УДК 621.391

А.В. ЛЕМЕШКО, д-р техн. наук, А.С. ЕРЕМЕНКО, д-р техн. наук,
А.В. ПЕРСИКОВ, БАТУЛЬ СЛЕЙМАН

МОДЕЛЬ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ НА ОСНОВЕ ОПРЕДЕЛЕНИЯ МАКСИМАЛЬНОГО КОЛИЧЕСТВА НЕПЕРЕСЕКАЮЩИХСЯ ПУТЕЙ ДЛЯ МИНИМИЗАЦИИ ВЕРОЯТНОСТИ КОМПРОМЕТАЦИИ КОНФИДЕНЦИАЛЬНЫХ СООБЩЕНИЙ

Введение

Под сетевой безопасностью понимается деятельность, направленная на обеспечение защиты передаваемой информации и сети в целом, которая включает в себя как аппаратные, так и программные технологии [1 – 5], реализуемые в инфокоммуникационных сетях (ИКС). Сетевая безопасность сочетает в себе несколько уровней защиты на границе сети, а также на уровне транспортной ИКС. При этом каждый уровень сетевой безопасности должен реализовывать соответствующие функции защиты сетевой инфраструктуры, обеспечивающей безопасность сетевых элементов (таких как маршрутизаторы, серверы, каналы связи) и маршрутов в целом.

Процесс маршрутизации является фундаментальным механизмом функционирования инфокоммуникационных сетей, в том числе с точки зрения обеспечения их безопасности при предоставлении сетевых сервисов и предотвращения возможных атак [6]. Разработка и внедрение протоколов безопасной маршрутизации является актуальной научно-практической задачей. Одно из направлений обеспечения заданного уровня безопасности в ИКС – реализация механизма SPREAD [7, 8], основанного на многопутевой доставке фрагментов конфиденциального сообщения. При этом исходное сообщение разделяется на фрагменты (части) в соответствии со схемой Шамира [7 – 9]. Цель механизма SPREAD заключается в минимизации вероятности компрометации сообщения вследствие того, что злоумышленнику необходимо скомпрометировать не один маршрут, по которому передается неразделенное сообщение, а все пути, по которым передаются его фрагменты. В ходе безопасной маршрутизации конфиденциального сообщения в сети в соответствии с механизмом SPREAD необходимо решить следующие задачи [7, 8]:

1. Определение множества непересекающихся путей между заданной парой узлов отправитель и получатель.
2. Разделение исходящего сообщения на множество фрагментов в соответствии с выбранной схемой Шамира и их балансировка по множеству непересекающихся путей, определенных в ходе решения первой задачи.

Благодаря обоснованному выбору путей прохождения пакетов между парой узлов отправитель-получатель определяются численные значения показателей безопасности, а использование непересекающихся маршрутов гарантирует, что компрометация одного элемента сети (узла или канала) приведет к компрометации лишь одного, а не множества маршрутов [7, 8]. В общем случае при использовании схемы Шамира вероятность компрометации k-го сообщения рассчитывается согласно выражению [7, 8, 10]

$$P_{msg}^{k} = \prod_{i=1}^{\mathrm{M}^{k}} p_n , \qquad (1)$$

где p_n – вероятность компрометации n-го пути; M^{k} – общее число используемых непересекающихся путей при передаче фрагментов конфиденциального сообщения.

Стоит отметить, что чем большее путей M^{k} используется, тем ниже вероятность компрометации сообщения. С этой целью в данной работе предлагается математическая модель расчета максимального количества непересекающихся путей, использование которых спо-

собствует снижению вероятности компрометации конфиденциальных сообщений при реализации безопасной маршрутизации.

1. Обзор существующих решений

Как показал анализ [10 – 20], в публикациях, посвященных решению маршрутных задач, достаточное внимание уделяется вопросам расчета множества непересекающихся путей, а также *N*-путевой маршрутизации. Особенности этих подходов представлены ниже.

