УДК 621.391

ДОСЛІДЖЕННЯ ПОТОКОВОЇ МОДЕЛІ БЕЗПЕЧНОЇ TRAFFIC ENGINEERING МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ З НОРМОВАНИМИ УМОВАМИ БЛОКУВАННЯ КАНАЛІВ

О.В. Лемешко, А.В. Персіков, О.С. Єременко
Харківський національний університет радіоелектроніки

Abstract *– The work improves the flow-based model of secure routing with load balancing in accordance with the Traffic Engineering concept by considering the network security parameters in an information and communication network (ICN). Within the framework of the proposed model, the solution to the technological problem of secure routing with load balancing in an ICN was reduced to solving an optimization problem of linear programming, which guarantees the predictable computational complexity of solutions and low requirements for the computing power of devices responsible for solving routing problems – routers, route servers, controllers, etc. The novelty of the proposed model is the modification of the exponential model of blocking communication links, taking into account normalized conditions to prevent a situation where even the most secure links will be blocked, leading to inefficient use of the link resource. The results of the study of secure routing processes with load balancing in ICN confirmed the model's effectiveness in considering the network state: its topology, flow characteristics, bandwidth, and congestion of communication links, as well as the probability of their compromise. This made it possible to orient the resulting routing solutions to reduce the congestion of communication links that have a high compromise probability by redistributing traffic to more secure links. In the course of the study, a comparative analysis of the effectiveness of using secure and TE routing models was carried out by a number of indicators. It has been established that the use of SecTE and NormSecTE secure routing models focused on finding a compromise between the Quality of Service and network security indicators. At the same time, the proposed improved model of secure TE routing NormSecTE, based on a more accurate consideration of the probability of compromising communication links, allowed, compared to the SecTE model, to improve the level of network security (packet compromise probability), but with a certain decrease in the level of Quality of Service (average end-to-end packet delay) in the ICN.*

Анотація *– У роботі вдосконалено потокову модель безпечної маршрутизації з балансуванням навантаження відповідно до концепції Traffic Engineering на основі врахування параметрів мережної безпеки в інфокомунікаційній мережі (ІКМ). У межах запропонованої моделі вирішення технологічної задачі безпечної маршрутизації з балансуванням навантаження в ІКМ було зведено до розв'язання оптимізаційної задачі лінійного програмування, що гарантує прогнозовану обчислювальну складність рішень та невисокі вимоги до обчислювальних потужностей пристроїв, які відповідають за розв'язання задач маршрутизації – маршрутизаторів, серверів маршрутів, контролерів тощо. Новизною запропонованої моделі є модифікація експоненціальної моделі блокування каналів зв'язку з урахуванням нормалізованих умов для запобігання ситуації, коли блокуватись будуть навіть найбільш безпечні канали, що призведе до неефективного використання канального ресурсу. Результати дослідження процесів безпечної маршрутизації з балансуванням навантаження в ІКМ підтвердили ефективність моделі з погляду врахування стану мережі: її топології, характеристик потоків, пропускної здатності та завантаженості каналів зв'язку, а також імовірностей їхньої компрометації. Це дозволило зорієнтувати отримані маршрутні рішення на зменшення завантаженості каналів зв'язку, які мають високу ймовірність компрометації, шляхом перерозподілу трафіка на більш безпечні канали. В процесі дослідження здійснено порівняльний аналіз ефективності використання моделей безпечної та ТЕ-маршрутизації за множиною показників. Встановлено, що використання моделей безпечної маршрутизації SecTE та NormSecTE орієнтувало на пошук компромісу між показниками якості обслуговування та мережної безпеки. При цьому саме запропонована вдосконалена модель безпечної ТЕ-маршрутизації NormSecTE на основі більш точного врахування ймовірностей компрометації каналів зв'язку дозволила у порівнянні з моделлю SecTE покращити рівень мережної безпеки (ймовірності компрометації пакетів), але при певному зниженні рівня якості обслуговування (середньої міжкінцевої затримки пакетів) в ІКМ.*

Вступ

Зростаюча складність і різноманітність мереж вимагає прийняття нових підходів до управління та забезпечення якості обслуговування (Quality of Service, QoS) і безпеки

[1-3] в інфокомунікаційних мережах (ІКМ). Водночас програмно-конфігуровані ІКМ пропонують нові можливості для гнучкого управління трафіком, дозволяючи враховувати вимоги і до QoS, і до безпеки [4]. Ця еволюція ставить нові виклики перед засобами маршрутизації, які повинні адаптивно враховувати різні вимоги до якості обслуговування та безпеки, визначаючи оптимальні маршрути передачі потоків трафіку [1, 2]. Адаптивність до змін у мережі є вирішальним фактором, що впливає на ефективність протоколів маршрутизації в складних середовищах [5 – 8]. Разом зі здатністю враховувати показники продуктивності та безпеки це має сприяти швидкому відновленню після збоїв та забезпечити досягнення високого рівня QoS і мережної безпеки в межах комплексного підходу до управління трафіком [9 – 11].

