УДК 004.056.5

МЕТОД БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ МУЛЬТИФРАКТАЛЬНОГО ТРАФІКА

Т.А. РАДІВІЛОВА

Харківський національний університет радіоелектроніки

Abstract *– The paper proposes a solution to the current problem of ensuring the quality of service of infocommunication networks, taking into account network security, which provides a greater number of services with high efficiency. In the paper, experiments were conducted to analyze the effect of fractality and vulnerabilities on the quality of service parameters. The safety route provision method for the transfer of multifractal traffic in infocommunication networks was proposed. The proposed method takes into account the specified limits on the delay time and the number of lost packets for each type of traffic quality service. The results of the analysis show that the overload during traffic transmission on a switched channel occurs due to the multifractal characteristics of traffic and the presence of an attack. This method is based on a special procedure for calculating the cost of routes with the further use of these data when choosing the shortest paths. In this paper, an experiment was conducted to analyze the effectiveness of the proposed method under conditions of multifractal traffic and the presence of attack traffic. The results showed that the use of the proposed method allows to reduce latency and jitter in the network, as well as to increase the effectiveness of blocking attack traffic.*

Анотація *– В роботі запропоновано метод безпечної маршрутизації, що враховує параметри мультифрактальності трафіка та агрегований критерій якості виявлення атак в інфокомунікаційних мережах. Даний метод базується на особливій процедурі розрахунку вартості маршрутів з подальшим використанням цих даних при виборі найкоротших шляхів. В роботі проведено експеримент з аналізу ефективності запропонованого методу в умовах мультифрактального трафіка і наявності трафіка атак. Результати дослідження показали, що використання запропонованого методу дозволяє зменшити затримку і джитер пакетів у мережі, а також підвищити ефективність блокування трафіка атак.*

Аннотация *– В работе предложен метод безопасной маршрутизации, учитывающий параметры мультифрактальности трафика и агрегированный критерий качества обнаружения атак в инфокоммуникационных сетях. Данный метод базируется на особой процедуре расчёта стоимости маршрутов с дальнейшим использованием этих данных при выборе кратчайших маршрутов. В работе проведён эксперимент по анализу эффективности предложенного метода в условиях мультифрактального трафика и наличии трафика атак. Результаты исследования показали, что использование предлагаемого метода позволяет уменьшить задержку и джиттер пакетов в сети, а также повысить эффективность блокирования трафика атак.*

Вступ

Інфокомунікаційна мережа являє собою складну і дорогу систему, яка відіграє важливу роль у сучасному суспільстві та обслуговує велику кількість користувачів. Як під час створення, так і під час експлуатації ключовою задачею є забезпечення ефективного функціонування інфокомунікаційної мережі. Основними характеристиками

ефективності є продуктивність, надійність і безпека [1]. При забезпеченні продуктивності мережі використовуються методи забезпечення якості обслуговування (Quality of Service, QoS), які підтримують стабільну роботу сучасних сервісів: IP-телефонії, відео- і радіомовлення, інтерактивного дистанційного навчання тощо. Методи забезпечення QoS спрямовані на покращення робочих характеристик, надійності мережі, зменшення затримок і втрат пакетів у періоди перевантаження мережі [2, 3]. До основних причин зниження рівня якості обслуговування відноситься різнорідність мережних ресурсів та їх обмеженість при передачі трафіку, що призводить до виникнення вузьких місць у мережі. Це може бути виражено у тимчасовому зниженні швидкості передачі пакетів, у збільшені затримок, джитеру та втрат пакетів через перевантаження мережі. В цілому використання методів забезпечення QoS спрямовано на запобігання негативним наслідкам тимчасових перевантажень, що виникають у мережах з комутацією пакетів.