Так, в работе [10] разработан метод безопасной быстрой перемаршрутизации сообщений в сети, который относится к классу проактивных и реактивных решений по обеспечению заданного уровня информационной безопасности. Новизна метода заключается в том, что в случае нарушения требований информационной безопасности в сети, вызванного повышением вероятности компрометации одного или множества композитных непересекающихся путей, входящих в основной мультипуть, многопутевая передача частей конфиденциального сообщения с обеспечением заданных значений вероятности его компрометации будет осуществляться уже по заранее рассчитанному множеству резервных композитных путей, реализуя защиту или основного мультипути в целом, или одного или нескольких заранее заданных композитных путей, входящих в этот основной мультипуть.

В работе [12] предложено комплексное решение безопасной отказоустойчивой маршрутизации при расчете мультипути, который состоит из непересекающихся путей, основанное на схеме распределенной внутрисетевой верификации. Предложенные решения являются эвристическими и ориентированы только на применение в беспроводных сенсорных сетях.

В [13] предложены алгоритмы определения пары путей, не пересекающихся по узлам и проходящих через определенные узлы сети. В этой работе представлены эвристические алгоритмы, позволяющие найти решение задачи определения непересекающейся пары основного и резервного путей минимальной стоимости. В то же время авторы пытались найти решение, близкое к оптимальному, с минимальными временными затратами. Однако ограничением представленного решения является используемая стратегия однопутевой маршрутизации. В свою очередь, в [14] представлена эффективная эвристика глобальной защиты пути при получении непересекающихся путей (основного и резервного), использующих максимальную пропускную способность. Преимуществами предлагаемого решения являются поддержка защиты уровня качества обслуживания (Quality of Service, QoS) по показателю пропускной способности и достаточная вычислительная сложность.

Работы [15 – 17] посвящены задачам вычисления *N* путей. Так, в [15] найдено решение для поиска множества непересекающихся путей между источником и получателем таким образом, что общая «длина» путей минимизируется, а их условная стоимость ограничена заданным бюджетом.

В [18] предложено решение, основным преимущество которого – сокращение времени, необходимого для расчета основного и резервного межконцевых непересекающихся путей. В работе показано, что эта задача актуальна для ситуации, когда происходит сбой сетевого оборудования, что приводит к нескольким попыткам определения соответствующих альтернативных путей, а также к периодическим обновлениям схемы отказоустойчивой маршрутизации.

Алгоритм многопутевой маршрутизации при использовании непересекающихся по узлам путей для беспроводной mesh-сети был предложен в [19]. В этой работе используется маршрутизация от источника в процессе определения маршрутов и вычисляются непересекающиеся по узлам пути. Преимущество такого выбора мультипути заключается в том, что этот алгоритм легко вычислительно реализуем.

В [20] предложен улучшенный алгоритм, используемый для расчета множества непересекающихся минимальных (кратчайших) путей. Преимуществами этого решения являются его эффективность, с точки зрения возможности проанализировать надежность территориально-распределенных сетей.

Анализ существующих решений показал актуальность разработки эффективной модели безопасной маршрутизации на основе определения максимального количества непересекающихся путей с целью минимизации вероятности компрометации конфиденциальных сообщений. Данная модель может быть применена как основа алгоритмического обеспечения соответствующих протокольных решений, которые должны быть ориентированы на обеспечение безопасности сети.

2. Математическая модель расчета максимального количества непересекающихся путей при безопасной маршрутизации конфиденциальных сообщений

В рамках предлагаемой модели расчета максимального количества непересекающихся путей предположим, что структуру ИКС (рис. 1) описывает граф $G = (R, E)$, в котором:

$R = \left\{ R_i ; i = \overline{1, m} \right\}$ – множество вершин, моделирующих маршрутизаторы;

$E = \left\{ E_{i,j} ; i, j = \overline{1, m}; i \neq j \right\}$ – множество дуг, представляющих каналы связи.