Не менш важливим є застосування математичних інструментів у розробці та оптимізації рішень маршрутизації, що дозволяє ефективно вирішувати проблеми балансування навантаження та безпеки [1, 2]. Такий підхід лежить в основі нових стратегій маршрутизації, здатних відповідати вимогам сучасних мереж і програмованих інфраструктур.

Відомо, що більшість існуючих протоколів IP-маршрутизації, як-от RIP та OSPF, базуються на графових моделях та алгоритмах пошуку найкоротшого шляху [1, 5]. Вони були ефективними за умов обмеженої обчислювальної потужності маршрутизаторів, коли їхня продуктивність складала десятки пакетів за секунду. Проте ці протоколи не враховують ні характеристики потоків, ні показники безпеки мережі. Сучасні маршрутизатори, які працюють на основі багатоядерних архітектур, здатні обробляти мільйони пакетів за секунду. Це відкриває можливості для використання складніших моделей маршрутизації, що враховують багатопотоковий трафік і оптимізують QoS та безпеку. Останні дослідження активно зосереджуються на розробці методів QoS-маршрутизації, що враховують показники мережної безпеки [12 – 16].

Одним із перспективних напрямків є реалізація принципів Traffic Engineering (TE) для збалансованого використання (завантаження) мережних ресурсів, що допомагає уникнути перевантаження окремих сегментів мережі та зниження QoS [17 – 20]. Існує низка рішень у цій сфері, які адаптують балансування навантаження з урахуванням безпеки, пропонуючи компроміси між одношляховою та багатошляховою маршрутизацією [2, 8 – 11]. Запропонована модель безпечної ТЕ-маршрутизації є подальшим розвитком цих рішень, з акцентом на балансування навантаження та блокування трафіку в умовах можливої компрометації каналів мережі.

Отже, стаття присвячена актуальній науково-прикладній задачі, пов'язаній із вдосконаленням та дослідженням потокової моделі безпечної Traffic Engineering маршрутизації в інфокомунікаційної мережі, яка оптимізує продуктивність мережі шляхом інтеграції удосконалених умов балансування навантаження та нормалізованої моделі блокування каналів зв'язку, тим самим підвищуючи загальний рівень якості обслуговування та безпеки.

I. Опис потокової моделі безпечної Traffic Engineering маршрутизації з нормованими умовами блокування каналів

У даному розділі наведено позначення, що використовуються у постановці задачі. Нехай ядро мережі представлено у вигляді орієнтованого графа $G=(R,E)$ з вершинами (маршрутизаторами) $R=\left\{R_i; i=\overline{1,m}\right\}$ та гілками (каналами зв'язку між маршрутизаторами) $E=\left\{E_{i,j}; i,j=\overline{1,m}; i\neq j\right\}$. Кожен канал $E_{i,j}\in E$ має певну пропускну здатність $\varphi_{i,j}$ в пакетах за секунду (пак/с). Відповідно кількість каналів зв'язку визначається потужністю множини $\left|E\right|=n$.

У базовій моделі Traffic Engineering кожен *k*-й потік є одноадресним з певними характеристиками: множина потоків *K*, маршрутизатор-відправник s_k, маршрутизатор-отримувач d_k і середня інтенсивність потоку λ^k (пак/с). Для розв'язання задачі Traffic Engineering необхідно обчислити маршрутні змінні $x_{i,j}^k$, які представляють частину *k*-го потоку, що передається каналом зв'язку $E_{i,j}\in E$ вздовж маршруту.

