

МАТЕМАТИЧНА МОДЕЛЬ РОЗРАХУНКУ МАКСИМАЛЬНОЇ КІЛЬКОСТІ ШЛЯХІВ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ, ПРИ БЕЗПЕЧНІЙ МАРШРУТИЗАЦІЇ

Процес маршрутизації є фундаментальним механізмом функціонування інфокомунікаційних мереж (ІКМ) в тому числі з точки зору забезпечення їх безпеки при наданні мережних сервісів та запобігання можливим атакам. Розробка та впровадження протоколів безпечної маршрутизації наразі залишається актуальним науково-практичним завданням. Одним з напрямків забезпечення заданого рівня безпеки в ІКМ є реалізація механізму SPREAD [1-4], заснованого на багатошляховій доставці фрагментів таємного повідомлення. При цьому вихідне повідомлення розділяється на фрагменти (частини) відповідно до схеми Шаміра [2]. Мета механізму SPREAD полягає в мінімізації ймовірності компрометації повідомлення завдяки тому, що зловмиснику необхідно скомпрометувати не один маршрут, по якому передається нерозділене повідомлення, а всі шляхи, по яких передаються його фрагменти. В ході безпечної маршрутизації повідомлення в мережі відповідно до механізму SPREAD необхідно вирішити наступні завдання [2-4]:

1. Визначення множини шляхів, що не перетинаються, між заданою парою вузлів відправник та одержувач.

2. Розподіл вихідного повідомлення на множину фрагментів відповідно до обраної схеми Шаміра та їх балансування за множиною шляхів, що не перетинаються, визначених у ході вирішення першого завдання.

При цьому завдяки обґрунтованому вибору шляхів проходження пакетів між парою вузлів відправник-одержувач визначаються числові значення показників безпеки, а

використання маршрутів, що не перетинаються, гарантує, що компрометація одного елемента мережі (вузла або каналу) спричинить компрометацію лише одного, а не декількох маршрутів [1, 2, 5]. В загальному випадку при використанні схеми Шаміра ймовірність компрометації k -го повідомлення розраховується відповідно до виразу [2, 6, 7]

$$P_{msg}^k = \prod_{i=1}^{M^k} p_i ,$$

де p_i – ймовірність компрометації i -го шляху. Варто зазначити, що чим більша кількість шляхів використовується, тим нижчою буде ймовірність компрометації повідомлення. Тому в даній роботі пропонується математична модель розрахунку максимальної кількості шляхів, що не перетинаються, при реалізації безпечної маршрутизації.

В рамках пропонованої моделі розрахунку максимальної кількості шляхів, що не перетинаються, припустимо, що структуру ІКМ описує граф $G=(R,E)$, в якому $R=\{R_i; i=\overline{1,m}\}$ – множина вершин, що моделюють маршрутизатори, а $E=\{E_{i,j}; i, j=\overline{1,m}; i \neq j\}$ – множина дуг, що представляють канали зв'язку. Нехай з кожним k -м повідомленням пов'язано ряд функціональних параметрів: s_k – вузол-відправник; d_k – вузол-одержувач, при $k \in K$, де K – множина повідомлень. В результаті розв'язання задачі розрахунку максимальної кількості шляхів, що не перетинаються, при безпечній маршрутизації необхідно розрахувати множину змінних $a_{i,j}^k$, кожна з яких визначає належність каналу зв'язку $E_{i,j} \in E$ множині розрахованих шляхів, що не перетинаються, для фрагментованої передачі k -го повідомлення. Кількість керуючих змінних $a_{i,j}^k$ відповідає добутку $|K| \cdot |E|$.

На маршрутні змінні $a_{i,j}^k$ накладаються обмеження виду:

$$a_{i,j}^k \in \{0;1\}. \quad (1)$$

Крім того, мають виконуватися наступні умови для пари вузлів відправник-одержувач:

$$\sum_{j:E_i, j \in E} a_{j,i}^k = M^k; \quad k \in K, \quad R_i = s_k; \quad (2)$$

$$\sum_{j:E_i, j \in E} a_{j,i}^k = M^k; \quad k \in K, \quad R_i = d_k, \quad (3)$$

де M^k – цілочисельна змінна, яка характеризує кількість шляхів, що не перетинаються ($M^k \geq 0$) та використовуються в ході реалізації безпечної маршрутизації.

Тоді для транзитних вузлів ІКМ ($R_i \neq s_k, d_k$) мають місце обмеження:

$$\begin{aligned} \sum_{j:E_i, j \in E} a_{j,i}^k &\leq 1; \quad \sum_{j:E_i, j \in E} a_{j,i}^k \leq 1; \\ \sum_{j:E_i, j \in E} a_{j,i}^k - \sum_{j:E_j, i \in E} a_{j,i}^k &= 0; \quad k \in K. \end{aligned} \quad (4)$$

Критерієм оптимальності рішень задачі розрахунку максимальної кількості шляхів, що не перетинаються, обрано умову

$$\max_{x, M^k} M^k. \quad (5)$$

Таким чином, рішення актуального наукового та практичного завдання, пов'язаного з розробкою математичної моделі розрахунку максимальної кількості шляхів, що не перетинаються, при реалізації безпечної маршрутизації в інфокомунікаційних мережах було зведено до розв'язання оптимізаційної задачі цілочисельного програмування з критерієм (5) при наявності лінійних обмежень (1)-(4), так як маршрутні змінні є булевими, а змінні, які визначають кількість використаних шляхів, приймають лише цілі значення.

Використання максимальної кількості шляхів при фрагментованій передачі таємного повідомлення сприяє мінімізації його ймовірності компрометації.

Література:

1. Alouneh, S. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing [Text] / S. Alouneh, A. Agarwal, A. En-Nouary // Computer Networks: The International Journal of Computer and Telecommunications Networking. – 2009. – Vol. 53, Issue 9. – PP. 1530 – 1545.

2. Lou, W. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks [Text] / W. Lou, Y. Kwon // Vehicular Technology, IEEE Transactions on. – 2006. – Vol. 55, Issue 4. – PP. 1320 – 1330.

3. Лемешко, А.В. Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам [Текст] / А.В. Лемешко, А.С. Еременко // Захист інформації, Національний авіаційний університет. – 2015. – Т. 17, №2. – С. 135-142.

4. Yeremenko, O.S. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET [Text] / O.S. Yeremenko, Ali S. Ali // Radioelectronics and Informatics. – 2015. – № 1 (68). – С. 26–29.

5. Еременко, А.С. Поточковая модель многопутевой маршрутизации по непересекающимся путям в телекоммуникационной сети [Електронний ресурс] / А.С. Еременко // Проблеми телекомунікацій. – 2015. – № 1 (16). – С. 85–93. – Режим доступу до журн.: http://pt.journal.kh.ua/2015/1/1/151_yeremenko_disjoint.pdf.

6. Yeremenko, O. Secure Routing in Reliable Networks: Proactive and Reactive Approach [Text] / O. Yeremenko, O. Lemeshko, A. Persikov // 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

7. Yeremenko, O. Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in

Communication Network [Text] / O. Yeremenko, O. Lemeshko, A. Persikov // 2017 XIIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), 2017. – P. 87–90.