Пусть с каждым k-м сообщением связан ряд функциональных параметров: K – множество сообщений, передающихся в сети; s_k – узел-отправитель ($k \in K$); d_k – узел-получатель ($k \in K$).

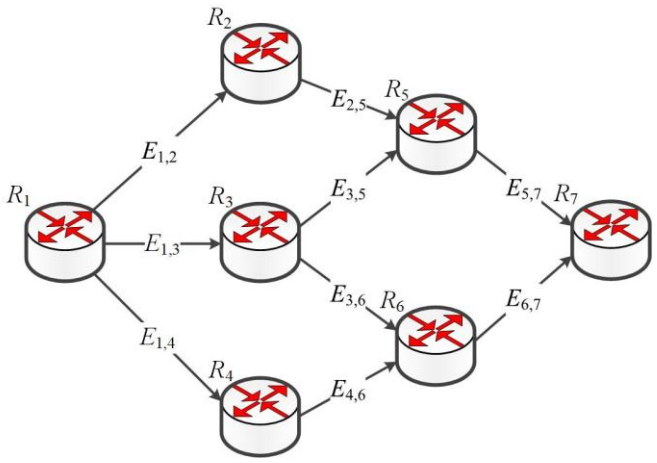

Рис. 1

В результате решения задачи расчета максимального количества непересекающихся путей при безопасной маршрутизации необходимо рассчитать множество переменных $a_{i,j}^k$, каждая из которых определяет принадлежность канала связи $E_{i,j} \in E$ множеству рассчитанных непересекающихся путей для фрагментированной передачи k-го сообщения. Количество управляющих переменных $a_{i,j}^k$ соответствует произведению $|K| \cdot |E|$.

На маршрутные переменные $a_{i,j}^k$ накладываются ограничения вида

$$a_{i,j}^k \in \{0;1\}. \tag{2}$$

Кроме того, должны выполняться условия для пары узлов отправитель-получатель:

$$\sum_{j:E_{i,j} \in E} a_{i,j}^k = \mathrm{M}^k;\ k \in K,\ \ R_i = s_k; \tag{3}$$

$$\sum_{j:E_{i,j} \in E} a_{j,i}^k = \mathrm{M}^k;\ k \in K,\ R_i = d_k, \tag{4}$$

где M^k уже трактуется как целочисленная переменная, характеризующая количество непересекающихся путей $\mathrm{M}^k \geq 1$, использующихся при реализации безопасной маршрутизации.

Тогда для транзитных узлов ИКС ($R_i \neq s_k, d_k$) имеют место ограничения:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k \leq 1, \quad k \in K; \\ \sum\limits_{j:E_{i,j}\in E} a_{j,i}^k \leq 1, \quad k \in K; \\ \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} a_{j,i}^k = 0, \quad k \in K. \end{cases} . \tag{5}$$

В качестве критерия оптимальности решения задачи расчета максимального количества непересекающихся путей при безопасной маршрутизации выбран максимум целевой функции

$$J = \mathrm{M}^k - \sum_{E_{i,j}\in E} w_{i,j} a_{i,j}^k . \tag{6}$$

В целевой функции (6) весовые коэффициенты $w_{i,j}$ выбираются таким образом, чтобы выбор множества M^k непересекающихся путей был ориентирован на минимизацию вероятности компрометации передаваемого конфиденциального сообщения:

$$w_{i,j} = -\log_{10}(1 - p_{i,j}) , \tag{7}$$

где $p_{i,j}$ – вероятность компрометации канала связи $E_{i,j} \in E$.

В свою очередь, вероятность компрометации отельного пути рассчитывается как

$$p_n = 1 - \prod_{E_{i,j}\in L_n} (1 - p_{i,j}) , \tag{8}$$

где L_n – упорядоченное множество каналов связи, составляющих n-й путь.