У разі використання стратегії багатошляхової маршрутизації встановлюються наступні обмеження [1, 9]:

$$0\le x_{i,j}^k\le 1. \tag{1}$$

Умови збереження потоку вводяться для забезпечення зв'язності маршруту [9]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=0;\ k\in K,\ R_i\neq s_k,d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=1;\ k\in K,\ R_i=s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=-1;\ k\in K,\ R_i=d_k. \end{cases} \tag{2}$$

Середня інтенсивність пакетів *k*-го потоку в каналі може бути обчислена, як показано нижче:

$$\lambda_{i,j}^k=\lambda^k x_{i,j}^k,\ E_{i,j}\in E. \tag{3}$$

Наступна формула використовується для кількісної оцінки коефіцієнта завантаженості кожного каналу:

$$\alpha_{i,j}=\frac{\sum\limits_{k\in K}\lambda^k x_{i,j}^k}{\varphi_{i,j}},\ E_{i,j}\in E. \tag{4}$$

Як показав аналіз [21, 22], балансування використання ресурсів мережі має вирішальне значення для задоволення вимог ТЕ на підставі запобігання перевантаженню. Отже, під час реалізації балансування навантаження, враховуючи показник мережної безпеки, пропонується пов'язати з кожним каналом $E_{i,j} \in E$ ймовірність компрометації $p_{i,j}$. Далі завдання полягає в тому, щоб максимізувати використання безпечних каналів, мінімізувати використання каналів з високою ймовірністю компрометації, а канали з критичним рівнем компрометації взагалі заблокувати

Тому пропонуються вдосконалені умови балансування навантаження [9, 10]:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha v_{i,j}(p_{i,j}) \varphi_{i,j}, \; E_{i,j} \in E, \tag{5}$$

де α – керуюча змінна, яка задає верхню границю завантаженості каналу мережі з урахуванням його можливого блокування і відповідає обмеженням [1, 22]:

$$0 \le \alpha \le 1, \tag{6}$$

а $v_{i,j}$ – вагові коефіцієнти. Водночас функція $v_{i,j}(p_{i,j})$ є моделлю блокування каналів зв'язку під час безпечної маршрутизації з балансуванням навантаження, вказуючи, яка частина пропускної здатності каналу буде використана (або заблокована) через зміну його ймовірності компрометації.

Таким чином, пропонується модифікувати умови, представлені в [9, 11], якщо прогнозований сценарій компрометації та межі (норми) ймовірностей компрометації каналів $p_{\min}$ і $p_{\max}$ відомі заздалегідь:

$$v_{i,j}(p_{i,j}) = \begin{cases} 0, & \text{коли } p_{i,j} = p_{\max}; \\ 1, & \text{коли } p_{i,j} = p_{\min}, \end{cases} \tag{7}$$

$$p_{\min} \le p_{i,j} \le p_{\max}. \tag{8}$$

Значення $p_{\min}$ зазвичай являє собою ймовірність компрометації найбільш захищеного каналу на момент розрахунку. Порогове значення $p_{\max}$ встановлює максимально допустиму ймовірність компрометації, при перевищенні якої канал блокується. Для успішного розв'язання задачі безпечної маршрутизації повинна виконуватись умова:

$$0 \le p_{\min} < p_{\max} \le 1. \tag{9}$$

Відповідно до мети ТЕ, необхідно мінімізувати граничне значення α, як це зроблено в роботах [9 – 11]:

$$\min_{x,\alpha} \alpha . \tag{10}$$

Таким чином, завдання безпечної ТЕ-маршрутизації формулюється як оптимізаційна задача з критерієм (10) та обмеженнями (1), (2), (5) і (6) для досягнення оптимального балансування навантаження в процесі мінімізації завантаженості кожного каналу зв'язку. Оптимізація процесу багатошляхової маршрутизації покращує продуктивність мережі, показники QoS, як-от середню затримку пакетів і джиттер, а також показники надійності, наприклад, імовірність втрат пакетів.

У подальшому дослідженні безпечної ТЕ-маршрутизації з використанням запропонованої моделі (1)-(10) буде зосереджено увагу на експоненціальній моделі блокування, що задається наступним виразом за модифікованих умов (7), (8):

$$v_{i,j}(p_{i,j}) = \exp(-n(p_{i,j} - p_{\min}) / (p_{\max} - p_{\min})), \tag{11}$$

де n – коефіцієнт, за допомогою якого можна регулювати чутливість процедури блокування каналів залежно від їхньої імовірності компрометації. Для забезпечення виконання умов (7) необхідно, щоб $n \geq 7$ (рис. 1).

