УДК 621.391

ДОСЛІДЖЕННЯ МЕТОДУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ КОНФІДЕНЦІЙНИХ ПОВІДОМЛЕНЬ ЗА ШЛЯХАМИ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ

О.В. Лемешко
Харківський національний університет радіоелектроніки

Ю.В. Грачов
ТОВ "ЕПАМ СИСТЕМЗ" Україна

Б. Слейман
Харківський національний університет радіоелектроніки

Abstract *– The article proposes a secure routing method of confidential messages in a telecommunication network by disjoint paths and its research results. The presented method of disjoint paths secure routing of confidential messages is based on the sequential solution of two optimization problems: calculating disjoint routes and secure balancing of confidential message fragments on a set of precalculated paths. An optimization model was chosen to determine the set of routes, namely, to calculate the maximum number of disjoint paths, including communication links with minimum compromise probability. Additionally, a model of fragmented transmission using a precalculated set of disjoint paths was selected according to the SPREAD mechanism and Shamir's scheme to ensure the minimum possible probability of message compromise. The study of the proposed secure routing method on the selected network configuration for three different variants of the link compromise probabilities has been conducted. The study results confirmed the effectiveness of the proposed secure routing method and the efficiency of the underlying optimization models to determine both the set of disjoint paths and the order of secure balancing of confidential message fragments. Prospects for further research in the field of secure routing in telecommunication networks are related to considering the link compromise probabilities and other essential indicators of network security.*

Анотація *– У статті запропоновано метод безпечної маршрутизації конфіденційних повідомлень у телекомунікаційній мережі за шляхами, що не перетинаються, та результати його дослідження. В основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв'язання двох оптимізаційних задач: розрахунку маршрутів, що не перетинаються, та безпечного балансування фрагментів конфіденційного повідомлення за множиною попередньо розрахованих шляхів. Для визначення множини шляхів обрано модель розрахунку максимальної кількості шляхів, що не перетинаються, з включенням у них каналів зв'язку, які мають мінімальну ймовірність компрометації. Для забезпечення мінімально можливої ймовірності компрометації повідомлень обрано модель їх фрагментованої передачі за попередньо розрахованою множиною шляхів, що не перетинались, відповідно до механізму SPREAD та схеми Шаміра. Проведено дослідження запропонованого методу безпечної маршрутизації на обраній мережній конфігурації для трьох різних варіантів імовірностей компрометації каналів зв'язку мережі. Результати дослідження підтвердили ефективність запропонованого методу безпечної маршрутизації та працездатність закладених в його основу оптимізаційних моделей щодо визначення як множини шляхів, що не перетинались, так і порядку безпечного балансування за ними фрагментів конфіденційного повідомлення. Перспективи подальших досліджень в області безпечної маршрутизації в телекомунікаційній мережі пов'язані з урахуванням не тільки ймовірності компрометації каналів зв'язку, але й інших важливих показників мережної безпеки.*

Вступ

Як показав проведений аналіз [1-5], проблема забезпечення мережної безпеки на сучасному етапі розвитку інформаційного суспільства є дуже актуальною. Саме різнотипні та взаємодоповнюючі організаційні, соціальні, технічні (апаратні та програмні) заходи та засоби повинні забезпечити належний рівень безпеки інформації, яка

передається в сучасних телекомунікаційних мережах (ТКМ). Перелік таких засобів невпинно розширюється, а ефективність їх використання постійно зростає, але й методи та стратегії виявлення та використання вразливостей мережного обладнання також безперервно вдосконалюються.

Досить дієвим засобом забезпечення мережної безпеки в ТКМ є протоколи маршрутизації [6-10]. Саме вони повинні забезпечити проактивний і реактивний захист телекомунікаційної мережі на основі збору та аналізу інформації про її стан. Водночас протоколи безпечної маршрутизації, крім звичних даних про стан мережі (її топологію, пропускні здатності, завантаженість та надійність каналів зв'язку), мають прогнозувати та оцінювати значення ключових показників безпеки комутаційного та серверного обладнання ТКМ, рівень їх уразливості та ймовірність компрометації. З цією метою математичне та алгоритмічне забезпечення протоколів маршрутизації ТКМ має бути вдосконалене та розширене під нові умови та завдання, пов'язані із забезпеченням заданого рівня мережної безпеки, оскільки більшість існуючих маршрутних протоколів у кращому випадку орієнтовані на покращення показників якості обслуговування (Quality of Service, QoS).