Таким образом, выбор $w_{i,j}$ на основании использования выражения (7) ориентирован на включение во множество непересекающихся путей каналов связи с минимальной вероятностью компрометации. Введение в (7) операции логарифмирования продиктовано тем, что при расчете вероятности компрометации путей (8) вероятности компрометации, выбранных в ходе полученного решения каналов, перемножаются, а второе слагаемое в (6) является аддитивной формой. Решение задачи расчета максимального количества непересекающихся путей свелось к решению оптимизационной задачи целочисленного линейного программирования (Integer Linear Programming, ILP) с критерием (6) при наличии линейных ограничений (2) – (5), поскольку маршрутные переменные являются булевыми, а переменные, характеризующие количество используемых непересекающихся путей M^k, принимают только целочисленные значения.

3. Численный пример решения задачи безопасной маршрутизации на основе расчета максимального количества непересекающихся путей

Особенности предложенной модели расчета максимального количества непересекающихся путей при безопасной маршрутизации продемонстрированы на следующем примере. Структура рассматриваемой сети показана на рис. 1, которая состоит из семи маршрутизаторов и девяти каналов связи. Пусть первый маршрутизатор будет отправителем, а седьмой –

получателем передаваемого конфиденциального сообщения. Рассмотрим порядок формирования множества непересекающихся путей при использовании предложенной модели на примере двух вариантов исходных данных, указанных в табл. 1 и отличающихся значениями вероятностей компрометации каналов связи на структуре ИКС, приведенной на рис. 1.

Таблица 1

Канал связи	$E_{1,2}$	$E_{1,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,5}$	$E_{3,6}$	$E_{4,6}$	$E_{5,7}$	$E_{6,7}$
Вероятности компрометации каналов связи									
Вариант 1	0,3	0,2	0,1	0,1	0,3	0,1	0,2	0,1	0,2
Вариант 2	0,3	0,1	0,1	0,1	0,2	0,1	0,2	0,1	0,2

В рамках рассматриваемой структуры сети (рис. 1) существует множество путей между первым и седьмым маршрутизаторами:

$$L_1 = \left\{E_{1,2}, E_{2,5}, E_{5,7}\right\};$$
$$L_2 = \left\{E_{1,3}, E_{3,5}, E_{5,7}\right\};$$
$$L_3 = \left\{E_{1,3}, E_{3,6}, E_{6,7}\right\};$$
$$L_4 = \left\{E_{1,4}, E_{4,6}, E_{6,7}\right\}.$$

Тогда при определении M^k могут быть получены три варианта возможных решений (табл. 2) по расчету непересекающихся путей, образующих соответствующий мультипуть. Использование того или иного мультипути обеспечивает результирующее значение вероятности компрометации сообщения (1).

Таблица 2

Мультипуть	L_1 и L_3	L_1 и L_4	L_2 и L_4
Вероятность компрометации сообщения			
Вариант 1	0,1836	0,1836	0,2103
Вариант 2	0,1524	0,1836	0,1492

Применение предложенной модели (1) – (8) позволило рассчитать оптимальный мультипуть (табл. 2) для каждого из вариантов исходных данных (табл. 1). В первом случае оптимальным по критерию (6) оказалось решение, связанное с использованием путей L_1 и L_4 (рис. 2). На рисунке сплошной линией выделены используемые в ходе получаемого решения каналы связи, в разрывах которых указаны их вероятности компрометации. Получаемое решение позволило обеспечить вероятность компрометации конфиденциального сообщения $P_{msg} = 0{,}1836$ (1). Это значение действительно является минимальным из трех возможных решений (табл. 2).