Теоретичні та експериментальні дослідження, проведені в останні десятиліття, показують, що трафік у інфокомунікаційних мультисервісних мережах має самоподібні властивості [1-5]. Пакети самоподібного трафіка, який має значні викиди, зазнають великих затримок і втрат, навіть якщо загальна інтенсивність всіх потоків далека від максимально допустимих значень. Крім того, великою проблемою для постачальників послуг є забезпечення QoS за умови наявності лавиноподібного трафіка вторгнень. Цей тип поведінки пов'язаний з такими загрозами, як розподілені атаки на відмову в обслуговуванні (Distributed Denial-of-Service attack, DDoS), інтернет-черв'яки, віруси, спам електронної пошти тощо. Обсяг трафіка, який генерується для проведення атак і через зараження, може порушити функціонування мережі та створити додатковий ризик для мережних пристроїв (маршрутизаторів, комутаторів). Безпека стає критично важливою характеристикою всіх сервісів і грає вирішальну роль у прибутковості постачальників послуг [6].

Завдання забезпечення безпеки мережі визначається тим, яким чином постачальник може ефективно пропонувати більш широкий перелік та обсяг послуг з більш високими показниками ефективності, ступенем керованості трафіком та ресурсами мережі [6]. Тому метою даної роботи є розробка методу безпечної маршрутизації, який заснований на врахуванні мультифрактальних властивостей трафіку та виявленні вторгнень для зменшення затримки пакетів у мережі при передачі легітимного трафіку за найкоротшими шляхами.

I. Самоподібні та мультифрактальні властивості трафіка

В інфокомунікаційних мережах трафік може розглядатися як випадковий процес. Прикладом такого випадкового процесу (який використовується у цій роботі) є залежність інтенсивності трафіку від часу. Таким чином, трафік, який можна описати самоподібним випадковим процесом, називається самоподібним.

Стохастичний процес безперервного часу $X(t)$ є самоподібним з параметром H, якщо процес $a^{-H}X(at)$, де a – константа, описується тими ж законами скінченновимірних розподілів, що і $X(t)$:

$$Law\{a^{-H}X(\mathrm{a}\,t)\} = Law\{X(t)\}, \forall\,\mathrm{a} > 0,$$

де параметр H, $0 < H < 1$ представляє ступінь самоподібності процесу і називається параметром Херста. Це означає, що якщо часовий ряд протягом якогось часу зростав (убував), то з імовірністю, близькою до показника Херста, ряд збереже цю тенденцію протягом аналогічного проміжку часу [7-9]. Для самоподібного випадкового процесу буде справедливим наступний вираз для розрахунку математичного очікування $M\left[\left|X(t)\right|^q\right] = C(q)\cdot t^{qH}$, де $C(q) = \mathrm{M}\left[\left|X(1)\right|^q\right]$, а параметр q приймає дійсні значення.

Мультифрактальний трафік можна визначити як розширення самоподібного трафіка з урахуванням масштабованих властивостей статистичних характеристик другого та більш високого порядків. Для мультифрактальних процесів виконується співвідношення $\mathrm{M}\left[\left|X(t)\right|^q\right] = c(q)\cdot t^{qh(q)}$, де $c(q)$ – деяка детермінована функція; $h(q)$ є узагальненим індексом Херста, який в загальному випадку є нелінійної функцією від q. Значення $h(q)$ при $q = 2$ співпадає зі значенням ступеня самоподібності H.

Мультифрактальний трафік має особливу структуру, яка зберігається в багатьох масштабах: завжди є кілька дуже великих сплесків з відносно невеликим середнім рівнем трафіка. В рамках дослідження, що проводиться, мультифрактальний трафік однозначно описують наступними статистичними параметрами: інтенсивність трафіка λ, коефіцієнт варіації σ_{var}, параметр Херста H і діапазон узагальненого індекса Херста: $\Delta h = h(q_{\min}) - h(q_{\max})$. Для монофрактальних процесів узагальнений індекс Херста не залежить від параметра q: $h(q) = H$, $\Delta h = 0$. Більш велика гетерогенність процесу, великі сплески трафіка призводять до збільшення діапазону Δh. Коефіцієнт варіації σ_{var} можна розглядати як найпростішу кількісну характеристику розподілу хвостів $\sigma_{\mathrm{var}}[X(t)]/M[X(t)]$, де σ – середнє квадратичне відхилення процесу $X(t)$ [9-11].

