ОГЛЯД ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В БЕЗПРОВОДОВИХ МЕРЕЖАХ

*Л*емешко В.О., Персіков М.А.

Харківський національний університет
радіоелектроніки, Україна

E-mail: valentyn.lemeshko@nure.ua
E-mail: mykhailo.persikov@nure.ua

Abstract

The paper reviews the leading network solutions for information security in wireless networks. These solutions include, first of all, routing protocols, fault-tolerant routing, fast rerouting, filtering, and traffic policing mechanisms. The use of composite metrics that consider the basic functional parameters of radio links, including and network security indicators, is a classic direction in the development of secure routing methods. To ensure the routing of confidential multimedia traffic, you can use the concept of Secure Traffic Engineering. Here the more secure radio links can be loaded more intensively, while the vulnerable links utilized less intensively or completely blocked. For reactive information security, it is expedient to use means (protocols) of traffic policing and fast rerouting with the protection of routers, links, routes, and their bandwidth. The highest level of network security can be achieved through the integrated and complementary use of all the network protocols and mechanisms mentioned above.

Бурхливий розвиток безпроводових технологій, який спричинений підвищенням доступності та мобільності інфокомунікаційних сервісів, підвищує актуальність досліджень, пов'язаних із забезпеченням безпеки інформації. Все частіше саме виносить елементи безпроводових мереж є об'єктами впливів та вторгнень з боку зловмисників [1]. При цьому на рівні доступу метою мережних атак, як правило, є заволодіння конфіденційною інформацією користувачів безпроводової мережі. На рівні транспортної мережі ціллю зловмисників може слугувати її перевантаження та/або компрометація окремих мережних елементів (маршрутизаторів або радіоканалів) чи блокування певних сегментів. Тому сучасні інфокомунікаційні мережі, а особливо безпроводові мережі, мають використовувати різноманітні засоби забезпечення інформаційної безпеки на всіх рівнях еталонної моделі взаємодії відкритих систем.

Як показав проведений аналіз, особлива роль у забезпечення проактивного та реактивного захисту інформації відводиться саме технологічним засобам мережного рівня – механізмам фільтрації та профілювання трафіка, протоколам маршрутизації та резервування ресурсів [2, 3]. Основною задачею безпечної маршрутизації у безпроводових мережах є забезпечення пошуку (розрахунку) шляхів, використання яких орієнтували на підвищення рівня інформаційної (мережної) безпеки. При цьому має враховуватись топологія радіомережі, пропускні здатності радіоканалів та показники інформаційної безпеки мережних елементів – маршрутизаторів та радіоканалів. Класичним варіантом врахування перелічених структурно-функціональних параметрів безпроводової мережі є відповідне формування маршрутних метрик, за аналізом яких і будуються в подальшому оптимальні (найкоротші) шляхи. Однак на цьому етапі можуть виникнути певні труднощі щодо забезпечення зваженого впливу на маршрутну метрику показників інформаційної безпеки та, наприклад, пропускної здатності радіоканалів, їх завантаженості та надійності [4, 5]. Це особливо актуальним є при маршрутизації конфіденційного мультимедійного трафіка. Метричний підхід є прикладом реалізації проактивного підходу до забезпечення інформаційної безпеки засобами маршрутизації.

Ще одним прикладом проактивної безпечної маршрутизації є використання запропонованого у роботах [6, 7] рішення Secure Traffic Engineering (SecTE). Проте відміну від метричного підходу концепція SecTE забезпечує пошук безпечних шляхів з врахуванням їх пропускної здатності та завантаженості. При цьому вплив ймовірності компрометації радіоканалів на порогові значення