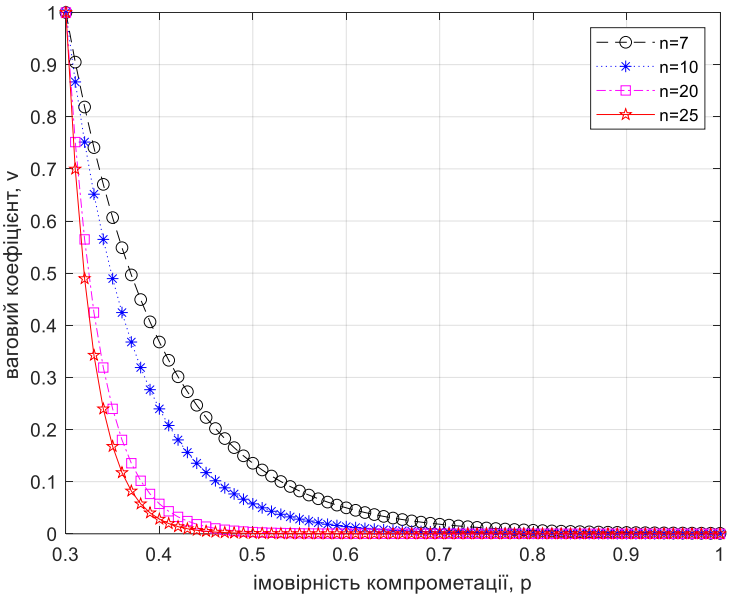

Рис. 1. Візуалізація моделі блокування каналів зв'язку (11) при $p_{\min} = 0,3$ та $p_{\max} = 1$

Як показано на рис. 1 при $n \geq 7$ модель (11) забезпечує досить високу чутливість до зміни $p_{i,j}$. Вже у разі ймовірності компрометації каналів $p_{i,j} = 0,45...0,7$ цей канальний ресурс фактично буде блоковано до використання при відповідних значеннях коефіцієнта n.

II. Дослідження процесу безпечної ТЕ-маршрутизації з використанням запропонованого рішення

У процесі проведеного дослідження аналізувались та порівнювались чотири моделі ТЕ-маршрутизації:

- модель Sec, яка визначала для передачі пакетів найбільш безпечний маршрут [1, 2];
- модель ТЕ, яка не враховувала параметри безпеки ІКМ та була представлена виразами (1)-(6), (11) при $v_{i,j}(p_{i,j}) = 1$ [22];
- модель SecTE, яка враховувала параметри безпеки ІКМ у межах всього діапазону значень ймовірності компрометації каналів та була представлена виразами (1)-(11), коли $p_{\min} = 0$ та $p_{\max} = 1$;
- модель NormSecTE, яка є вдосконаленою версією моделі SecTE на основі врахування нормалізованих параметрів безпеки ІКМ та представлена виразами (1)-(11), коли, наприклад, $p_{\min} = 0,3$ та $p_{\max} = 1$.

Подальше дослідження дозволило порівняти ефективність запропонованої моделі безпечної маршрутизації ТЕ з існуючими моделями за трьома показниками. Першим показником була верхня границя використання каналів мережі $\alpha_{\max}$, розрахована як найбільше значення завантаженості каналів (4). Другий показник оцінював безпеку мережі шляхом обчислення міжкінцевої ймовірності компрометації пакетів для *k*-го потоку p_{E2E}^{k} по всіх використовуваних шляхах. Третій показник відповідав середній міжкінцевій затримці пакетів *k*-го потоку τ_{E2E}^{k} [9 – 11].

Продемонструємо особливості розв'язання задачі безпечної ТЕ-маршрутизації на прикладі структури ІКМ, яка представлена на рис. 2.