II. Математичний опис інфокомунікаційної мережі

В загальному випадку до складу інфокомунікаційної мережі входить множина вузлів, які з'єднані між собою каналами зв'язку. Всі вузли мережі підтримують функцію маршрутизації. В кожному граничному вузлі встановлюється детектор системи виявлення вторгнень для перевірки вхідного трафіка на наявність загроз. Всередині мережі один із вузлів є центральним і виконує збір статистичної інформації про стан мережі та характеристики трафіка. На основі цих даних він обчислює необхідні значення параметрів мультифрактальності, рівня загроз, якості виявлення атак тощо та

надсилає цю інформацію на всі вузли мережі. В мережу надходить самоподібний трафік, який у рамках цього дослідження поділяється за класами обслуговування згідно з інформацією, яка міститься у відповідному полі заголовку пакета.

Маршрутизатор містить n вхідних інтерфейсів, на які надходить трафік від суміжних вузлів мережі. При цьому пакети з вхідного інтерфейсу передаються на вихідний інтерфейс згідно з таблицею маршрутизації, обираючи маршрут мінімальної вартості для відповідного класу обслуговування. Для забезпечення розв'язання задачі маршрутизації здійснюється обмін службовою інформацією між маршрутизаторами про стан каналів зв'язку [12, 13].

В загальному випадку трафік, який передається в мережі, може бути атакою або містити шкідливі дані. Ефективність і продуктивність систем виявлення вторгнень оцінюється з використанням параметрів вартості, ступеня використання мережних ресурсів, швидкості виявлення атак [6]. Існують наступні типи систем виявлення вторгнень (СВВ) [11]:

- системи рівня мережі, на які передається трафік з маршрутизатора (Network-based);

- системи рівня хоста, які виявляють зміни на окремо взятому сервері, наприклад аналізуючи логжурнали або мережну активність (Host-based);

- системи, засновані на оцінці вразливостей (Vulnerability-assessment).

В цій роботі розглядається мережна система виявлення вторгнень (Network Intrusion Detection System, NIDS), яка збирає та аналізує трафік, що йде через маршрутизатор, для чого в маршрутизаторі є SPAN порт, з якого трафік перенаправляється в IDS. До складу СВВ входить класифікатор, який за результатами аналізу параметрів трафіка приймає рішення, чи цей трафік є легітимним, чи атакою. В рамках даного дослідження класифікатор був побудований на базі алгоритму Machine Learning [14]. У зв'язку з тим, що класифікатор, який використовується, є прикладом бінарної класифікації (трафік є легітимним чи атакою) в залежності від того, чи пройшла класифікація правильно чи ні, можливі наступні випадки:

- істино позитивне рішення (True Positive, TP) – це випадок, коли трафік, який насправді є атакою, успішно класифікується як атака;

- хибно позитивне рішення (False Positive, FP), коли легітимний трафік класифікується як атака;

- істино негативне рішення (True Negative, TN) – це випадок, коли легітимний трафік правильно класифікується як легітимний;

- хибно негативний (False Negative, FN), коли трафік, який насправді є атакою, помилково класифікується як легітимний.

Чисельність подібних випадків утворюють матрицю помилок класифікації

$$Confusion\ matrix = \begin{bmatrix} TP & FP \\ FN & TN \end{bmatrix}.$$

Якість процедури класифікації вторгнень також можна охарактеризувати точністю та повнотою, де

- точність (precision) показує, яку частку об'єктів, розпізнаних як об'єкти позитивного класу, передбачили правильно $Precision = TP/(TP + FP)$;

- повнота (recall) показує, яку частку об'єктів, які дійсно належать до позитивного класу, передбачили правильно $Recall = TP/(TP + FN)$.