Ґрунтуючись на результатах, отриманих у роботах [11-20], у даній статті пропонується метод безпечної маршрутизації конфіденційних повідомлень, які для зниження ймовірності їх компрометації мають передаватись за шляхами, що не перетинаються та включають в себе найбільш безпечні канали зв'язку. Фактично метод є подальшим узагальненням рішень, що охоплюють оптимізаційні моделі маршрутизації, які запропоновані у роботах [15-20] та доповнюють одне одну.

I. Математична модель розрахунку маршрутів, що не перетинаються, в телекомунікаційній мережі

Для опису математичної моделі розрахунку шляхів, запропонованої у роботах [15-18], будуть використані наступні позначення:

- $G = (R, E)$ – граф, що описує структуру ТКМ;
- $R = \left\{ R_i ; i = \overline{1, m} \right\}$ – множина вершин графа G, що представляють маршрутизатори мережі;
- $E = \left\{ E_{i,j} ; i, j = \overline{1, m}; i \neq j \right\}$ – множина дуг графа G, що описують канали зв'язку ТКМ;
- $\varphi_{i,j}$ – пропускна здатність каналу $E_{i,j} \in E$, що вимірюється в пакетах за секунду (1/с);
- K – множина конфіденційних повідомлень, що передаються в мережі;
- s_k – вузол-відправник (джерело) k-го повідомлення ($k \in K$);
- d_k – вузол-отримувач k-го повідомлення.

У процесі розв'язання задачі щодо розрахунку маршрутів, що не перетинаються, необхідно розрахувати множину маршрутних змінних $a_{i,j}^k$, кожна з яких визначає належність каналу $E_{i,j} \in E$ до множини обчислених шляхів, при передачі фрагментів k-го повідомлення. Позначимо через M^k цілочисельний параметр, що характеризуватиме кількість використаних фрагментами k-го повідомлення шляхів, що не перетинаються.

Відповідно до фізичної суті поставленої задачі на маршрутні змінні $a_{i,j}^k$ накладається система обмежень. По-перше, актуальними є такі умови

$$a_{i,j}^k \in \{0;1\}. \tag{1}$$

Для вузлів відправника та отримувача k-го повідомлення мають виконуватися наступні умови [15-18]:

$$\sum_{j:E_{i,j}\in E} a_{i,j}^k = \mathrm{M}^k;\ k \in K,\ \ R_i = s_k; \tag{2}$$

$$\sum_{j:E_{j,i}\in E} a_{j,i}^k = \mathrm{M}^k;\ k \in K,\ R_i = d_k. \tag{3}$$

При забезпеченні виконання умов (2) та (3) гарантується, що кількість шляхів, які виходять з вузла-відправника, співпадає з числом шляхів, які входять у вузол-отримувач k-го повідомлення. У процесі використання транзитних вузлів ТКМ ($R_i \neq s_k, d_k$) на маршрутні змінні накладаються такі обмеження [15-18]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k \le 1, \quad k \in K; \\ \sum\limits_{j:E_{j,i}\in E} a_{j,i}^k \le 1, \quad k \in K; \\ \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} a_{j,i}^k = 0, \quad k \in K. \end{cases} \tag{4}$$

Перша і друга умови в (4) відповідають за те, щоб через транзитний вузол R_i проходило не більше одного шляху. Виконання третьої умови в (4) гарантує, що з транзитного вузла R_i може виходити шлях лише у тому випадку, якщо він у цей вузол заходить. Виконання умов (1)-(4) відповідно до результатів дослідження, представлених у роботах [15-18], має забезпечити розрахунок шляхів у ТКМ, що не перетинаються, тобто спільними в них будуть лише вузли відправник (s_k) та отримувач (d_k).

