесс самоорганизации). Это есть задача формирования минимальной реализации системы, которую решают как несколько элементарных задач с условиями (2) и (3):

- формирование классов интересующих нас АС $\Im_D$;
- введение в каждом классе отношение эквивалентности;
- введение в каждом классе эквивалентности отношения порядка, с помощью которого определяется минимальность реализации.

Формирование классов АС выполняется путем задания функции, которая описывает решение той или иной телекоммуникационной задачи, определения множества ограничений и определения цели – множества возможных состояний. Эквивалентность реализаций АС может формулироваться как совокупность условий следующим образом [11]:

- эквивалентность относительно пар «вход-выход»: $S_0^{\rho} = S_0^{\hat{\rho}}$, т.е.

$$(\forall c)(\forall x)(\exists \hat{c})[\rho_0(c,x) = \hat{\rho}_0(\hat{c},\ x)] \,\&\, (\forall \hat{c})(\forall x)(\exists c)[\rho_0(c,x) = \hat{\rho}_0(\hat{c},x)].$$

- эквивалентность относительно реакций

$$(\forall c)(\exists \hat{c})(\forall x)[\rho_0(c,x) = \hat{\rho}_0(\hat{c},\ x)] \,\&\, (\forall \hat{c})(\exists c)(\forall x)[\rho_0(c,x) = \hat{\rho}_0(\hat{c},x)].$$

- эквивалентность относительно своих реакций на входные воздействия:

$$(\forall x)[\rho_0(c_0,x) = \hat{\rho}_0(\hat{c}_0,x)].$$

Отношение порядка $\leq$ на классе эквивалентности может определяться как $(\overline{\rho},\overline{\varphi}) \leq (\overline{\hat{\rho}},\overline{\hat{\varphi}}) \Leftrightarrow K(C) \leq K(\hat{C})$ исходя из мощностей множеств класса эквивалентности.

**Учет взаимных влияний отказов и событий безопасности**

Для современных ТКС не существует общепринятого понятия отказ, как как внутренние изменения в структуре системы из-за отказа отдельных элементов приводят, как правило, лишь к некоторому ухудшению ее надежности (через ухудшение показателей надежности объектов $p_i$), а не к полному отказу системы. Это объясняется тем, что в сложных системах с избыточной структурой имеется полное или частичное резервирование отдельных функций, а также различные обратные связи, средства коррекции ошибок и т.д.

Основной проблемой на сегодняшний день при оценке защищенности систем в целом является необходимость учета изменяющихся связей между сетевыми элементами и ПМ, реализующими управление. При реструктуризации сети изменение связей является необходимым и поэтому реальный уровень защиты системы в целом будет постоянно изменяться.

Основным нормативным документом, который используется для оценки степени защищенности программных систем, является стандарт «Общие критерии безопасности» [13-15]. Его применение справедливо, поскольку стандарт использует концепцию объекта оценки, структура которого произвольна и акцентирует внимание на процессах, происходящих в самом объекта и при информационном обмене объекта с внешней средой.

Оценка защищенности системы $E$ может формироваться путем задания множества функциональных классов $FC$, которым соответствует объект оценки. Затем определяется индикатор оценки, который есть значение интервала EAL (уровень защищенности), соответствующий

мощности множества $FC$ (рис. 3). Это справедливо, так как стандарт требует постоянного увеличения уровня защищенности путем ужесточнения требований защищенности [15].