Також можна використовувати агрегований критерій якості виявлення атак

$$F_\beta = (1+\beta^2)TP \Big/ \beta^2(TP+FP)(TP+FN),$$

де $\beta \in (0,\infty)$, при $\beta \to 0$ критерій F_β характеризуватиме точність, при $\beta = 1$ — непараметричну F-міру, при $\beta \to \infty$ – повноту.

Як елементи матриці помилок під час проведення дослідження приймаються відповідні значення вихідних параметрів алгоритму Machine Learning за результатом виконання класифікації, описаного в роботі [14].

Зазвичай в СВВ кількість хибно позитивних виявлень дуже велика, що є основною складністю для побудови цих систем, яка зменшує їх ефективність. А саме, високе значення FP призведе до менш ефективного виявлення, а високе значення FN зробить систему вразливою для вторгнень. Таким чином, для забезпечення необхідної продуктивності системи виявлення вторгнень FP і FN повинні бути мінімізовані при забезпеченні необхідної точності виявлення [13, 14]. Всі відомі підходи, запропоновані для зменшення помилкових спрацьовувань, недостатньо ефективні, оскільки вони орієнтовані тільки на зменшення помилкових спрацьовувань. В ході роботи було використано метод, який описано в [14], що дозволяє одночасно зменшити як FN, так і FP, зберігаючи точність на заданому рівні або навіть збільшуючи її.

IV. Метод безпечної маршрутизації мультифрактального трафіка

Для забезпечення QoS необхідно обирати маршрути на основі класів обслуговування. В той же час різні потоки, які відправляються одному одержувачу, можуть бути направлені різними маршрутами. Крім того, в разі перевантаження або компрометації елементів мережі (вузлів та каналів) маршрути передачі потоків можуть бути змінені [15, 16] за допомогою відповідних алгоритмів та протоколів маршрутизації [11].

Опишемо математичну модель інфокомунікаційної мережі, яка використовується в дослідженні. До складу мережі входить множина вузлів $A = \{a_i\}$, яка з'єднана між собою множиною каналів зв'язку $L = \{l_{ij}\}$, де l_{ij} канал зв'язку між вузлами a_i та a_j, де $a_i, a_j \in A$. До мережі надходить множина потоків $B = \{b_{lk}\}$, де b_{lk} — це потік від вузла a_l до вузла a_k, при $a_l, a_k \in A$. Потоки, що надходять до мережі, поділяються за множиною класів якості обслуговування $Z = \{z_s\}$. Кожний з потоків, який передається в мережі, описується набором параметрів $b_{lk}^s = (a_l, a_k, z_s, \lambda_{lk}^s, H_{lk}^s, \Delta h_{lk}^s, \sigma_{\text{var}lk}^s, F_\beta^s)$, де

λ_{lk}^{s} — це інтенсивність трафіка s-го класу обслуговування, що передається від вузла a_l до вузла a_k; H_{lk}^{s} — це показник Херста для трафіка s-го класу обслуговування, що передається від вузла a_l до вузла a_k; Δh_{lk}^{s} — це діапазон узагальненого індексу Херста трафіка s-го класу обслуговування, що передається від вузла a_l до вузла a_k; $\sigma_{\mathrm{var}}{}_{lk}^{qs}$ — це коефіцієнт варіації трафіка s-го класу обслуговування, що передається від вузла a_l до вузла a_k; F_{β}^{s} —це агрегований критерій якості виявлення атак у трафіку s-го класу обслуговування, що передається від вузла a_l до вузла a_k.

Запропонований у даній статті метод безпечної маршрутизації базується на алгоритмі маршрутизації за станом каналів з модифікацією способу визначення вартості (метрики) маршруту. Для кожного каналу зв'язку l_{ij} між суміжними вузлами a_i та a_j призначається метрика c_{ij}, яка в загальному випадку залежить від надійності та пропускної здатності каналу зв'язку, а також середньої затримки пакетів у цьому каналі. В момент часу t у кожному вузлі мережі a_x визначається множина маршрутів $\Pi_{xk}^{s}(t)=\left\{\pi_{xk,m}^{s}(t)\right\}$ до кожного вузла-одержувача a_k та s-го класу обслуговування, де m – це номер маршруту. Маршрути ранжуються згідно з їхньою вартістю. При цьому вартість кожного маршруту дорівнює сумі метрик каналів зв'язку уздовж цього маршруту $C_{xk,m}^{s}(t)=\sum\limits_{l_{ij}\in\pi_{xk,m}^{s}(t)} c_{ij}(t)$.