На цілочисельний параметр M^k накладаються обмеження виду

$$\mathrm{M}^k \geq 1. \tag{5}$$

Для врахування параметрів мережної безпеки у процесі розрахунку множини шляхів, що не перетинаються в ТКМ, у роботах [15-18] запропоновано до використання критерій оптимальності, що забезпечує максимум наступної цільової функції:

$$J_1 = w_k \mathrm{M}^k - \sum_{E_{i,j} \in E} w_{i,j} a_{i,j}^k, \tag{6}$$

де w_k та $w_{i,j}$ – додатні вагові коефіцієнти, які визначають важливість відповідних доданків у (6). Коефіцієнти $w_{i,j}$ визначають маршрутні метрики каналів зв'язку мережі $E_{i,j} \in E$, які будуть пов'язані з імовірністю їх компрометації [15]

$$w_{i,j} = -\log_{10}(1 - p_{i,j}), \tag{7}$$

де $p_{i,j}$ – імовірність компрометації каналу зв'язку $E_{i,j} \in E$.

Для того, щоб першочергово забезпечувалась максимізація кількості шляхів, які не перетинаються, у цільовій функції (6) вибір вагових коефіцієнтів треба здійснювати згідно умови

$$w_k >> w_{i,j}, \tag{8}$$

У цьому разі другий доданок у (6) буде впливати на включення в розраховану множину шляхів найбільш безпечних каналів.

Таким чином, задача щодо розрахунку шляхів, що не перетинаються, була сформульована в оптимізаційній формі. Критерієм оптимальності виступає максимум цільової функції (6), а на керуючі змінні $a_{i,j}^k$ та M^k накладаються обмеження (1)-(5). Оптимізаційна задача (1)-(6) відноситься до класу задач цілочисельного лінійного програмування (Integer Linear Programming, ILP).

II. Математична модель безпечного балансування фрагментів конфіденційного повідомлення у телекомунікаційній мережі

У роботах [19, 20] представлено рішення щодо розробки та вдосконалення механізму SPREAD (Secure Protocol for Reliable dAta Delivery), що відноситься до засобів безпечної маршрутизації. В основу SPREAD покладено принцип порогового розділення конфіденційного повідомлення (КП) відповідно до обраної схеми Шаміра на окремі фрагменти (частини), які в подальшому передаються в ТКМ до отримувача за множиною шляхів, що не перетинаються. Крім того, у роботах [21-25] запропоновано вдосконалену модель механізму SPREAD, в межах якої допускається певний характер перетину шляхів у ТКМ, що супроводжується покращенням показників мережної безпеки при передачі КП. Закон (схема) розділення

повідомлення на фрагменти в загальному випадку може бути відомим зловмиснику, але скомпрометувати конфіденційне повідомлення він зможе лише тоді, коли скомпрометує всі використані для доставки шляхи. Тому рівень мережної безпеки у цьому випадку цілком залежить від кількості та безпечності шляхів, що використовуються для доставки фрагментів КП.

З метою пояснення принципу роботи механізму SPREAD будуть використані такі позначення:

- M_i^k – кількість каналів зв'язку в i-му шляху, що можуть бути скомпрометовані ($i=\overline{1,M^k}$);
- p_i^j – імовірність компрометації j-го каналу зв'язку i-го шляху ($i=\overline{1,M^k}$, $j=\overline{1,M_i^k}$);
- $\left(T,N\right)$ – параметри схеми Шаміра, де N – загальна кількість фрагментів, на які розділяється повідомлення, що передається, унаслідок застосування схеми Шаміра; T – мінімальна кількість фрагментів, за якими можливо відновити повідомлення, що передається $\left(T\le N\right)$;
- p_i – імовірність компрометації i-го шляху ($i=\overline{1,M^k}$);
- P_{msg}^k – імовірність компрометації повідомлення загалом за умови його фрагментованої передачі мережею;
- n_i^k – цілочисельна змінна, яка характеризує кількість фрагментів k-го КП, що передаються за i-м шляхом $i=\overline{1,M^k}$.

