МЕТОД БЕЗПЕЧНОЇ ШВИДКОЇ ПЕРЕМАРШРУТИЗАЦІЇ ПОВІДОМЛЕНЬ ЗА КОМПОЗИТНИМИ ШЛЯХАМИ

Єременко О.С., Лемешко О.В., Персіков А.В.
Кафедра інфокомунікаційної інженерії, Харківський національний університет радіоелектроніки, Харків, Україна, E-mail: oleksandra.yeremenko.ua@ieee.org, oleksandr.lemeshko@nure.ua, persikovanatoliy@gmail.com

Анотація – Синтезовано метод безпечної швидкої перемаршрутизації повідомлень в мережі, що відноситься до класу проактивних і реактивних рішень щодо забезпечення заданого рівня інформаційної безпеки. Новизна методу полягає в тому, що в разі порушення вимог інформаційної безпеки в мережі, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, що входять в основний мультишлях, багатошляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації буде здійснюватися вже за заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху в цілому, або одного чи декількох заданих композитних шляхів, що входять в цей основний мультишлях.

Ключові слова – маршрутизація, компрометація, шлях, відмовостійкість, безпека.

I. Вступ

З метою розширення функціональних можливостей засобів безпечної маршрутизації, важливо щоб запропонований метод реалізував принципи не тільки проактивного, але і реактивного підходу. Іншими словами, в структурі методу безпечної маршрутизації важливо передбачити процедури оперативної реакції на можливі порушення рівня інформаційної безпеки [1-3]. В даний час протоколи маршрутизації реагують на можливі зміни стану мережі в масштабі часу десятків секунд, що не завжди є прийнятним як з точки зору необхідного рівня якості обслуговування, так й інформаційної безпеки [1].

У зв'язку з цим все частіше на практиці застосовуються методи та протоколи швидкої перемаршрутизації, в ході яких попередньо розраховуються два типи шляхів: основний і резервний. При цьому використання окремо кожного типу шляхів повинно приводити до задоволення вимог щодо рівня інформаційної безпеки. Тоді при відмові основного шляху дані, що передаються, практично миттєво (із затримкою в десятки мілісекунд) будуть маршрутизуватися з використанням резервних маршрутів. Очевидно, що основний і резервний маршрути не повинні перетинатися з елементами мережі, які відмовили (маршрутизаторами, каналами зв'язку або маршрутами в цілому) [4, 5]. При цьому причинами відмов в обслуговуванні можуть виступати як перевантаження і поломка мережного обладнання, так і наслідки мережних атак і впливу шкідливого програмного забезпечення (вірусів).

II. Метод безпечної швидкої перемаршрутизації повідомлень за композитними шляхами: проактивний і реактивний підходи

Тоді в рамках безпечної швидкої перемаршрутизації (Secure Fast ReRouting, S-FRR) використання множини основних шляхів відноситься до рішень проактивного підходу щодо забезпечення заданого рівня інформаційної безпеки, а застосування резервних шляхів відповідає вимогам реактивного підходу. При цьому в рамках запропонованого методу розрахунок множини основних і резервних шляхів повинен здійснюватися максимально злагоджено для підвищення ефективності кінцевих рішень.

Поділ шляхів на основні та резервні має на увазі, що частини повідомлення будуть передаватися не за всіма доступними композитними та простими шляхами, а лише за їх обмеженою кількістю при виконанні вимог по ймовірності компрометації $P_{msg} \le \gamma_P$, де P_{msg} – ймовірність компрометації повідомлення в цілому при його передачі частинами по мережі, а γ_P – допустима ймовірність компрометації повідомлення в мережі [3]. В даному контексті простий шлях завжди утворений послідовним з'єднанням каналів зв'язку. У свою чергу, композитні шляхи являють собою більш складні структурні форми, що включають в себе перетин простих шляхів.

З огляду на те, що для підвищення рівня інформаційної безпеки повідомлень, що передаються, необхідно реалізувати багатошляхову маршрутизацію їх частин, то в якості основного та резервного будуть виступати не окремі композитні або прості шляхи, а утворені ними мультишляхи. При цьому до складу як основного, так і резервного мультишляху можуть входити кілька композитних та (або) простих шляхів.