У роботах [5-8, 10, 15] показано, що при навантаженні, коли коефіцієнт утилізації каналу $\rho>0,6$, значеннях $H>0,5$ та $\sigma_{\mathrm{var}}\geq 3$ (що приблизно відповідає значенням $\Delta h>1$) або при $H\geq 0,9$, коефіцієнт втрат пакетів становить більше ніж 5-10%. Також слід відмітити, що передача трафіка з більшими значеннями H за умови збереження заданого рівня якості обслуговування вимагає збільшення пропускних здатностей каналів зв'язку мережі. Згадані властивості трафіка необхідно було врахувати в методі, що пропонується, шляхом використання маршрутів з меншою вартістю для передачі потоків з великими значеннями H в той час, як потоки з невеликими значеннями H можуть передаватись маршрутами з більшою вартістю. Наприклад, якщо у вузлі мережі було виявлено, що потік, який передається, з великою ймовірністю містить зловмисний трафік (має мале значення TP), то він згідно з методом, що пропонується, передається за маршрутом з більшою вартістю.

Метод безпечної маршрутизації полягає в періодичному (з періодом ΔT) перерахунку маршрутів з використанням стандартних алгоритмів маршрутизації з модифікованими значеннями вартості маршрутів. При цьому на кожній з ітерацій здійснюються наступні операції:

1. На центральному вузлі здійснюється аналіз трафіка, що надходить до маршрутизатора, в інтервалі $[t-T_0,t)$, де T_0 – тривалість інтервалу.

2. На інтервалі аналізу T_0 розраховуються інтенсивність вхідного трафіку λ_{xk}^s, вибіркове значення функції узагальненого показника Херста $h_{xk}^s(q)$, значення параметра Херста $H_{xk}^s = h_{xk}^s(2)$, діапазон значень узагальненого показника Херста $\Delta h_{xk}^s = h_{xk}^s(q_{\min}) - h_{xk}^s(q_{\max})$, де $q_{\min} = -5, q_{\max} = 5$ та агрегований критерій якості виявлення атак $F_\beta^s = (1+\beta^2)TP^s \Big/ \beta^2(TP^s + FP^s)(TP^s + FN^s)$ для ділянки трафіку на інтервалі $[t - T_0, t)$.

3. Для поточної множини маршрутів $\Pi_{xk}^s(t) = \left\{\pi_{xk,m}^s(t)\right\}$, які існують у мережі, здійснюється розрахунок значень метрик $C_{xk,m}^s(t)$, де $m = 1...m_s$, а m_s – це кількість маршрутів, що використовуються для передачі трафіка s-го класу обслуговування.

4. Для цієї ж множини маршрутів $\left\{\pi_{xk,m}^s(t)\right\}$ через регулярні проміжки часу ΔT оновлюються і розраховуються за наступною формулою поточні значення метрики шляхів $C'^s_{xk,m}(t)$ на основі врахування мультифрактальних властивостей трафіку:

$$C'^s_{xk,m}(t) = \begin{cases} C_{xk,m}^s(t), & H_{xk}^s \geq 0,9 \text{ або } H_{xk}^s > 0,5,\ \sigma_{\text{var}}{}^s_{xk} \geq 3 \text{ або } F_\beta^s > 0,7; \\ C_{xk,m}^s(t) + (H_{xk}^s - 0,5)C_0, & 0,5 < H_{xk}^s < 0,9,\ 1 < \sigma_{\text{var}}{}^s_{xk} < 3 \text{ або } 0,6 < F_\beta^s < 0,7; \\ C_{xk,m}^s(t) + (H_{xk}^s - 0,5)2\sigma_{\text{var}}{}^s_{xk} C_0, & 0,5 < H_{xk}^s < 0,9, \sigma_{\text{var}}{}^s_{xk} \leq 1, \text{ або } 0,5 < F_\beta^s < 0,6; \\ C_{xk,m}^s(t) + C_0, & H_{xk}^s = 0,5 \text{ або } F_\beta^s < 0,5, \end{cases}$$