Тоді ймовірність компрометації i-го шляху, що складається з M_i^k елементів, можна розрахувати таким чином

$$p_i=1-\left(1-p_i^1\right)\left(1-p_i^2\right)\ldots\left(1-p_i^{M_i}\right)=1-\prod_{j=1}^{M_i^k}\left(1-p_i^j\right). \tag{9}$$

Для керуючих змінних n_i^k ($i=\overline{1,M^k}$) має виконуватися така умова [19, 20]:

$$\sum_{i=1}^{M^k} n_i^k = N. \tag{10}$$

У випадку реалізації схеми Шаміра з параметрами $T<N$ мають виконуватися умови [19, 20]

$$N-n_i^k<T,\ (i=\overline{1,M^k}). \tag{11}$$

Якщо ж використовується схема без надмірності, тобто $T=N$, мають місце такі умови [19, 20]:

$$1 \le n_i^k \le T-1,\ (i=\overline{1,M^k}). \tag{12}$$

Імовірність компрометації k-го конфіденційного повідомлення, розділеного відповідно до схеми Шаміра на N фрагментів з подальшим використанням M^k шляхів, визначається згідно з виразом [19, 20]

$$P_{msg} = \prod_{i=1}^{M^k} p_i\ . \tag{13}$$

Фактично вираз (13) визначає ймовірність компрометації всіх M^k шляхів, що не перетинаються та використовуються для передачі фрагментів k-го конфіденційного повідомлення.

Задачу безпечного балансування фрагментів конфіденційного повідомлення за множиною попередньо розрахованих, наприклад, за допомогою моделі (1)-(8), шляхів можна також представити в оптимізаційній формі. Критерієм оптимальності може виступати мінімум цільової функції [21-25]

$$J = \sum_{i=1}^{M} p_i n_i\ . \tag{14}$$

Таким чином, в основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв'язання двох задач:

- розрахунку маршрутів, що не перетинаються, в телекомунікаційній мережі за допомогою моделі (1)-(8);
- безпечного балансування фрагментів конфіденційного повідомлення (9)-(14) за множиною попередньо розрахованих шляхів (1)-(8).

III. Результати дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються

Дослідження процесу безпечної маршрутизації конфіденційних повідомлень, організованого за допомогою запропонованого методу, буде продемонстровано на прикладі ТКМ, структура якої представлена на рис. 1.

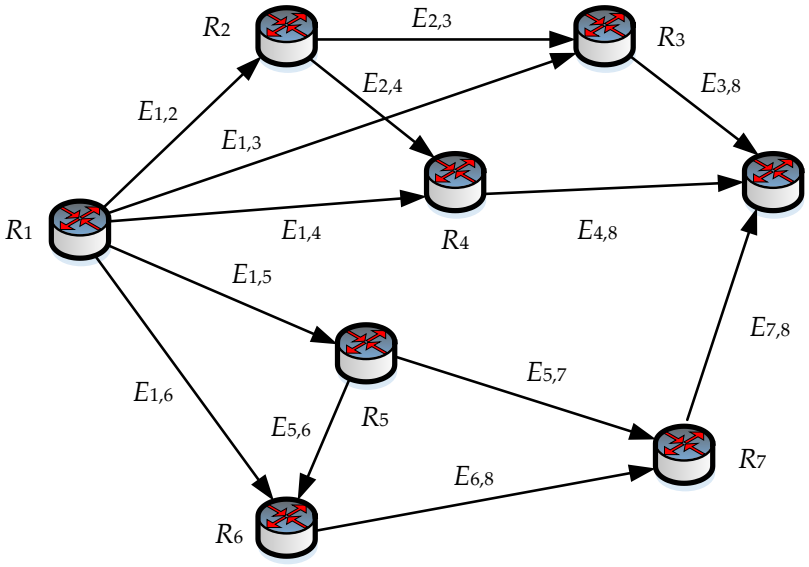

Рис. 1. Структура телекомунікаційної мережі

До складу мережі входить вісім маршрутизаторів і тринадцять каналів зв'язку. Нехай конфіденційне повідомлення треба передати між маршрутизаторами R_1 і R_8. В процесі дослідження розглядалось три варіанти ймовірностей компрометації каналів зв'язку ТКМ (табл. 1).