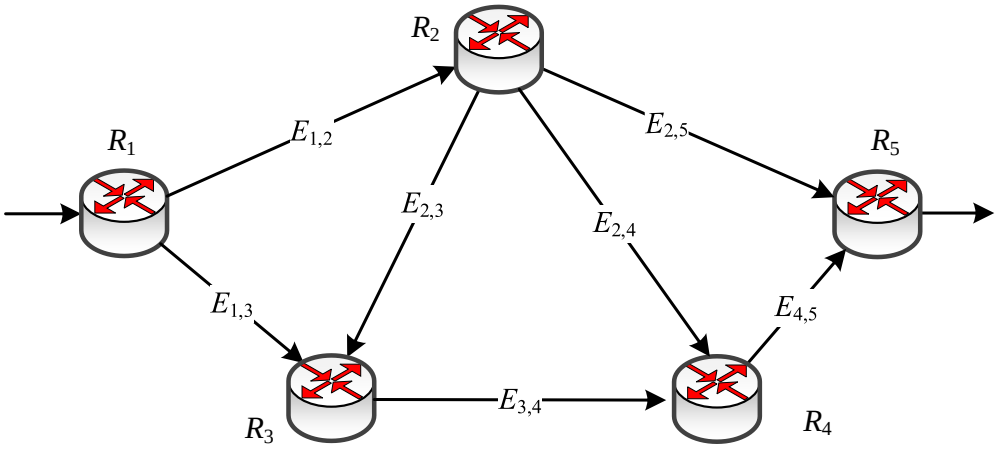

Рис. 2. Варіант структури ІКМ, яка досліджувалась

Моделювався випадок маршрутизації одного потоку пакетів, коли пакети передавалися від першого до п'ятого маршрутизатора. Тому у подальшому номер потоку було опущено. В табл. 1 наведено пропускні здатності каналів зв'язку та ймовірності

їхньої компрометації. Відповідно до інформації про структуру ІКМ (рис. 2) та характеристики її каналів у табл. 2 наведено дані про доступні маршрути між маршрутизатором-джерелом (R_1) і маршрутизатором-отримувачем пакетів (R_5), а також імовірності їхньої компрометації.

Таблиця 1. Характеристики каналів зв'язку ІКМ

Канал зв'язку	$E_{1,2}$	$E_{2,5}$	$E_{1,3}$	$E_{3,4}$	$E_{4,5}$	$E_{2,3}$	$E_{2,4}$
Пропускна здатність	900	300	400	700	900	800	300
Імовірність компрометації	0,4	0,3	0,4	0,42	0,5	0,35	0,3

Таблиця 2. Імовірності компрометації маршрутів ІКМ

Маршрут/ його номер	$R_1 \to R_2 \to R_5$	$R_1 \to R_3 \to R_4 \to R_5$	$R_1 \to R_2 \to R_3 \to R_4 \to R_5$	$R_1 \to R_2 \to R_4 \to R_5$
	1	2	3	4
Імовірність компрометації	0,58	0,826	0,8869	0,79

Таким чином, відповідно до змісту табл. 1, залежності, представлені на рис. 1, є актуальними для досліджуваного прикладу. Тоді у табл. 3 наведено результати розрахунків, отриманих з використанням досліджуваних трьох моделей ТЕ-маршрутизації при $\lambda = 250$ пак/с та $n = 7$, тобто моделювався випадок маршрутизації одного потоку пакетів. У разі використання моделі Sec всі пакети передавалися першим маршрутом, який був найбільш безпечним серед інших рішень (табл. 2).

Таблиця 3. Результати порівняльного аналізу отриманих рішень щодо безпечної маршрутизації та балансування навантаження ($\lambda = 250$ пак/с, $n = 7$)

Канал зв'язку	TE		SecTE		NormSecTE	
	$\lambda_{i,j}$	$\alpha_{i,j}$	$\lambda_{i,j}$	$\alpha_{i,j}$	$\lambda_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	187,5	0,2083	214,0711	0,2379	196,2364	0,218
$E_{2,5}$	62,5	0,2083	143,6954	0,479	177,8086	0,5927
$E_{1,3}$	62,5	0,1563	35,9289	0,0898	53,7636	0,1344
$E_{3,4}$	145,8333	0,2083	35,9289	0,0513	72,1914	0,1031
$E_{4,5}$	187,5	0,2083	106,3046	0,1181	72,1914	0,0802
$E_{2,3}$	83,3333	0,1042	0	0	18,4278	0,023
$E_{2,4}$	41,6667	0,1389	70,3757	0,2346	0	0

Відповідно до особливостей структури мережі (рис. 1 і табл. 2) інтенсивність потоку пакетів у першому маршруті (λ_1) визначала інтенсивність потоку в каналі $E_{2,5}$; інтенсивність потоку пакетів у другому маршруті (λ_2) визначала інтенсивність потоку в

каналі $E_{1,3}$; інтенсивність потоку пакетів у третьому маршруті (λ_3) визначала інтенсивність потоку у каналі $E_{2,3}$; інтенсивність потоку пакетів у четвертому маршруті (λ_4) визначала інтенсивність потоку в каналі $E_{2,4}$.