завантаженості радіоканалів може регулюватись виборов відповідної функції блокування каналів. Тобто більш безпечні радіоканали можуть завантажуватись більше, а ніж небезпечні канали. У граничному випадку небезпечні радіоканали можуть повністю блокуватись та не використовуватись у процесі визначення оптимальних маршрутів. До реактивних засобів забезпечення інформаційної безпеки у безпроводових мережах варто віднести протоколи відмовостійкої маршрутизації та швидкої перемаршрутизації, а також механізми профілювання трафіка. Основною метою протоколів відмовостійкої маршрутизації із захистом (резервуванням) шлюзу за замовчуванням – FHRP (First Hop Redundancy Protocols) – є забезпечення доступності мереж доступу до ресурсу транспортної мережі у випадку відмови приграничного маршрутизатора, який виконує функції шлюзу за замовчуванням. Саме протоколи HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), GLBP (Gateway Load Balancing Protocol) та CARP(Common Address Redundancy Protocol) здатні розв'язати цю задачу у випадку, наприклад, компрометації, перевантаження або виходу з ладу приграничного маршрутизатора [8-12].

На рівні транспортної мережі забезпечити локальний, глобальний та сегментний захист мережних елементів повинні протоколи швидкої перемаршрутизації – FRR (Fast ReRouting). Саме вони здатні дуже швидко, за десятки мілісекунд, відреагувати на відмови мережного обладнання та перемкнути трафік на попередньо розраховані резервні маршрути. Обладнання Cisco та Juniper підтримує реалізацію схем захисту маршрутизаторів, каналів, маршрутів та їх пропускної здатності [2, 12]. Рішення FRR ґрунтуються на введені ресурсної надлишковості, бо для потоків пакетів необхідно резервувати до використання не тільки основні, але й резервні маршрути. Тобто підвищення рівня відмовостійкості та безпеки може негативно вплинути на продуктивність безпроводової мережі.

З метою забезпечення керованості процесам боротьби з перевантаженням у безпроводовій мережі варто налаштувати механізми профілювання трафіку – Traffic Shaping/Policing (TSP). Їх фунціонал дозволяє обмежити навантаження, яке надходить до мережі. У роботах [6, 13-16] представлені рішення, в межах яких функції профілювання трафіку адаптовані під задачі підвищення відмовостійкості та кіберстійкості інфокомунікаційних мереж. При цьому трафік, який має високий пріоритет, обумовлений високими вимогами до рівня якості обслуговування та інформаційної безпеки, на границі мережі буде обмежуватись менш інтенсивно, а ніж потоки з нижчим пріоритетом.

Перспективним напрямком забезпечення високого рівня інформаційної безпеки засобами маршрутизації є реалізація моделей та методів, які базуються на використання шляхів, які не перетинаються [17-21]. Подібні рішення можна віднести як до засобів проактивного забезпечення інформаційної безпеки, так і до реактивних рішень. При використанні шляхів, які не перетинаються, значно ускладняється робота зловмисника щодо конмпрометації або перевантаження елементів безпроводової мережі. Зловмисник повинен розподілити свої зусилля та ресурси між множиною каналів, які входять до маршрутів, які не перетинаються. З іншого боку, використання шляхів, які не перетинаються, дозволяє без додаткових зусиль реалізувати різноманітні за надлишковістю схеми резервування шляхів при швидкій перемаршрутизації.

Література:

1. Chapman, C. (2016), Network Performance and Security (Testing and Analyzing Using Open Source and Low-Cost Tools), 1st edition, Syngress, 380 p.

2. Schudel, G., Smith, D. J. (2008), Router Security Strategies Securing IP Network Traffic Planes, Cisco Press, 673 p.

3. Edgar, T., Manz, D. (2017), Research Methods for Cyber Security, 1st edition. Syngress, 2017, 428 p.

4. Snihurov, A., Chakrian, V., Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters, Scholars Journal of Engineering and Technology, 2015, No. 3(8), P. 707-714.

5. Євдокименко, М. О., Шаповалова, А. С., Шаповал, М. М. Потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей, Проблеми телекомунікацій, 2020, No. 1(26), С. 48-62. Режим доступу: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.

6. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Lemeshko V. Network Security Approach Based on Traffic Engineering Fast ReRoute with support of Traffic Policing. Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021). Kyiv, Ukraine. CEUR, 2021. Vol. 2923. P. 81-90.

7. Lemeshko O., Yeremenko O. Linear Optimization Model of MPLS Traffic Engineering Fast ReRoute for Link, Node, and Bandwidth Protection // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018. – P. 1-5.

8. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість / О. В. Лемешко, О. С. Єременко, О. С. Невзорова. – Харків, 2020. – 307 с.

9. Єременко О.С., Мерсні А. Підвищення відмовостійкості елементів сучасних інфокомунікаційних мереж із застосуванням протоколів резервування шлюзу за замовчуванням. Проблеми телекомунікацій, 2020, No. 2(27), С. 68-81. Режим доступу: https://pt.nure.ua/wp-content/uploads/2021/11/202_mersni_FHRP.pdf.

10. Shahriar, F., Fan, J. Performance Analysis of FHRP in a VLAN Network with STP, 2020 IEEE 3rd International Conference on Electronics Technology (ICET), 2020, P. 814-818. DOI: https://doi.org/10.1109/ICET49382.2020.9119624.

11. Anwar, U., Teng, J., Umair, H. A., Sikander, A. Performance Analysis and Functionality Comparison of FHRP Protocols. 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), 2019P. 111-115. DOI: https://doi.org/10.1109/ICCSN.2019.8905333

12. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2, Cisco Press. 2019.

13. Lemeshko O., Yevdokymenko M., Yeremenko O., Shapovalova A. Investigation of Load-Balancing Fast ReRouting Model with Providing Fair Priority-Based Traffic Policing. In: Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, 2021, vol 1247. Springer, Cham. pp 108-119.

14. Lemeshko O., Yeremenko O., Hailan A.M., Yevdokymenko M., Shapovalova A. Policing Based Traffic Engineering Fast ReRoute in SD-WAN Architectures: Approach Development and Investigation. In: Al-Bakry A. et al. (eds) New Trends in Information and Communications Technology Applications. NTICT 2020. Communications in Computer and Information Science, 2020, vol 1183. Springer, Cham.

15. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Ilyashenko A., Sleiman B. Traffic Engineering Fast ReRoute Model with Support of Policing // IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)., July 2 – 6, 2019. – Lviv, Ukraine. – P. 842-845.

16. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Hailan A.M., Mersni A. Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing // The 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 18-21 September, 2019, Metz, France. – P. 117-122.

17. Лемешко О.В., Єременко О.С., Євдокименко М.О., Слейман Б. Модель розрахунку множини маршрутів, що не перетинаються, з максимальною пропускною здатністю в MANET // Збірник наукових праць четвертої міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС – 2019)». - Харків: ХНУРЕ, 2019. – С. 75-76.

18. Лемешко О.В., Грачов Ю.В., Слейман Б. Дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, які не перетинаються // Проблеми телекомунікацій. 2020. 2(27). С. 43-55. URL: https://pt.nure.ua/wp-content/uploads/2021/11/202_lemeshko_secure.pdf.

19. Lemeshko O., Yeremenko O., Sleiman B., Yevdokymenko M. Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN // Advances in Electrical and Electronic Engineering. 2020. Vol. 18, № 1. P. 23-30.

20. Lemeshko O., Romanyuk A., Kozlova H. Design schemes for MPLS Fast ReRoute // XIIth International Conference THE EXPERIENCE OF DESIGNING AND APPLICATION OF CAD SYSTEMS IN MICROELECTRONICS, Polyana-Svalyava-(Zakarpattya), UKRAINE 19-23 February 2013: Publishing House of Lviv Polytechnic, 2013. – P. 202-203.

21. Lemeshko O., Yeremenko O., Yevdokymenko M., Sleiman B., Segeč P., Papán J. Advanced Performance-Based Fast ReRouting Model with Path Protection. 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 23-28, DOI: 10.1109/DESSERT50317.2020.9125034.