Таблиця 1. Варіанти ймовірностей компрометації каналів зв'язку ТКМ

Номер варіанту компрометації каналів ТКМ	$E_{1,2}$	$E_{1,3}$	$E_{1,4}$	$E_{1,5}$	$E_{1,6}$	$E_{2,3}$	$E_{2,4}$	$E_{3,8}$	$E_{4,8}$	$E_{5,6}$	$E_{5,7}$	$E_{6,7}$	$E_{7,8}$
1	0,1	0,8	0,3	0,4	0,8	0,2	0,5	0,6	0,5	0,4	0,3	0,9	0,2
2	0,9	0,6	0,1	0,2	0,8	0,3	0,1	0,3	0,7	0,4	0,9	0,2	0,1
3	0,1	0,1	0,9	0,9	0,6	0,1	0,3	0,8	0,4	0,6	0,2	0,1	0,1

Тоді в табл. 2 зазначені всі можливі маршрути ($L_1 \div L_7$) між маршрутизаторами R_1 та R_8, які виступали відправником та отримувачем КП. В цій же таблиці вказані ймовірності компрометації шляхів $L_1 \div L_7$, які розраховані відповідно до виразу (9).

В табл. 3 наведено ймовірності компрометації мультишляхів $LL_1 \div LL_7$, що складались з множини шляхів, які не перетинались. Фактично в табл. 3 вказані ймовірності компрометації, які розраховані відповідно до формули (13).

Таблиця 2. Імовірності компрометації шляхів у ТКМ для різних варіантів компрометації каналів мережі

Шлях		Номер варіанту компрометації каналів ТКМ		
		1	2	3
L_1	$R_1 \to R_2 \to R_3 \to R_8$	0,712	0,951	0,838
L_2	$R_1 \to R_3 \to R_8$	0,92	0,72	0,82
L_3	$R_1 \to R_2 \to R_4 \to R_8$	0,775	0,973	0,622
L_4	$R_1 \to R_4 \to R_8$	0,65	0,73	0,94
L_5	$R_1 \to R_5 \to R_7 \to R_8$	0,664	0,928	0,928
L_6	$R_1 \to R_5 \to R_6 \to R_7 \to R_8$	0,9712	0,6544	0,9676
L_7	$R_1 \to R_6 \to R_7 \to R_8$	0,984	0,856	0,676

Таблиця 3. Імовірності компрометації мультишляхів у ТКМ, що складаються зі шляхів, що не перетинаються, для різних варіантів компрометації каналів мережі

Мультишлях	Шляхи, що входять до мультишляху	Номер варіанту компрометації каналів ТКМ		
		1	2	3
LL_1	L_1, L_4, L_5	0,3073	0,6442	0,731
LL_2	L_1, L_4, L_6	0,4495	0,4543	0,7622
LL_3	L_1, L_4, L_7	0,4554	0,5943	0,5325
LL_4	L_2, L_4, L_5	0,3971	0,4878	0,7153
LL_5	L_2, L_4, L_6	0,5808	0,344	0,7458
LL_6	L_2, L_4, L_7	0,5884	0,4499	0,5211
LL_7	L_2, L_3, L_5	0,4734	0,6501	0,4733
LL_8	L_2, L_3, L_6	0,6925	0,4584	0,4935
LL_9	L_2, L_3, L_7	0,7016	0,5997	0,3448

Використання математичної моделі (1)-(6) дозволило визначити таку множину використаних шляхів, що відповідає мінімальному значенню ймовірності компрометації повідомлення (13), яке буде ними передаватись окремими фрагментами. Ці шляхи в табл. 3 для кожного варіанту компрометації каналів зв'язку виділено сірим кольором. Таким чином, результати дослідження, наведені в табл. 2 та 3, підтвердили адекватність моделі розрахунку маршрутів, що не перетинаються, в телекомунікаційній мережі (1)-(6).