де значення C_0 обирається мережним адміністратором. Вартість шляху не змінюється, тобто $C'^s_{xk,m}(t) = C_{xk,m}^s(t)$, якщо трафік має значення $H \geq 0,9$, $H_{xk}^s > 0,5,\ \sigma_{\text{var}}{}^s_{xk} \geq 3$ або $F_\beta^s > 0,7$. Якщо $0,5 < H_{xk}^s < 0,9$ та $1 < \sigma_{\text{var}}{}^{qs}_{xk} < 3$ або $0,6 < F_\beta^{qs} < 0,7$, то значення $C'^s_{xk,m}(t)$ збільшується пропорційно до значення показника Херста. Вартість з максимальним значенням $C_{xk,m}^s(t) + C_0$ обчислюється при H=0,5 або $F_\beta^s < 0,5$ для можливості додаткового аналізу трафіка на виявлення вторгнень. У маршрутів, які не використовуються $\left\{\pi_{xk,m}^s(t)\right\}$, $m = m_s + 1 \ldots \left|\Pi_{xk}^s(t)\right|$, вартість не змінюється. Після перерахунку службова інформація про стан та вартість всіх шляхів відправляється на інші маршрутизатори.

5. Розраховані вартості (метрики) маршрутів записуються в таблицю маршрутизації. Далі маршрутизатор використовує ці значення для маршрутизації трафіку у межах кожного класу обслуговування потоків, що надходять до нього.

Основна ідея цього підходу полягає в тому, що введення штрафних доданків призводить до того, що трафік з більшою ймовірністю атаки передається за маршрутом з більшою вартістю. Це є також справедливим для трафіку без властивостей самоподібності (самоподібний трафік передається за маршрутом з низькою вартістю). Якщо трафік з великою ймовірністю відноситься до трафіку атаки та має великі значення ступеня самоподібності, то він буде передаватись за маршрутом з великою вартістю.

V. Імітаційне моделювання методу безпечної маршрутизації

При імітаційному моделюванні проведена перевірка роботи запропонованого методу, для чого були розроблені програмні модулі з використанням Python. В процесі моделювання було згенеровано трафік із заданими фрактальними властивостями з параметрами, що аналогічні реальному трафіку [8, 10]. Також генерувались атаки з властивостями, що аналогічні трафіку реальних атак. Ці атаки додавались до згенерованого трафіка у випадкові моменти часу. Сумарна інтенсивність доданих атак змінювалася від 10% до 40% від загальної інтенсивності трафіку. Це пов'язано з тим, що атаки з інтенсивністю, меншою ніж 10%, слабо впливають на функціонування мережі, а атаки з інтенсивністю, більшою ніж 40%, ідентифікуються з імовірністю, близькою до 1. Інтенсивність трафіка змінювалась від 10 Гбіт/с до 100 Гбіт/с. Імітаційне моделювання проводилось для мереж з різною структурою, кількістю маршрутизаторів, їх зв'язністю, пропускною здатністю каналів, кількістю та характеристиками потоків.

Для наочності розглянемо роботу методу на прикладі мережі, структура якої представлена на рис. 1, що складається з десяти маршрутизаторів $\{a_1, a_{10}\}$ і чотирнадцяти каналів зв'язку. На вхід подавались три потоки інтенсивністю $\lambda_1 = 200$ 1/с, $\lambda_2 = 200$ 1/с, $\lambda_3 = 200$ 1/с. У розривах каналів зв'язку представлено дріб: у чисельнику наведена інтенсивність потоку, що протікає в даному каналі, а в знаменнику – його пропускна здатність (1/с). Під час експерименту вимірювались наступні параметри: коефіцієнт утилізації каналів (ρ), коефіцієнт втрат пакетів, джитер, відсоток заблокованого атакованого трафіку, середня затримка пакетів у мережі. Параметри QoS, узагальнені для всієї мережі (середнє мережне значення), які отримані під час експериментів, наведено у табл. 1.