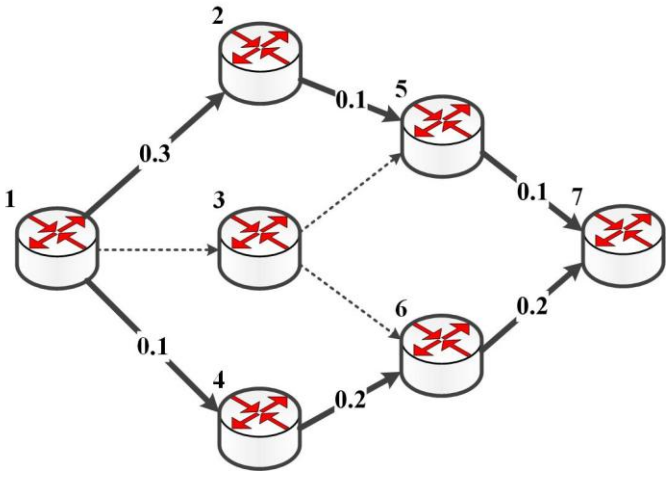

Рис. 2

Во втором варианте исходных данных (табл. 1) были изменены вероятности компрометации каналов связи $E_{1,3}$ и $E_{3,5}$. Поэтому применение предложенной модели (1) – (8) позволило получить новое оптимальное решение, которым является использование путей L_2 и L_4 (рис. 3). При этом обеспечивалась вероятность компрометации сообщения $P_{msg} = 0{,}1492$, значение которой также является минимальным из трех возможных решений (табл. 2). Обозначения на рис. 3, аналогичные рис. 2.

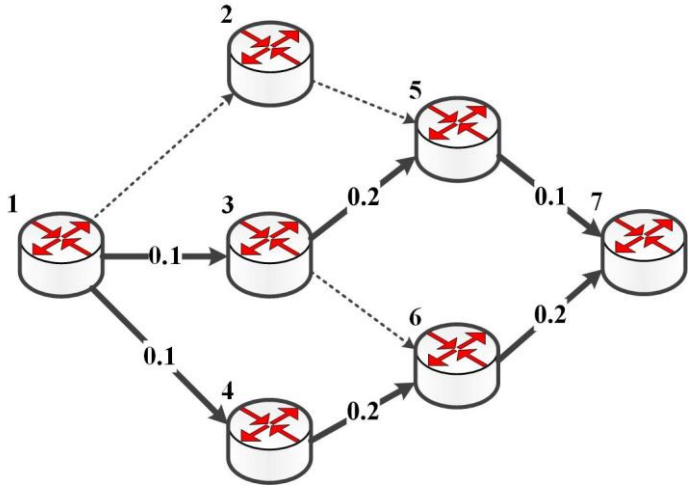

Рис. 3

Таким образом, результаты расчетов подтвердили адекватность используемой модели (1) – (8), а также ее эффективность с точки зрения получения множества непересекающихся путей, обеспечивающих минимальную вероятность компрометации передаваемого в сети конфиденциального сообщения.

Заключение

Предложена математическая модель безопасной маршрутизации на основе определения максимального количества непересекающихся путей для минимизации вероятности компрометации конфиденциальных сообщений. В модели (1) – (8) решение важной научно-практической задачи, связанной с реализацией безопасной маршрутизации в инфокоммуникационных сетях, свелось к решению оптимизационной задачи целочисленного линейного программирования с критерием (6) при наличии линейных ограничений (2) – (5), поскольку маршрутные переменные являются булевыми, а переменные, определяющие количество используемых маршрутов, принимают только целые значения.

Использование метрики (7) в критерии оптимальности (6) позволяет рассчитать множество непересекающихся путей, использование которых минимизирует вероятность компрометации конфиденциального сообщения при фрагментированной передаче, что было подтверждено на ряде численных примеров. Таким образом, использование предложенной модели для расчета максимального количества непересекающихся путей при реализации безопасной маршрутизации позволяет повысить уровень сетевой безопасности по показателю вероятности компрометации передаваемых сообщений.

Список литературы:

1. ITU-T X-805. Security architecture for systems providing end-to-end communications. October 2003. 28 p. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en.

2. ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989. 32 p.

3. ITU-T X-800. Security architecture for Open Systems Interconnection for CCITT applications. March 1991. 48 p. URL: https://www.itu.int/rec/T-REC-X.800-199103-I.

4. Stallings W. Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2016. 768 p.

5. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015. 398 p.