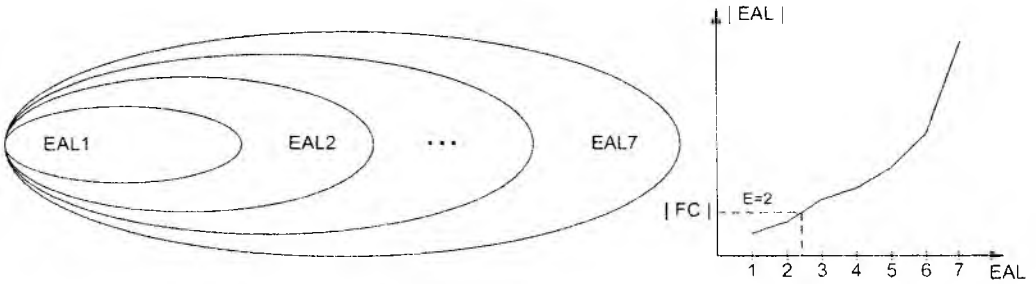


Рис. 3

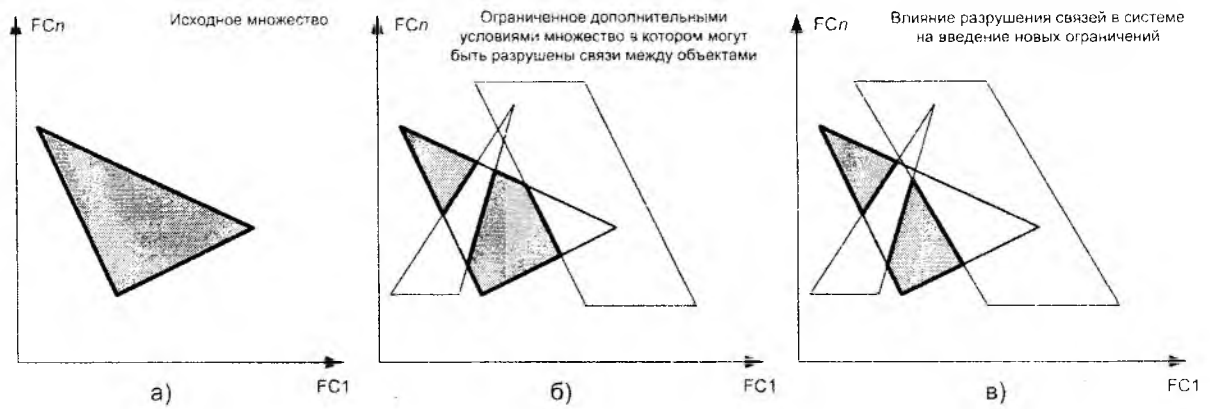


Рис. 4

Интегральная оценка характеристик системы в целом может формироваться как мощность множества точек в гиперпространстве соответствования требованиям функциональных классов ( $FC1-FCn$ ) (рис. 4). Оценку динамически изменяющейся структуры телекоммуникационной сети необходимо получать с учетом совокупного влияния двух явлений:

- влияния надежности элементов и отказоустойчивости системы на корректность работы системы безопасности (переход рис. 3, *а*, *б*, с уменьшением мощности множества);
- влияния деструктивных явлений, нивелируемых системой безопасности на надежность элементов и отказоустойчивость системы управления (переход рис. 3, *б*, *в*, дальнейшее уменьшение мощности множества, сформированного из допустимых вариантов реализации).

Для АС с произвольной структурой определим ее надежность через надежность работы ее объектов. АС состоит из $n$ объектов $j$, $j \in J = \{1,2,...,n\}$. Объекты $s_j$, входящие в структуру АС, могут находиться только в одном из двух состояний: работоспособности и отказа ($s_j = \begin{cases} 1, \text{ если объект } j \text{ работоспособен;} \\ 0, \text{ если объект } j \text{ неработоспособен;} \end{cases}$), и при этом отказы происходят независимо друг от друга. АС может быть в данном случае представлена в виде вектора $s = (s_1,...,s_j,...,s_n)$, который характеризует состояние системы через состояния объектов.

Надежность (индексы указывают работоспособные объекты) определяется по формуле

$$P = \sum_{(j_1,...,j_l) \in G} \Phi_{j_1,...,j_l} H_{j_1,...,j_l}, \qquad (4)$$

где $H$ – вероятность нахождения системы в определенном состоянии; $\Phi$ – показатель условной вероятности работоспособности системы; и суммирование производиться по всему множеству $G$, которое представляет собой все возможные комбинации индексов объектов, требуемых для каждого из вариантов в $V$.

Предполагая взаимные независимости отказов объектов, вероятности $H$ вычисляются через вероятности работоспособности $p_j$, $j \in J$, объектов:

$$H = \prod_{\substack{j \in J \\ j = j_1 \dots j_l}} p_j \prod_{\substack{r \in J \\ r \neq j_1 \dots j_l}} (1 - p_r). \qquad (5)$$

Когда АС приобретает жесткую структуру и объем информационного обмена с другими объектами уменьшается практически до нуля, оценка вероятности отказа внешнего объекта может быть получена на основе двух предположений:

- постепенного уменьшения надежности объекта со временем $t$

$$\hat{H}(t) = H(0) \cdot (\lambda(t) \cdot e^{-\lambda(t)t}), \qquad (6)$$

где $\lambda(t)$ – интенсивность отказа ($\lambda(t) = f(E,t)$, $f(E)$ – функционал от оценки защищенности, обычно ступенчатая функция [16]), зависящая от времени и начального значения оценки защищенности;

- мгновенного перехода в состояние отказа объекта после истечении определенного интервала времени $\hat{H}(t) = \begin{cases} H(0), & t_0 \le t < t_{отк}; \\ 0, & t \ge t_{отк}. \end{cases}$. Здесь $H(0) = H(t_0)$ – вероятность отказа объекта, оцененная на момент окончания информационного обмена с ним.