При використанні запропонованого методу коефіцієнт втрат пакетів самоподібного трафіка вище, ніж при використанні стандартного методу маршрутизації за станом каналів, тому що деякі пакети втрачаються при проходженні за маршрутом з великою вартістю. Збільшення відсотку заблокованого атакованого трафіку пов'язано з ідентифікацією атак, яка здійснювалась вузлами мережної системи виявлення вторгнень. Було також забезпечено зменшення джитеру та коефіцієнту завантаженості ка-

налів зв'язку. Середня за потоками міжкінцева затримка пакетів у мережі збільшується за рахунок перенаправлення потоків для ідентифікації атак. Трафік, який містить вразливості або є атакою, блокується і не передається далі в мережі. Таким чином, отримані дані свідчать про те, що запропонований метод безпечної маршрутизації є ефективним щодо забезпечення безпеки та якості обслуговування в мережі.

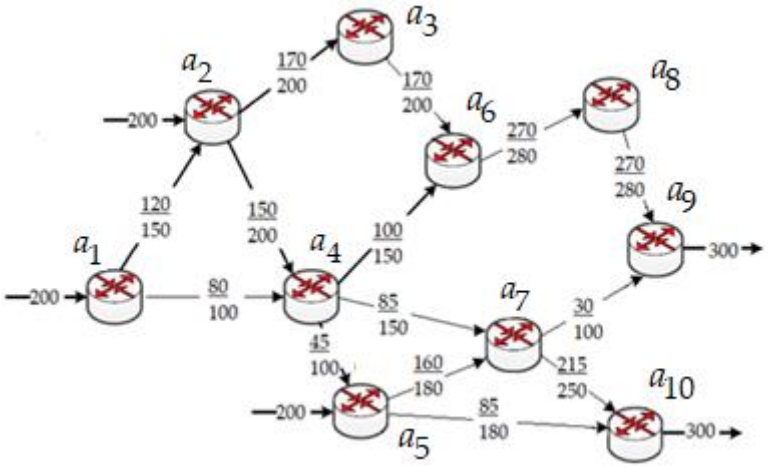

Рис. 1. Порядок маршрутизації потоків на обраній для дослідження структурі інфокомунікаційної мережі

Таблиця 1. Значення параметрів якості обслуговування мережі

Методи	Джитер, мс	Коефіцієнт завантаженості каналів	Втрачені пакети, %	Заблокований трафік (трафік атак), %	Середня затримка пакетів у мережі, мс
Метод безпечної маршрутизації в мережі	15	0,65	1,7	10	88
Стандартний метод маршрутизації за станом каналів	19	0,7	1,5	1,2	67

Висновки

У даній роботі запропоновано метод безпечної маршрутизації в інфокомунікаційній мережі, який засновано на врахуванні самоподібних властивостей трафіку та агрегованого критерію якості виявлення вторгнень. При роботі запропонованого методу легітимний трафік передається за найкоротшими маршрутами, а підозрілий трафік – за більш довгими для проведення більш детального його аналізу. Запропонований метод дозволив зменшити джитер та поліпшити використання каналів при забезпеченні безпеки передачі даних. Загальна кількість втрачених даних і затримка даних у мережі незначно збільшується, але кількість заблокованого атакованого трафіку збільшується у дев'ять разів за рахунок раннього виявлення вторгнень у мережі. Майбутні дослідження планується спрямувати на виявлення впливу та залежності різних типів і рівнів атак на параметри QoS мережі.

Список літератури:

1. *Acharya H. S., Dutta S. R., Bhoi R.* The Impact of self-similarity Network traffic on quality of services (QoS) of Telecommunication Network. International Journal of IT Engineering and Applied Sciences Research (IJIEASR). 2013. Vol. 2. P. 54-60.