В ході розрахунку резервного мультишляху пропонується реалізувати наступні дві схеми:

– схему захисту основного мультишляху в цілому, при якій основний і резервний мультишляхи не перетинаються ні за вузлами, ні за каналами зв'язку;
– схему захисту окремого шляху (композитного або простого) основного мультишляху, при якій резервний мультишлях не повинен містити шлях, який захищається, основного мультишляху.

Реалізація кожної зі схем захисту націлена на відновлення заданого рівня інформаційної безпеки за рахунок відмови від основного мультишляху та переходу до використання резервного. У зв'язку з цим уточнимо введені в [3] та введемо додаткові позначення (табл. 1).

ТАБЛИЦЯ 1

УМОВНІ ПОЗНАЧЕННЯ

$\widetilde{p}_i^{pr}$	ймовірність компрометації i-го композитного або простого шляху основного мультишляху ($i = \overline{1, \widetilde{M}}$)
$\widetilde{p}_i^{b}$	ймовірність компрометації i-го композитного або простого шляху резервного мультишляху ($i = \overline{1, \widetilde{M}}$)
$\widetilde{P}_{msg}^{pr}$	ймовірність компрометації повідомлення в цілому при його передачі частинами за композитними або простими шляхами основного мультишляху
$\widetilde{P}_{msg}^{b}$	ймовірність компрометації повідомлення в цілому при його передачі частинами за композитними або простими шляхами резервного мультишляху
n_i	цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним або простим шляхом, що входить до складу основного мультишляху ($i = \overline{1, \widetilde{M}}$)
$\overline{n}_i$	цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним або простим шляхом, що входить до складу резервного мультишляху ($i = \overline{1, \widetilde{M}}$)

Відповідно до введених позначень для розрахунку ймовірності компрометації повідомлення, яке передається частинами за множиною композитних шляхів, необхідно використовувати наступні вирази

$$\widetilde{P}_{msg}^{pr} = \prod_{i=1}^{\widetilde{M}} \widetilde{p}_i^{pr} \text{ і } \widetilde{P}_{msg}^{b} = \prod_{i=1}^{\widetilde{M}} \widetilde{p}_i^{b} . \quad (1)$$

Варто відзначити, що ймовірності компрометації мережних фрагментів $\widetilde{p}_i^{pr}$ і $\widetilde{p}_i^{b}$ є функціями від кількості частин повідомлення, що передаються в них, тобто від n_i і $\overline{n}_i$. Тоді мають місце умови

$$\widetilde{p}_i^{pr} = \begin{cases} 1 - \prod_{j=1}^{\widetilde{M}_i} (1 - \widetilde{p}_i^{j}), n_i > 0; \\ 1, n_i = 0, \end{cases} \text{ і}$$

$$\widetilde{p}_i^{b} = \begin{cases} 1 - \prod_{j=1}^{\widetilde{M}_i} (1 - \widetilde{p}_i^{j}), \overline{n}_i > 0; \\ 1, \overline{n}_i = 0. \end{cases} \quad (2)$$

Системи (2) можуть бути записані як:

$$\widetilde{p}_i^{pr} = 1 - H_0(n_i) \prod_{j=1}^{\widetilde{M}_i} (1 - \widetilde{p}_i^{j}) \text{ і}$$

$$\widetilde{p}_i^{b} = 1 - H_0(\overline{n}_i) \prod_{j=1}^{\widetilde{M}_i} (1 - \widetilde{p}_i^{j}) , \quad (3)$$

де H_0 – функція Хевісайда, яка з урахуванням виразу 2(2.20) розраховується наступним чином

$$H_0(n) = \begin{cases} 0, n = 0; \\ 1, n > 0. \end{cases}$$

З огляду на реалізацію S-FRR також мають виконуватися умови

$$\sum_{i=1}^{\widetilde{M}} n_i = N \text{ і } \sum_{i=1}^{\widetilde{M}} \overline{n}_i = N . \quad (4)$$

В свою чергу, для захисту основного мультишляху, за аналогією з [4, 5], необхідно забезпечити виконання наступної умови:

$$\sum_{i=1}^{\widetilde{M}} n_i \overline{n}_i = 0 . \quad (5)$$

При необхідності захисту окремого *i*-го композитного шляху важливо забезпечити виконання умови

$$n_i \overline{n}_i = 0 , \quad (6)$$

яка також є нелінійною (білінійною).