В табл. 4 для кожної моделі маршрутизації наведено розраховані показники ефективності, що характеризують якість балансування навантаження та аспекти, пов'язані з мережною безпекою та якістю обслуговування. Порівняльна характеристика показана для n=7, що відповідає результатам, наведеним у табл. 4 як для $\lambda = 250$ пак/с, так і для $\lambda = 200$ пак/с.

Таблиця 4. Порівняльна характеристика показників ефективності рішень щодо безпечної маршрутизації та балансування навантаження (n=7)

Модель	$\lambda = 250$ пак/с			$\lambda = 200$ пак/с		
	$\alpha_{\max}$	p_{E2E}	τ_{E2E} (мс)	$\alpha_{\max}$	p_{E2E}	τ_{E2E} (мс)
Sec	0,8333	0,58	21,5	0,6667	0,58	11,4
TE	0,2083	0,7788	6,1	0,1667	0,7788	5,8
SecTE	0,479	0,6745	7,3	0,3832	0,6745	6,6
NormSecTE	0,5927	0,6555	8,5	0,4742	0,6555	7,1

За результатами порівняльного аналізу (табл. 4) можна зробити висновок, що модель Sec використовує найбільш безпечні шляхи, поки вистачає їхньої пропускної здатності. Модель TE-маршрутизації забезпечує балансування, орієнтоване лише на покращення QoS-показників, наприклад, середньої міжкінцевої затримки пакетів. Використання моделей безпечної маршрутизації SecTE та NormSecTE орієнтує на пошук компромісу між показниками якості обслуговування та мережної безпеки. За використання експоненціальної моделі блокування пакетів (11) при збільшенні параметру n (рис. 1) блокування каналів підсилюється, і моделі SecTE та NormSecTE більше уваги приділяють покращенню рівня мережної безпеки, а при зменшенні n у процесі балансування навантаження сильніше враховуються параметри QoS. Водночас модель NormSecTE за умови одних і тих самих вихідних даних забезпечувала більш високий рівень мережної безпеки, аніж SecTE або TE. Це реалізувалось на підставі певного зниження рівня якості обслуговування.

Як і очікувалось, модель Sec забезпечувала найкращий рівень мережної безпеки (p_{E2E}=0,58) серед усіх інших моделей маршрутизації (табл. 4). Використання моделі TE-маршрутизації призводило до підвищення імовірності компрометації пакетів на 34%. Застосування рішень SecTE та NormSecTE у порівнянні з моделлю Sec також призводило до погіршення рівня мережної безпеки, але ймовірність компрометації пакетів зростала лише на 15,83% та 13,4% відповідно. Зі свого боку мінімальну середню міжкінцеву затримку забезпечувала саме модель TE-маршрутизації (6,1 мс та 5,8 мс). Використання моделі безпечної маршрутизації Sec призводило до суттєвого погіршення середньої затримки – від 1,96 до 3,5 разів. Застосування моделі SecTE супроводжувалось менш суттєвим зростанням затримки пакетів: приблизно від 13,21% до 20,41%.

Реалізація моделі NormSecTE супроводжувалось також певним зростанням затримки пакетів – приблизно від 21,75% до 39,57%.

Висновки

1. Перспективними напрямками розвитку та вдосконалення рішень щодо забезпечення мережної безпеки є вдосконалення засобів управління трафіком і маршрутизації. Новітні рішення в області управління трафіком і маршрутизації мають враховувати не тільки параметри мережної продуктивності (пропускну здатність, затримки та рівень втрат пакетів), але й параметри мережної безпеки, що характеризують ефективність роботи задіяних у мережі систем виявлення вторгнень та аналізу вразливостей і ризиків.

2. У роботі вдосконалено потокову модель безпечної маршрутизації з балансуванням навантаження відповідно до концепції Traffic Engineering на основі врахування параметрів мережної безпеки в ІКМ, яка представлена виразами (1)-(6), (9)-(11). У межах даної моделі вирішення технологічної задачі безпечної маршрутизації з балансуванням навантаження в ІКМ було зведено до розв'язання оптимізаційної задачі з критерієм оптимальності (10) та обмеженнями (1), (2), (5) і (6). У разі реалізації багатошляхової маршрутизації (1) сформульована оптимізаційна задача відноситься до класу задач лінійного програмування, що гарантує прогнозовану обчислювальну складність рішень і невисокі вимоги до обчислювальних потужностей пристроїв, які відповідають за розв'язання задач маршрутизації – маршрутизаторів, серверів маршрутів, контролерів тощо.

