

УДК 621.391

Вдосконалення способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами

Єременко О.С., докторант, oleksandra.yeremenko@nure.ua,
Добришкін В.Ю., студент, avlem@ukr.net

Харківський національний університет радіоелектроніки, м. Харків

Як показав проведений аналіз, однією з найважливіших задач, яка регламентується стандартами побудови мереж наступного покоління NGN, є завдання реалізації функцій інформаційної безпеки. Відповідно до вимог стандартів Міжнародного Союзу Електрозв'язку (МСЕ) забезпечення інформаційної безпеки здійснюється в рамках трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки додатків [1]. При цьому ефективність роботи верхніх двох рівнів цілком і повністю визначається ефективністю функціонування засобів рівня безпеки інфраструктури, основними завданнями якого є: забезпечення безпеки на рівні мережевих елементів (комутаторів, маршрутизаторів, серверів), каналів зв'язку і маршрутів, які вони складають, в цілому.

Як правило, рівень безпеки мережевих елементів оцінюється за допомогою такого важливого показника як ймовірність компрометації, де під компрометацією розуміється факт несанкціонованого доступу до захищеної інформації, а також підозра здійснення такого доступу. Серед існуючих методів забезпечення заданого рівня безпеки можна виділити захищену передачу повідомлення, розділеного на фрагменти і переданого від відправника отримувачу за допомогою багатошляхової маршрутизації з балансуванням числа фрагментів за шляхами, які не перетинаються. У цьому випадку в ході багатошляхової маршрутизації і балансуванні числа фрагментів повідомлення за шляхами необхідно забезпечити заданий рівень мережевої безпеки, представленої ймовірністю компрометації переданого повідомлення P_{msg} :

$$P_{msg} \leq \gamma_P, \quad (1)$$

де γ_P – допустима ймовірність компрометації повідомлення в мережі. На сьогодні відомі тільки методики оцінки ймовірності компрометації для випадку використання шляхів, що не перетинаються, тобто для шляхів, в яких загальними є тільки вузли відправник та отримувач [2, 3].

В разі використання відомих аналітичних виразів для розрахунку ймовірності компрометації повідомлення, яке передається частинами за множиною шляхів, що не перетинаються, передбачаються такі вихідні дані:

S_{msg} і D_{msg} – вузли відправник та отримувач повідомлення, що передається;

M – кількість використовуваних шляхів, що не перетинаються, при маршрутизації частин повідомлення;

p_i^j – ймовірність компрометації j -го елемента (вузла, каналу) i -го шляху;

M_i – число елементів в i -м шляху, які можуть бути скомпрометовані.

В ході подальших міркувань вважається, що відправник та отримувач безпечні, тобто ймовірності компрометації вузла-відправника та вузла-отримувача дорівнюють нулю. Крім того, як і в роботах [2-4], вважається, що якщо елемент (вузол, канал) шляху скомпрометований, то всі фрагменти, що передаються через цей елемент, також будуть скомпрометовані. Тоді ймовірність компрометації i -го шляху, що складається з M_i елементів, можна розрахувати за допомогою виразу

$$p_i = 1 - (1 - p_i^1)(1 - p_i^2) \dots (1 - p_i^{M_i}) = 1 - \prod_{j=1}^{M_i} (1 - p_i^j). \quad (2)$$

Однією з основних умов, яка в обов'язковому порядку повинна виконуватися в ході безпечної маршрутизації, є те, що ймовірність компрометації повідомлення при його передачі по мережі не повинна перевищувати заданого допустимого значення (1). Тоді, наприклад, ймовірність компрометації повідомлення, розділеного на N частин відповідно до схеми Шаміра (N, N) і переданого за M шляхами, визначається виразом [2,4]

$$P_{msg} = \prod_{i=1}^M p_i. \quad (3)$$

В свою чергу використання шляхів, які не перетинаються, призводить до неефективного використання мережних ресурсів і зниження якості обслуговування, перш за все за показниками продуктивності.

Таким чином, пропонується вдосконалення існуючого способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами, причому необхідно вирішити наступне:

1. Розрахунок множини маршрутів між заданими вузлами відправник та отримувач. У роботі [5] з метою підвищення продуктивності телекомунікаційної мережі при багатошляховій безпечній маршрутизації запропоновано задіяти в тому числі і маршрути, що перетинаються за каналами та/або вузлами. При цьому представлена методика розрахунку ймовірності компрометації повідомлення при використанні маршрутів, які перетинаються, з послідовно-паралельною та комбінованою структурою. На ряді числових прикладів проведений аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих елементів (каналів зв'язку) і фрагментів мережі, а також доведено доцільність її використання. В якості методу визначення множини маршрутів, що перетинаються за вузлами, можливе використання моделі, представленій в [6].

2. Фрагментація повідомлення, що передається, відповідно до обраної схеми Шаміра.

3. Розподілення числа фрагментів повідомлення, що передається, між множиною маршрутів, визначених у ході вирішення першого завдання.

Отже запропоноване вдосконалення способу безпечної багатошляхової маршрутизації повідомлення з балансуванням числа його фрагментів за маршрутами розширює застосування існуючих способів з метою підвищення продуктивності телекомунікаційної мережі за рахунок використання маршрутів, що перетинаються за каналами та/або вузлами.

Список літератури

1. ITU-T X-805. Security architecture for systems providing end-to-end communications, 2003.
2. Lou W. SPREAD: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Zhang, Y. Fang // Wireless Networks. – 2009. – Vol. 15, Issue 3. – PP. 279–294.
3. Alouneh S. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing / 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.
4. Yeremenko O.S. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET / O.S. Yeremenko, Ali S. Ali // Radioelectronics and Informatics. – 2015. – № 1 (68). – С. 26–29.
5. Еременко А.С. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной или комбинированной структурой / А.С. Еременко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №6(40) – С. 64-71.
6. Yeremenko O.S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths / O.S. Yeremenko // Second International IEEE Conference Problems of Infocommunications. Science and Technology (PICS&T-2015). Proceedings. – Kharkiv: Kharkiv National University of Radio Electronics. Ukraine, Kharkiv, October 13–15, 2015. – PP. 42-45.