ОГЛЯД ПРОТОКОЛІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В БЕЗПРОВОДОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

Євдокименко М.О., Шаповал М.М., Порохняк В.Ю.

Кафедра «Інфокомунікаційної інженерії»
ім. В.В. Поповського», ХНУРЕ, Україна

E-mail: marina.ievdokymenko@nure.ua,
maryna.shapoval@nure.ua,
volodymyr.porokhniak@nure.ua

Abstract

The paper provides an overview of existing secure routing protocols in wireless networks IEEE 802.11. Their benefits and disadvantages are presented. Based on the analysis, requirements were obtained for the development of promising routing solutions at the network level, which, with a high level of protection, will taking into account the features of structural and functional construction of wireless networks; the security parameters of both individual wireless elements and the network as a whole; the limited resources of wireless networks; the information security risks based on existing and identified vulnerabilities on the structural elements of the wireless network; and have acceptable computational complexity and scalability.

При побудові та експлуатації безпроводових мереж стандарту IEEE 802.11 однією з найгостріших проблем є забезпечення їхнього захисту. Це пов'язано з тим, що в безпроводових мережах, в порівнянні з проводовими, отримати доступ до інформації набагато простіше, так само як і вплинути на їх канал передачі даних. Тому актуальною є задача забезпечення захисту безпроводових мереж на всіх рівнях моделі OSI. Дана робота присвячена огляду методів захисту на мережному рівні, а саме існуючим протоколам безпечної маршрутизації в безпроводових мережах стандарту IEEE 802.11 та виявленню їх недоліків.

Протоколи безпечної маршрутизації можна розподілити на три групи [1-7]: проактивні, реактивні та гібридні протоколи маршрутизації. Відомим представником проактивного протоколу безпечної маршрутизації в безпроводових мережах є Secure Efficient Ad hoc Distance (SEAD) [1, 2], який відіграє важливу роль в мережі з обмеженою пропускною здатністю, використовуючи ефективні і недорогі криптографічні примітиви та односторонні хеш-ланцюги замість ретрансляції дорогих асиметричних криптографічних операцій. Недоліком SEAD є «чутливість» до атак типу «відмова в обслуговуванні» (Denial of Service, DoS). Наступним протоколом є проактивний протокол безпечної маршрутизації для мереж Ad Hoc – Ariadne [3]. Ariadne забезпечує автентифікацію точка-точка вздовж маршруту з використанням автентифікації і загального ключа між двома сторонами, стійкий для атак Rogue Access Point (RAP) та Wormhole. В якості недоліків цього протоколу виступає те, що його використання потребує великих обсягів пам'яті безпроводових пристроїв для зберігання розподілених загальних ключів та обчислення ланцюжка ключів, а також наявність Private Key Infrastructure (PKI) або Certification Authority (CA).

Одним з представників реактивного протоколу безпечної маршрутизації є Authenticated Routing for Ad hoc Networks (ARAN), що заснований на цифрових сертифікатах [4, 5]. Цей протокол забезпечує автентифікацію та цілісність повідомлень, що передаються. Перевагами ARAN є його стійкість до спуфінгу, модифікації повідомлень, фальсифікації та DoS атак. Недоліками даного протоколу є його ресурсомісткість внаслідок використання асиметричної криптографії та шифрування. Крім того, даний протокол не містить метрику для розрахунку оптимальних шляхів.

Прикладом гібридного протоколу безпечної маршрутизації виступає Secure Ad hoc On-demand Distance Vector (SAODV), що використовує цифрові підписи під час автентифікації та забезпеченні цілісності повідомлень, що передаються [6, 7]. При цьому високий рівень захисту, що досягається використанням цього протоколу вимагає безпроводове обладнання високої продуктивності.

Слід зазначити, що проведений аналіз існуючих протоколів безпечної маршрутизації показав, що для забезпечення захисту безпроводових мереж на мережному рівні потрібен перегляд та вдосконалення маршрутних рішень. Крім того, виявилась відсутність протоколів маршрутизації, які б враховували ризики інформаційної безпеки внаслідок використання вразливостей безпроводового обладнання. Отже, подальше вдосконалення протоколів і моделей безпечної маршрутизації для усунення недоліків наявних рішень має відповідати таким вимогам:

- урахування особливостей структурної та функціональної побудови безпроводових мереж;
- підтримка потокового характеру різноманітних типів трафіку;
- урахування параметрів безпеки як окремих безпроводових елементів, так і мережі загалом;
- прийнятна ресурсомісткість із врахуванням обмежених ресурсів безпроводових мережах;
- урахування ризиків інформаційної безпеки, що ґрунтуються на наявних і виявлених уразливостях на структурних елементах безпроводової мережі;
- прийнятна обчислювальна складність та масштабованість кінцевих рішень, які підлягатимуть подальшій протокольній реалізації.

Література:

1. Hu Y. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks / Y. Hu, D. Johnson, A. Perrig. // Elsevier. – 2003. – С. 175–192.

2. A Secure Protocol for Ad hoc Networks [Електронний ресурс] / [B. Hahill, B. Dahill, K. Sanzgiri та ін.] // 0th IEEE International Conference on Network Protocols. – 2002. – Режим доступу до ресурсу: https://doi.org/10.1007/978-3-540-39867-7_69.

3. Hu Y. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks [Електронний ресурс] / Y. Hu, D. Johnson, A. Perrig // Elsevier. – 2005. – Режим доступу до ресурсу: https://doi.org/10.1007/s11276-004-4744-y.

4. Dahill B. ARAN: A Secure Routing Protocol for Ad Hoc Networks / B.Dahill, B. Levine, C. Shields, E. Royer. // Umass Tech Report. – 2002. – №2. – С. 32

5. Pearlman M. Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks / M. Pearlman, Z. Haas, P. Samar. // IEEE/ACM Transactions on Networking (TON). – 2004. – №12. – С. 596–608.

6. Mulert J. Security Threats and Solutions in MANETs: A case study using AODV and SAODV / J. V Mulert. // Journal of Network and Computer Application. – 2012. – №35. – С. 1249–1259.

7. Kuzminykh I. Investigation of the IoT device lifetime with secure data transmission. / I. Kuzminykh; A. Carlsson; M. Yevdokymenko, V. Sokolov // In Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2019, ruSMART 2019; Galinina, O.; Andreev, S.; Balandin, S.; Koucheryavy, Y.. Eds.; LNCS, Volume 11660, Springer, Cham.