3. До новизни запропонованої моделі варто віднести модифікацію експоненціальної моделі блокування каналів зв'язку (11) з урахуванням нормалізованих умов (7)-(9) для запобігання ситуації, коли блокуватись будуть навіть найбільш безпечні канали, що призведе до неефективного використання канального ресурсу.

4. Результати дослідження процесів безпечної маршрутизації з балансуванням навантаження в ІКМ підтвердили ефективність запропонованої моделі з погляду врахування стану мережі: її топології, характеристик потоків, пропускної здатності та завантаженості каналів зв'язку, а також імовірностей їхньої компрометації. Це дозволило зорієнтувати отримані маршрутні рішення на зменшення завантаженості каналів зв'язку, які мають високу ймовірність компрометації, шляхом перерозподілу трафіка на більш безпечні канали. Зазвичай більш інтенсивно завантажувались ті канали, які мали високу пропускну здатність і низьку ймовірність компрометації.

5. В процесі дослідження здійснено порівняльний аналіз ефективності використання моделей безпечної та ТЕ-маршрутизації за множиною показників. Встановлено, що класична модель ТЕ-маршрутизації [22] завжди забезпечує найнижчий рівень завантаженості каналів зв'язку ІКМ і, як висновок, найкращу середню міжкінцеву затримку пакетів. Проте ця модель ніяким чином не враховує показники мережної безпеки елементів мережі (каналів, маршрутизаторів, шляхів), тому отримані за допомогою

неї рішення мали найгіршу ймовірність компрометації пакетів. Використання моделей безпечної маршрутизації SecTE та NormSecTE орієнтувало на пошук компромісу між показниками якості обслуговування та мережної безпеки (табл. 4). Водночас саме запропонована вдосконалена модель безпечної ТЕ-маршрутизації NormSecTE на основі більш точного врахування ймовірностей компрометації каналів зв'язку дозволила у порівнянні з моделлю SecTE покращити рівень мережної безпеки (ймовірності компрометації пакетів), але при певному зниженні рівня якості обслуговування (середню міжкінцеву затримку пакетів) в ІКМ.

6. Розвиток запропонованих у даній роботі рішень бачиться у розширенні множини моделей блокування каналів [9 – 11], які потрібно адаптувати до нормалізованих умов (7)-(9). Додаткового дослідження потребують питання аналізу впливу топології мережі, сценаріїв компрометації та об'єму навантаження на мережу на комплексне забезпечення заданого рівня ефективності ІКМ як за QoS-показниками, так і показниками мережної безпеки.

Список літератури

1. *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. **DOI**: https://doi.org/10.30837/978-966-659-282-1

2. *Лемешко, О.В., Єременко, О.С., Євдокименко, М.О., Шаповалова, А.С., Слейман, Б.* (2022), Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах, Харків: ХНУРЕ, 198 с. **DOI**: https://doi.org/10.30837/978-966-659-378-1

3. *Mohammed, S.A., Ralescu, A.L.* (2023), Future Internet Architectures on an Emerging Scale—A Systematic Review. Future Internet, 15, 166. https://doi.org/10.3390/fi15050166

4. *Tache, M.D., Păscuțoiu, O., Borcoci, E.* (2024), Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization. Applied Sciences, 14, 5967. https://doi.org/10.3390/app14145967

5. *Medhi, D., Ramasamy, K.* (2018), Network Routing (Algorithms, Protocols, and Architectures), 2nd edition, Elsevier Inc, 1018 p.

6. *Rak, J.* (2020), Guide to Disaster-Resilient Communication Networks, 1st edition, Springer, 813 p.

7. *Єременко, О. С.* (2019), "Огляд теоретичних рішень щодо безпечної маршрутизації в інфокомунікаційних мережах", Проблеми телекомунікацій, No. 1(24). С. 3–23. **DOI**: https://doi.org/10.30837/pt.2019.1.01.

8. *Єременко, О. С., Євдокименко, М. О.* (2018), "Огляд теоретичних рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах", Проблеми телекомунікацій, No. 1(22), С. 25–42. **DOI**: https://doi.org/10.30837/pt.2018.1.02.

9. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Baranovskyi, O.* (2022), "Complex Investigation of the Compromise Probability Behavior in Traffic Engineering Oriented Secure Routing Model in Software-Defined Networks", in Klymash, M., Beshley, M., Luntovskyy, A. (eds) Future Intent-Based Networking, Lecture Notes in Electrical Engineering, Vol. 831, Springer, Cham, P. 145–160. **DOI**: https://doi.org/10.1007/978-3-030-92435-5_8.

10. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Lemeshko, V., Persikov, M.* (2021), "Analysis of Secure Routing Processes Using Traffic Engineering Model", Proceedings of the

2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22-25 September, pp. 951–955, **DOI**: https://doi.org/10.1109/IDAACS53288.2021.9660980.

11. *Lemeshko, O., Yeremenko, O., Shapovalova, A., Yevdokymenko, M., Omowumi, S.O., Hailan, A.M.* (2021), "Secure Routing with Power Link Blocking Model and Load Balancing", Proceedings of the 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 21-25 September, P. 216–219, **DOI**: https://doi.org/10.1109/AICT52120.2021.9628938.

12. *Xu, Y., Liu, J., Shen, Y., Jiang, X., Ji, Y., Shiratori, N.* (2021), "QoS-Aware Secure Routing Design for Wireless Networks With Selfish Jammers", IEEE Transactions on Wireless Communications, No. 20(8), P. 4902–4916. **DOI**: https://doi.org/10.1109/TWC.2021.3062885.

13. *Li, C., Liu, Y., Xiao, J. and Zhou, J.* (2022), "MCEAACO-QSRP: A Novel QoS-Secure Routing Protocol for Industrial Internet of Things", IEEE Internet of Things Journal, No. 9(19), P. 18760–18777. **DOI**: https://doi.org/10.1109/JIOT.2022.3162106.

14. *Pathak, A., Al-Anbagi, I. and Hamilton, H.J.* (2022), "An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs", IEEE Internet of Things Journal, No. 9(23), P. 23826–23840. **DOI**: https://doi.org/10.1109/JIOT.2022.3189832.

15. *Gehlot, A., Kumar, S.* (2022), "Trust-Based Safe QoS Routing in Mobile Ad Hoc Networks", Proceedings of the 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 16-17 December, P. 1–6. **DOI**: https://doi.org/10.1109/ICATIECE56365.2022.10047396.

16. *Soundararajan, S., Prabha, R., Baskar, M. and Nagalakshmi, T. J.* (2023), "Region Centric GL Feature Approximation Based Secure Routing for Improved QoS in MANET", Intelligent Automation & Soft Computing, No. 36(1), P. 267–280. **DOI**: https://doi.org/10.32604/iasc.2023.032239.

17. *Palani, U., Amuthavalli, G., Alamelumangai, V.* (2020), "Secure and load-balanced routing protocol in wireless sensor network or disaster management", IET Information Security, No. 14(5), P. 513–520. **DOI**: https://doi.org/10.1049/iet-ifs.2018.5057.

18. *Cyriac, R. and Durai M. A., S.* (2022), "LMH-RPL: a load balancing and mobility aware secure hybrid routing protocol for low power lossy network", International Journal of Pervasive Computing and Communications. **DOI**: https://doi.org/10.1108/ijpcc-05-2022-0213.

19. *Thahniyath, G., Jayaprasad, M.* (2022), "Secure and load balanced routing model for wireless sensor networks", Journal of King Saud University – Computer and Information Sciences, No. 34(7), P. 4209–4218. **DOI**: https://doi.org/10.1016/j.jksuci.2020.10.012.

20. *Selvan, T., Malathi, P., Freeda, S.* (2020), "An Efficient Method for Adjustable Load Equalization for Reducing Traffic in Routing for Mobile Ad Hoc Networks", Wireless Personal Communications, No. 110, P. 2149–2164. **DOI**: https://doi.org/10.1007/s11277-019-06834-9.

21. *Seok, Y., Lee, Y., Choi, Y., Kim, C.* (2001), "Dynamic Constrained Multipath Routing for MPLS Networks", Proceedings of the Tenth International Conference on Computer Communications and Networks (Cat. No. 01EX495), Scottsdale, AZ, USA, 15-17 October 2001, P. 348–353. **DOI**: https://doi.org/10.1109/ICCCN.2001.956289.

22. *Lee, Y., Seok, Y., Choi, Y., Kim, C.* (2002), "A constrained multipath traffic engineering scheme for MPLS networks", Proceedings of the 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333), Vol. 4, New York, NY, USA, 28 April 2002 – 02 May 2002, P. 2431–2436. **DOI**: https://doi.org/10.1109/ICC.2002.997280.