**Выводы**

Исследованы подходы к обеспечению безопасности систем, построенных на основе концепции Autonomic Computing (автономных систем), активно развиваемой производителями телекоммуникационных технологий и фирмой Intel. Был предложен метод формирования общего секретного ключа (секрета) на основе схемы Шамира с использованием ЭЦП объектов АС. Это позволяет, используя единственный доверительный объект, функционирующий на самозащищающейся платформе начать безопасный сеанс обмена данными между объектами. Рассмотрен подход к формированию оценок защищенности АС, определению доступности функций АС, а также условия формирования оптимальной структуры АС для решения конкретной телекоммуникационной задачи.

**Список литературы:** 1. *Персиков А.В., Еременко А.С.* Вопросы обеспечения безопасности пользователей в динамических операционных средах на основе беспроводных технологий // Специализированное издание журнала «Труды УНИИРТ». 2007. С.81-84. 2. *Persikov A.* Private security in smart environments in wireless local area networks // Тези доповідей наук.-техн. конференції «Проблеми телекомунікацій». 2007. С. 185-186. 3. *Поповський В.В., Персіков А.В.* Методика оценки защищенности корпоративных сетей при наличии в них сегментов, построенных на основе технологий беспроводных сетей // Тези доповіді 3-го наук.-практ. семінару «Безпека систем безпроводового зв'язку». Київ, 2004. 4. *Поповский В.В.* Модель управления реструктуризацией телекоммуникационной сети. // Радиотехника 2004. №138. С. 25-31. 5. *Agosta J.M. et al.* Towards autonomic enterprise security: self-defending platforms, distributed detection, and adaptive feedback // Intel Developer Journal, 2006. vol. 10, issue 4, p. 285-297. 6. *Поповский В.В., Персиков А.В.* Защита информации в телекоммуникационных системах. Т. 1.Харьков: ООО «Компания СМИТ», 2006. 238с. 7. *An architectural* blueprint for autonomic computing. IBM Corporation 2006. pp. 37., 8. *Сейдж Э., Мелс Дж.* Теория оценивания и ее применение в связи и управлении. М.: Связь, 1976. 496 с. 9. *Kumar R., Yao D.D., Bagchi A., Ross K.W., Rubenstein D.* Fluid modeling of pollution proliferation in P2P networks. ACM Sigmetrics 2006, St. Malo, France, 2006. 10. *Персиков А.В., Еременко А.С.* Исследование методов балансировки вычислительной нагрузки инфраструктуры точек доступа к мультисервисным системам // Восточно-Европейский журнал передовых технологий. 2004. №5.С.82-87. 11. *Месарович М., Такахара Я.* Общая теория систем. Математические основы. М.: Мир, 1978. 314с. 12. *RFC 4120.* Neuman C., Yu T., Hartman S., Raeburn K. The Kerberos Network Authentication Service (V5). July 2005. 13. *Common* Criteria for Information Technology Security Evaluation v. 3.0 Part 1: Introduction and general model. 14. *Common* Criteria for Information Technology Security Evaluation v. 3.0 Part 2: Security functional components. 15. *Common* Criteria for Information Technology Security Evaluation v. 3.0 Part 3: Security assurance components. 16. *Тихонов В.И.* Статистическая радиотехника. М.: Радио и связь, 1982. 623 с. 17. *Волкович В. Л., Волошин А. Ф., Заславский В. А., Ушаков И. А.* Модели и методы оптимизации надежности сложных систем. К.: Наук. думка, 1992. 312 с. 18. *Мину М.* Математическое программирование. Теория и алгоритмы. М.: Наука, 1990. 488 с.

*Харьковский национальный университет радиоэлектроники*

*Поступила в редколлегию 07.11.2007*