ОГЛЯД МЕТОДІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Стаднік В.В., Крепко А.В.

Харківський національний університет
Повітряних Сил імені Івана Кожедуба, Україна

E-mail: stadnikvova1@ukr.net,
krepkoalla@ukr.net

Abstract

The relevance of research on ensuring the implementation of secure routing in information and communication networks for military purposes has been determined. A brief review of secure routing methods in information and communication networks of this class is conducted. Each group of analyzed methods is aimed at secure routing in networks with a certain topology when transmitting individual messages or packet flows. Some methods support regulation of the load balancing process depending on the requirements for network security and Quality of Service level.

Захист інформації, яка циркулює в інфокомунікаційних мережах військового призначення (ІКМ ВП), є найбільш пріоритетною задачею, успішне розв'язання якої може здійснюватися навіть шляхом деякого допустимого погіршення інших показників ефективності ІКМ ВП, наприклад, показників якості обслуговування. З цією метою практично до кінця минулого століття звичайною практикою було використання у мережах зв'язку військового призначення комунікаційного обладнання, апаратури засекречування та протоколів обміну, принципи роботи яких були здебільшого унікальними та таємними, що з часом дуже негативно почало впливати на сумісність мереж різних ланок управління. Для забезпечення максимально можливої сумісності апаратно-програмного та інноваційного забезпечення ІКМ, які використовуються в різних видах збройних сил та родах військ, а навіть у різних країнах одного військового блоку, більшість економічно розвинених країн з початку 2000-х років здійснили перехід до використання відкритих інфокомунікаційних стандартів на чотирьох нижніх (технологічно залежних) рівнях еталонної моделі взаємодії відкритих систем (Open Systems Interconnection model, OSI): фізичному, канальному, мережному та транспортному. Задачі ж забезпечення інформаційної безпеки шляхом шифрування даних, що передаються в ІКМ ВП, були віднесені до протоколів прикладного рівня моделі OSI.

З часом задачі зловмисників значно розширились, їх метою стало не тільки заволодіння конфіденційною інформацією або її компрометація, але й зрив самого процесу передачі інформації шляхом організації мережних атак, направлених на перевантаження комутаційного обладнання. Тому зараз для повноцінного забезпечення мережної безпеки мають задіється увесь доступний мережний ресурс на кожному з рівнів OSI. Важливе місце у цьому переліку займають протоколи маршрутизації, які використовуються на мережному рівні OSI з метою визначення оптимальних маршрутів з точки зору мінімізації або максимізації обраних показників ефективності ІКМ [1, 2]. На жаль існуючі протоколи маршрутизації досить обмежено враховують стан безпеки елементів ІКМ та мережі у цілому при розрахунку маршрутів передачі пакетів. Тому актуальним напрямком наукових та прикладних досліджень є розробка ефективних методів безпечної маршрутизації, які б стали алгоритмічно-програмною основою перспективних маршрутних протоколів.

У галузі безпечної маршрутизації накопичено досить потужний об'єм рішень та підходів, які відрізняються один від одного, перш за все, областю застосування, орієнтацією на певний контент, що передається, та рівнем безпеки, який має бути досягнутий. Так, наприклад, для передачі ключів та іншої конфіденційної інформації за допомогою окремих повідомлень, науковцями запропоновано

механізм SPREAD [3], у основу якого покладено схему Шаміра та використання множини шляхів, які не перетинаються. Базовий підхід було розвинено у роботах [4, 5] під випадок залучення шляхів, які допускають вузловий та канальний перетин, що дозволило біль ефективно використовувати доступний мережний та кіберресурс. Інший підхід, який розглядається, наприклад, у роботах [6-8], заснований на використанні метрик маршрутизації, які враховують рівень мережної безпеки елементів ІКМ, через які мають прокладатись маршрути. Прикладом такої метрики може слугувати ймовірність компрометації вузла та/або каналу або ж більш складна функція, яка враховує ризики інформаційної безпеки за допомогою базових метрик критичності вразливостей [6, 7]. Третя група методів базується на спробі комплексного забезпечення як високого рівня мережної безпеки, так і якості обслуговування шляхом управління процесом балансування трафіку за множиною найбільш безпечних/продуктивних шляхів [9-11].

Література

1. Лемешко О.В., Єременко О.С., Невзорова О.С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ. 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1

2. Лемешко О.В., Єременко О.С., Євдокименко М.О., Шаповалова А.С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. – Харків: ХНУРЕ, 2022. – 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1

3. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.

4. Yeremenko O., Lemeshko O., Persikov A. Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in Communication Network. Computer Sciences and Information Technologies (CSIT): Proceedings of the 2017 12th International Scientific and Technical Conference, Lviv, Ukraine, 5–8 September, 2017. IEEE, 2017. P. 87–90. DOI: 10.1109/STC-CSIT.2017.8098743

5. Лемешко О.В., Єременко О.С., Євдокименко М.О., Коваленко Т.М. Методика розрахунку ймовірності компрометації конфіденційних повідомлень при безпечній маршрутизації в інфокомунікаційних мережах з використанням шляхів, які перетинаються. Проблеми телекомунікацій. 2021. № 2 (29). С. 15–27.

6. Snihurov, A., Chakrian, V. “Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics”, Second International IEEE Conference on Problems of Infocommunications. Science and Technology (PIC S&T-2015), 2015, Kharkiv, P. 263-265, DOI: https://doi.org/10.1109/INFOCOMMST.2015.7357331

7. Lemeshko O., Yevdokymenko M., Shapoval M. Routing Model with Load Balancing on the Traffic Engineering Principles based on Information Security Risks, 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 572-576, doi: 10.1109/PICST54195.2021.9772193

8. Lemeshko O., Yeremenko O., Yevdokymenko M., Sleiman B. System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems. Vol. 152. Springer, Cham. 2021. P. 191–205. DOI: 10.1007/978-3-030-58359-0_10.

9. Lemeshko O., Shapovalova A., Al- Dulaimi A.M.K., Yeremenko O., Yevdokymenko M. Flow-Based Routing Model With Load Balancing Under Network Security Parameters // Information and Telecommunication Sciences. No 2 (2020). P. 44-50.

10. Lemeshko O., Yeremenko O., Shapovalova A., Hailan A.M., Yevdokymenko M., Persikov M. Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach. 2021 16th International Conference on the Experience of Designing and Application of CAD System in Microelectronic (CADSM), 22-26 February 2021. Lviv, Ukraine. P. 4/23-4/26.

11. Lemeshko O., Hu Z., Shapovalova A., Yeremenko O., Yevdokymenko M. Research of the Influence of Compromise Probability in Secure Based Traffic Engineering Model in SDN. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, 2021, vol 83. pp 47-55. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_5.