2. *Lakhmi P. D., Sanjay K.P.* Fractal Behavior of TCP/IP in Network Traffic. International Journal of Advance Computing Technique and Applications. 2015. Vol. 3, No. 1. P.124-128.

3. *Czarkowski M., Kaczmarek S., Wolff M.* Influence of Self-Similar Traffic Type on Performance of QoS Routing Algorithms. INTL Journal of electronics and telecommunications. 2016. Vol. 62, No. 1. P. 81-87. DOI: https://doi.org/10.1515/eletel-2016-0011.

4. *Shelukhin O. I., Smolskiy S.M., Osin A.V.* Self-Similar Processes in Telecommunications. New York : John Wiley & Sons. 2007. 334 p.

5. *Ageyev D.V., Salah M.T.* Parametric synthesis of overlay networks with self-similar traffic. Telecommunications and Radio Engineering. 2016. Vol. 75, No. 14. P. 1231-1241. DOI: 10.1615/TelecomRadEng.v75.i14.10.

6. *Pietro R. D., Mancini L. V.* Intrusion Detection Systems. Springer Science & Business Media. 2008. 250 p.

7. *Riedi R.H.* Multifractal processes. Long Range Dependence: Theory and Applications. / In eds. Doukhan P., Oppenheim G., Taqqu M.S. Birkhuser. Springer Science & Business Media. 2002. 720 p.

8. *Kirichenko L.O., Radivilova T.A., Kayali E.* Routing calculation value in the MPLS network based on fractal properties of traffic. Automated control systems and automation equipment. 2012. Vol. 161. P. 116-121.

9. *Kirichenko L., Radivilova T., Kayali E.* Modeling telecommunications traffic using the stochastic multifractal cascade process. Problems of Computer Intellectualization / ed. K. Markov, V. Velychko, O. Voloshin. Kiev–Sofia: ITHEA. 2012. P.55–63.

10. *Betker A., Gamrath I., Kosiankowski D., Lange C., Lehmann H., Pfeuffer F., Simon F., Werner A.* Comprehensive topology and traffic model of a nationwide telecommunication network. IEEE/OSA Journal of Optical Communications and Networking. 2014. Vol. 6, No. 11. P. 1038–1047. DOI: 10.1364/JOCN.6.001038

11. *Kirichenko L., Radivilova T., Alghawli A. S.* Mathematical simulation of self-similar network traffic with aimed parameters. Anale. Seria Informatică. 2013. Vol. 11, No. 1. P.17-22.

12. *Medhi D., Ramasamy K.* Network Routing, Second Edition: Algorithms, Protocols, and Architectures. 2nd Edition. The Morgan Kaufmann Series in Networking. Cambridge, MA, USA: Elsevier Inc. 2018. 1018 p.

13. *Donghyuk H., Jong-Moon C.* Self-Similar Traffic End-to-End Delay Minimization Multipath Routing Algorithm. IEEE Communications Letters. 2014. Vol. 18, No. 12. P. 2121-2124. DOI: 10.1109/LCOMM.2014.2362747.

14. *Kirichenko L., Radivilova T., Bulakh V.* Machine Learning in Classification Time Series with Fractal Properties. Data. 2019. Vol. 4(1), No. 5. P.1-13. DOI: https://doi.org/10.3390/data4010005.

15. *Kirichenko L., Radivilova T.* Analysis of network performance under self-similar system loading by computer simulation. Bionics intelligence. 2008. Vol. 1, No. 68. P. 158–160.

16. *Lemeshko O. V., Yeremenko O. S.* Dynamics Analysis of Multipath QoS-Routing Tensor Model with Support of Different Flows Classes. Smart Systems and Technologies (SST): Proceedings of the International Conference, Osijek, Croatia, 12-14 Oct. 2016. IEEE, 2016. P. 225–230. DOI: https://doi.org/10.1109/SST.2016.7765664.