Для того, щоб при використанні і основного, і резервного мультишляху виконувалися вимоги щодо ймовірності компрометації повідомлення, яке за ними передається, вводяться умови:

$$P_{msg}^{pr} \le \gamma_P \text{ і } P_{msg}^{b} \le \gamma_P . \quad (7)$$

Тоді в основу розроблюваного методу S-FRR може бути покладено рішення оптимізаційної задачі нелінійного цілочисельного програмування (Nonlinear Integer Programming) з критерієм оптимальності

$$J = \sum_{i=1}^{\widetilde{M}} \widetilde{p}_i n_i + \sum_{i=1}^{\widetilde{M}} \widetilde{p}_i \overline{n}_i , \quad (8)$$

і обмеженнями, представленими умовами, введеними в [3], та доповненими умовами (4), (5), (6) та (7). При цьому обмеження (5)-(7) є нелінійними, а змінні, що розраховуються, n_i і $\overline{n}_i$ носять цілочисельний характер. У критерії (8) значення $\widetilde{p}_i$ є вартісними ваговими коефіцієнтами. Цим забезпечується безпечна маршрутизація по мережі, коли максимальна кількість частин повідомлення буде передаватися за шляхом з мінімальною ймовірністю компрометації. Навпаки, за шляхом з найвищою ймовірністю компрометації передаватиметься мінімальна кількість частин повідомлення або не буде передано жодної.

III. Висновки

Синтезовано метод безпечної швидкої перемаршрутизації повідомлень в мережі, що відноситься до класу проактивних і реактивних рішень щодо забезпечення заданого рівня інформаційної безпеки. Новизна методу полягає в тому, що в разі порушення вимог інформаційної безпеки в мережі, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, що входять в основний мультишлях, багатошляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації буде здійснюватися вже за заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху в цілому, або одного чи декількох заздалегідь заданих композитних шляхів, що входять в цей основний мультишлях.

IV. Список літератури

[1] Stallings, W. Cryptography and Network Security: Principles and Practice, 7th Edition [Text] / W. Stallings. – Pearson, 2016. – 768 p.

[2] Lou, W. SPREAD: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks [Text] / W. Lou, W. Liu, Y. Zhang, Y. Fang // Wireless Networks. – 2009. – Vol. 15, Issue. 3. – P. 279-294.

[3] 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.

[4] Lemeshko, O.V. Fault-Tolerance Improvement for Core and Edge of IP Network [Text] / O.V. Lemeshko, O.S. Yeremenko, N. Tariki, A.M. Hailan // 2016 XIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), 2016. – P. 161-164.

[5] Lemeshko, O. Hierarchical Method of Inter-Area Fast Rerouting [Text] / O. Lemeshko, O. Yeremenko, O. Nevzorova // Transport and Telecommunication Journal. – 2017. – Vol. 18, Issue 2. – P. 155-167.

METHOD OF SECURE FAST REROUTING OF MESSAGES OVER COMPOSITE PATHS

Yeremenko O.S., Lemeshko A.V., Persikov A.V.

Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Abstract – The method of secure Fast ReRouting of messages on the network, which belongs to the class of proactive and reactive solutions to provide a given level of information security, is synthesized. The novelty of the method is that in the event of violations of the requirements of information security in the network, caused by increased probability of compromising one or a number of composite paths included in the primary multipath, transmission of parts of the confidential message over multipath with the provision of specified values of the probability of its compromise will be carried out already over a set of precomputed backup composite paths, implementing the protection of either the primary multipath as a whole or one or more precomputed composite paths included in this primary multipath. The proposed method can become the basis of mathematical and algorithmic support in the development of perspective protocols for secure and fault-tolerant routing in infocommunication networks. The use of the proposed solution is oriented, firstly, to increase the reliability of routing solutions in case of failure of the network elements; and secondly, to reduce the probability of compromising messages transmitted in network.