На рис. 2 – 4 показано множини шляхів у ТКМ, що не перетинаються, тобто мають спільними лише вузли відправника (R_1) та отримувача (R_8).

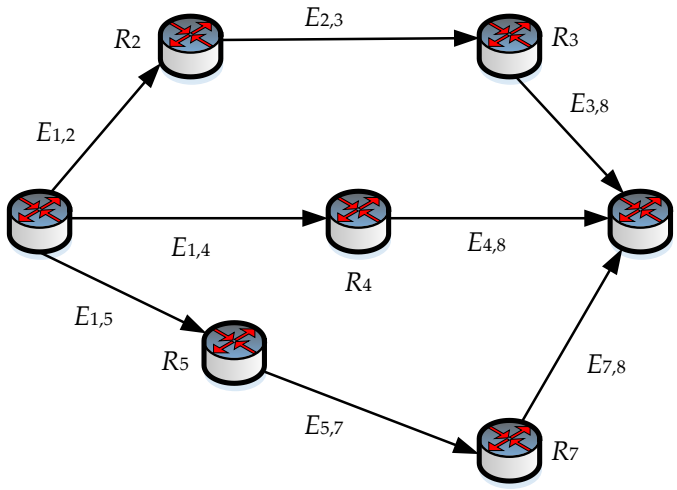

Рис. 2. Множина оптимальних шляхів L_1, L_4, L_5 для першого варіанту компрометації каналів зв'язку ТКМ ($P_{msg} = 0{,}3073$)

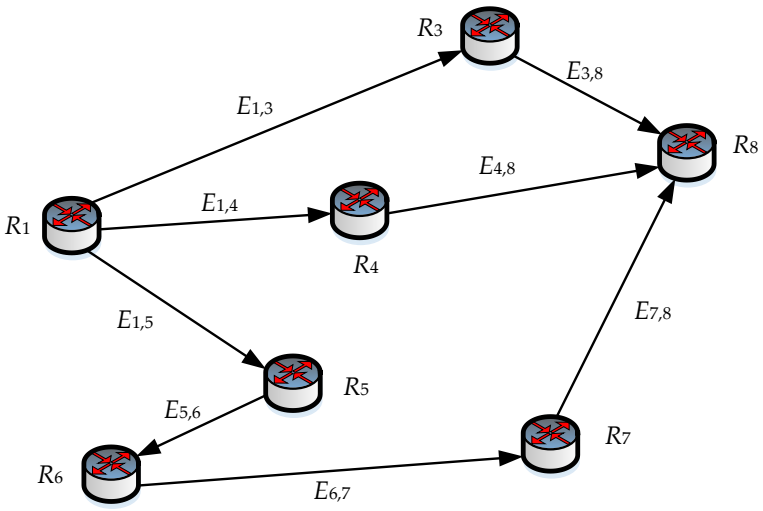

Рис. 3. Множина оптимальних шляхів L_2, L_4, L_6 для другого варіанту компрометації каналів зв'язку ТКМ ($P_{msg} = 0{,}344$)