6. Lemeshko A. V., Evseeva O. Yu., Garkusha S. V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices // Telecommunications and RadioEngineering. 2014. Vol. 73, No. 15. P. 1339-1360. DOI: 10.1615/TelecomRadEng.v73.i15.30.

7. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks // IEEE Transactions on Vehicular Technology. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.

8. Yeremenko O. S., Ali S. A. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET // Radioelectronics and Informatics. 2015. № 1 (68). P. 26–29.

9. Alouneh S., Agarwal A., En-Nouaary A. A Novel Path Protection Scheme for MPLS Networks using Multipath Routing. Computer Networks: The International Journal of Computer and Telecommunications Networking. 2009. Vol. 53, No. 9. P. 1530–1545. DOI: 10.1016/j.comnet.2009.02.001.

10. Yeremenko O., Lemeshko O., Persikov A. Secure Routing in Reliable Networks: Proactive and Reactive Approach. Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 689. P. 631–655. DOI: 10.1007/978-3-319-70581-1_44.

11. Yeremenko O. S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the IEEE Second International Scientific-Practical Conference, Kharkiv, Ukraine, 13−15 October, 2015. Kharkiv : Kharkiv National University of Radio Electronics, 2015. P. 42–45. DOI: 10.1109/INFOCOMMST.2015.7357264.

12. Challal Y., Ouadjaout A., Lasla N., Bagaa M., Hadjidj A. Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks // Journal of network and computer applications. July 2011. Vol. 34, Issue 4. P. 1380-1397. DOI: https://doi.org/10.1016/j.jnca.2011.03.022.

13. Gomes T., Martins L., Ferreira S., Pascoal M., Tipper D. Algorithms for determining a node-disjoint path pair visiting specified nodes // Optical Switching and Networking. 2017. Vol. 23. P. 189-204. DOI: https://doi.org/10.1016/j.osn.2016.05.002.

14. Cruz P., Gomes T., Medhi D. A Heuristic for Widest Edge-disjoint Path Pair Lexicographic Optimization // Reliable Networks Design and Modeling (RNDM): Proceedings of the IEEE 2014 6th International Workshop, Barcelona, Spain. 17-19 Nov. 2014. P. 9-15. DOI: 10.1109/RNDM.2014.7014925.

15. Guo L. Efficient approximation algorithms for computing k disjoint constrained shortest paths // Journal of Combinatorial Optimization. July 2016. Vol. 32, Issue 1. P. 144-158. DOI: https://doi.org/10.1007/s10878-015-9934-2.

16. Eppstein D. Finding the k shortest paths. SIAM // Journal on computing. 1998. Vol. 28, Issue 2. P. 652-673. DOI: 10.1137/S0097539795290477.

17. Chang Z., Zhao G., Sun Y. A Calculation Method for The Reliability of a Complex k-out-of-n System. Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE) // Proceedings of the 2013 International Conference, Chengdu, China. 15-18 July 2013. P. 204-207. DOI: 10.1109/QR2MSE.2013.6625566.

18. Myslitski K., Rak J. Evaluation of Time-Efficiency of Disjoint Paths Calculation Schemes. Transparent Optical Networks (ICTON) // Proceedings of the 17th International Conference, Budapest, Hungary. 5-9 July 2015. P. 1-4. DOI: 10.1109/ICTON.2015.7193309.

19. Qu Z., Ren W., Wang Q. A new node-disjoint multi-path routing algorithm of wireless Mesh network. Computer, Mechatronics, Control and Electronic Engineering (CMCE) // Proceedings of the 2010 International Conference, Changchun, China. 24-26 Aug. 2010. Vol. 4. P. 1-3. DOI: 10.1109/CMCE.2010.5609590.

20. Shi Y. Calculation of Network System Reliability Based on Improved Disjointed Minimal Path Set. E-Product E-Service and E-Entertainment // Proceedings of the 2010 International Conference, Henan, China. 7-9 Nov. 2010. P. 1-4. DOI: 10.1109/ICEEE.2010.5660486.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 07.05.2019