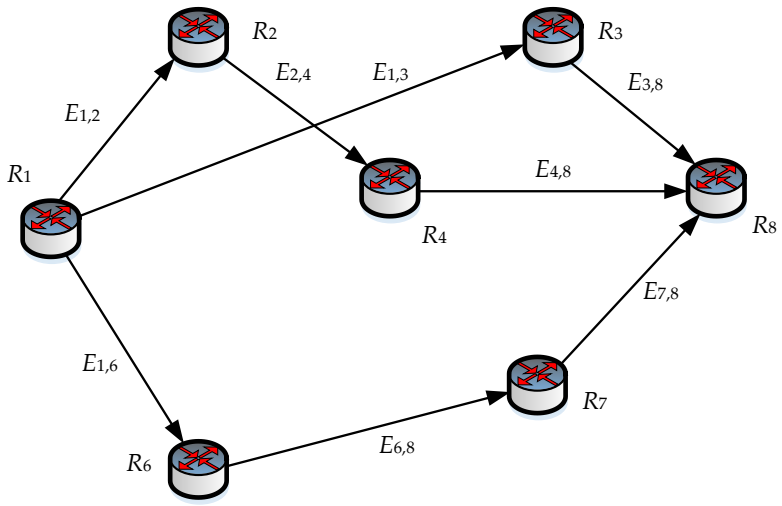

Рис. 4. Множина оптимальних шляхів L_2, L_3, L_7 для третього варіанту компрометації каналів зв'язку ТКМ ($P_{msg} = 0{,}3448$)

У табл. 4 представлено порядок фрагментованої передачі k-го повідомлення в ТКМ за допомогою множини розрахованих шляхів (табл. 3), що не перетинаються, для різних варіантів компрометації каналів мережі.

Таблиця 4. Порядок фрагментованої передачі k-го повідомлення в ТКМ за допомогою множини розрахованих шляхів, що не перетинаються, для різних варіантів компрометації каналів мережі

Номер варіанту компрометації каналів ТКМ	Мультишлях	Шлях	Кількість фрагментів k-го повідомлення, n_i	Ймовірність компрометації шляху
1	LL_1	L_1	3	0,712
		L_4	4	0,65
		L_5	3	0,664
2	LL_5	L_2	3	0,72
		L_4	3	0,73
		L_6	4	0,6544
3	LL_9	L_2	3	0,82
		L_3	4	0,622
		L_7	3	0,676

У процесі розділення конфіденційного повідомлення на фрагменти використовувалась схема Шаміра (8, 10). Як показано в табл. 3, кількість фрагментів, які передавались тим чи іншим шляхом, відповідала ймовірності його компрометації (14) та умовам (11). Чим вищою була ймовірність компрометації шляху, тим менше фрагментів повідомлення ним передавалось, але завжди для компрометації повідомлення зловмиснику необхідно скомпрометувати всі три використані для передачі маршрути, що не перетинались.

Висновки

У роботі запропоновано метод безпечної маршрутизації конфіденційних повідомлень в ТКМ за шляхами, що не перетинаються, та результати його дослідження. В основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв'язання двох оптимізаційних задач:

- розрахунку маршрутів, що не перетинаються, в телекомунікаційній мережі за допомогою моделі (1)-(8);
- безпечного балансування фрагментів конфіденційного повідомлення (9)-(14) за множиною попередньо розрахованих шляхів (1)-(8).

Модель (1)-(8) обрана для використання з причини її корисних можливостей щодо розрахунку максимальної кількості шляхів, що не перетинаються, із включенням у них каналів зв'язку з мінімальною ймовірністю компрометації. Модель (9)-(14) використана з метою забезпечення мінімально можливої ймовірності компрометації повідомлень (13), які фрагментовано передавались за попередньо розрахованою множиною шляхів, що не перетинались.

Результати проведеного дослідження на обраній мережній конфігурації (рис. 1) для трьох різних варіантів ймовірностей компрометації каналів зв'язку ТКМ (рис. 2 – рис. 4) підтвердили ефективність запропонованого методу безпечної маршрутизації та працездатність закладених в його основу оптимізаційних моделей щодо визначення множини шляхів, що не перетинались, та порядку безпечного балансування за ними фрагментів конфіденційного повідомлення (табл. 4).

Перспективи подальших досліджень в області безпечної маршрутизації в телекомунікаційній мережі пов'язані з урахуванням не тільки ймовірності компрометації каналів зв'язку, але й інших важливих показників мережної безпеки.

Список літератури

1. *Поповский, В. В., Персиков, А.В.* (2006), Защита информации в телекоммуникационных системах: Том 1, Харьков: СМИТ, 238 с.

2. *Ленков, С. В., Перегудов, Д. А., Хорошко, В. А.* (2008), Методы и средства защиты информации, Киев: Арий, 464 с.

3. *Stallings, W.* (2016), Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 768 p.

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

5. *Kenyon, T.* (2002), Data Networks: Routing, Security, and Performance Optimization, Digital Press, 1st edition, 806 p.

6. *Новиков, С. Н.* (2015), Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи, Москва: Горячая линия – Телеком, 128 с.

7. *Santos, O., Kampanakis, P., Woland, A.* (2016), Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP, 1st edition, Cisco Press, 368 p.

8. *Myslitski, K., Rak, J., Kuszner, Ł.* (2017), "Toward fast calculation of communication paths for resilient routing", Networks, No. 70(4), P. 308-326. **DOI**: https://doi.org/10.1002/net.21789

9. *Gharib, M., Yousefizadeh, H., Movaghar, A.* (2018), "Secure Overlay Routing for Large Scale Networks", IEEE Transactions on Network Science and Engineering, No. 1, P. 1-12. **DOI**: https://doi.org/10.1109/TNSE.2018.2812830

10. *Gupta, D., Segal, A., Panda, A., Segev, G., Schapira, M., Feigenbaum, J., Rexford, J., Shenker, S.* (2012), "A new approach to interdomain routing based on secure multi-party computation", Proceedings of the 11th ACM Workshop on Hot Topics in Networks (HotNets-XI), 29-30 October, P. 37-42. **DOI**: https://doi.org/10.1145/2390231.2390238

11. *Лемешко, О. В., Єременко, О. С., Невзорова, О. С.* (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с.

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

13. *Снегуров, А. В., Чакрян, В. Х.* (2012), "Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности", Системи управління, навігації та зв'язку, No. 4(24), С. 105-110.

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

15. *Lemeshko, O., Yeremenko, O., Persikov, A., Vavenko, T.* (2018), "Mathematical Model of Calculating the Maximum Number of Disjoint Paths in Secure Routing", Proceedings of the 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 10-14 September, P. 1–4. **DOI**: https://doi.org/10.1109/UkrMiCo43733.2018.9047581

16. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B.* (2019), "Enhanced Solution of the Disjoint Paths Set Calculation for Secure QoS Routing", Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 18-20 December, P. 210-213. **DOI**: https://doi.org/10.1109/ATIT49449.2019.9030520

17. *Lemeshko, O., Yeremenko, O., Sleiman, B., Yevdokymenko, M.* (2020), "Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN", Advances In Electrical And Electronic Engineering, No. 18(1), P. 23-30. **DOI**: https://doi.org/10.15598/aeee.v18i1.3548

18. *Єременко, О. С., Євдокименко, М. О., Слейман, Б.* (2020), "Удосконалена модель швидкої перемаршрутизації з реалізацією схеми захисту шляху та пропускної здатності в програмно-конфігурованих мережах", Сучасний стан наукових досліджень та технологій в промисловості, No. 1(11), С. 163–171. **DOI**: https://doi.org/10.30837/2522-9818.2020.11.163

19. *Lou, W., Kwon, Y.* (2006), "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", IEEE Transactions on Vehicular Technology, No. 55(4), P. 1320–1330. **DOI**: https://doi.org/10.1109/TVT.2006.877707

20. *Lou, W., Liu, W., Fang, Y.* (2004), "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, P. 2404-2413. **DOI**: https://doi.org/10.1109/INFCOM.2004.1354662

21. *Лемешко, А. В., Еременко, А. С.* (2015), "Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам", Захист інформації, No. 17(2), С. 135-142. **DOI**: https://doi.org/10.18372/2410-7840.17.8776

22. *Yeremenko, O. S., Ali, S. A.* (2015), "Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET", Radioelectronics and Informatics, No. 1(68), С. 26–29.

23. *Еременко, А. С.* (2015), "Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной или комбинированной структурой", Наукові записки Українського науково-дослідного інституту зв'язку, No. 6(40), С. 64–71.

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

25. *Yeremenko, O., Lemeshko, O., Persikov, A.* (2018), "Secure Routing in Reliable Networks: Proactive and Reactive Approach", Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655. **DOI**: https://doi.org/10.1007/978-3-319-70581-1_44