DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-31
УДК 004:02
Снайчук Яромир Любомирович, аспірант
https://orcid.org/0000-0002-9403-824X
Обельовська Квітослава Михайлівна, к.т.н., доцент
https://orcid.org/0000-0002-8714-460X
Національний університет «Львівська політехніка», м. Львів, Україна

АДАПТИВНА МАРШРУТИЗАЦІЯ В OSPF-МЕРЕЖАХ З НЕДОВІРЛИВИМИ ВУЗЛАМИ

Снайчук Я. Л., Обельовська К. М. Адаптивна маршрутизація в ospf-мережах з недовірливими вузлами. У статті розглянуто проблему забезпечення якості обслуговування, QoS (Quality of Service) в мережах, що використовують OSPF (Open Shortest Path First) протокол з урахуванням довіри до вузлів ретрансляторів. Запропоновано підхід до маршрутизації пакетів, що враховує вимоги трафіку до передачі щодо затримок та пропускної здатності з врахуванням наявності у мережевому середовищі недовірливих вузлів. Розроблений на його основі метод дозволяє адаптувати маршрути залежно від типу трафіку, забезпечуючи безпеку для конфіденційних даних та ефективність для даних, що обробляються в реальному часі. Моделювання показало, що у разі присутності у мережі вузлів, що з'єднанні каналами покращеної якості, але низькою довірою, запропонований метод забезпечує доставку трафіку до таких вузлів, проте не використовує їх як транзитні за умови наявності іншого шляху до вузла призначення. Перевагами методу є врахування пропускної здатності та затримок під час маршрутизації та вибір безпечних маршрутів, що не включають недовірливі вузли, якщо такі маршрути існують. Завдяки цьому метод може бути використаним у комп'ютерних мереж на основі протоколу OSPF для створення адаптивних маршрутів.
Ключові слова: OSPF, QoS, недовірливі маршрутизатори, довіра до вузла, багатокритеріальна маршрутизація, безпека мережі.

Snaichuk Y., Obelovska K. Adaptive routing in OSPF networks with distrustful nodes. This article addresses the problem of ensuring QoS (Quality of Service) in networks using the OSPF (Open Shortest Path First) protocol while considering trust in relay nodes. A routing approach is proposed that takes into account traffic transmission requirements regarding delays and bandwidth while considering the presence of untrusted nodes in the network environment. The method developed based on this approach allows route adaptation depending on traffic type, ensuring security for confidential data and efficiency for real-time processed data. Simulation showed that in the case of the presence of nodes in the network connected by enhanced quality channels but with low trust, the proposed method ensures traffic delivery to such nodes but does not use them as transit nodes when alternative paths to the destination node exist. The advantages of the method include consideration of bandwidth and delays during routing and selection of secure routes that do not include untrusted nodes if such routes exist. This allows its use in computer networks based on the OSPF protocol for creating adaptive routes.
Keywords: OSPF, QoS, untrusted routers, node trust, multi-criteria routing, network security.

Постановка наукової проблеми. У сучасних комп'ютерних мережах дедалі більшого значення набуває забезпечення якості обслуговування, QoS. Водночас питання забезпечення безпеки в мережі зберігає пріоритетне значення. Протокол OSPF, який широко застосовується у внутрішньодоменній маршрутизації, традиційно оптимізує маршрути за метрикою найменшої вартості, яка базується на пропускній здатності каналу [1]. Протокол OSPF не передбачає вбудованих механізмів для виявлення або нейтралізації загроз, що виникають унаслідок наявності чи появі в мережі недовірливих вузлів. До недовірливих відносимо вузли, про які відомо, що вони були скомпрометовані або перебувають під контролем зловмисних суб'єктів. Розглянемо детальніше роботу протоколу OSPF. Протокол OSPF базується на алгоритмі оголошення про стан каналу (Link State Advertisements), де кожен маршрутизатор створює повну карту топології мережі, обмінюючись інформацією про мережу з іншими маршрутизаторами. Протокол OSPF використовує алгоритм Дейкстри для знаходження дерева найкоротших шляхів на кожному маршрутизаторі. Це дозволяє побудувати повну карту мережі та визначати оптимальні маршрути. При цьому за основу ваг каналів береться їх пропускна здатність [2]. Проте в умовах зростання трафіку, різноманітності сервісів та загроз інформаційної безпеки виникає потреба у врахуванні різних критеріїв при виборі маршруту. Зокрема, це стосується рівня довіри до мережевих вузлів та здатності маршрутів задовольняти вимоги QoS за такими параметрами, як пропускна здатність, затримка та надійність [3, 4]. Таке розширення вимог призводить до того, що маршрути, обрані за допомогою протоколу OSPF, не завжди відповідають специфічним вимогам додатків реального часу, зокрема при передачі відео чи голосових даних, де критично важлива мінімізація затримок і варіативності часу передачі [5].

Крім того, постійні обміни службовими пакетами та обчислення маршрутів створюють додаткове навантаження на маршрутизатори, що негативно впливає на загальну ефективність передачі даних та може призводити до зміни показників якості обслуговування [6].

Різні типи трафіку мають власні вимоги до якості обслуговування, наприклад, затримки чи пропускної здатності, які необхідно враховувати під час маршрутизації. Це дозволяє забезпечити оптимальне використання мережевих ресурсів та необхідний рівень якості обслуговування для критично важливих даних [7]. В свою чергу, це свідчить про зростання необхідності розробки механізмів всередині традиційних OSPF мереж, які зможуть враховувати вимоги до передачі різних типів трафіку у мережі та забезпечувати гарантії якості обслуговування між кінцевими точками обміну даними [8, 9].

Аналіз останніх досліджень і публікацій. Порівняльний аналіз різних підходів до маршрутизації свідчить, що централізовані моделі, наприклад OpenFlow, здатні за певних умов забезпечувати адаптивну і швидку реакцію на зміни мережі, що дозволяє підтримувати необхідний рівень якості обслуговування [10]. Натомість у децентралізованих моделях підтримка якості обслуговування вимагає інтеграції ізолювання віртуальних ресурсів, динамічного балансування навантаження та захищеної координації між контролерами [11].

У динамічних мережевих середовищах рішення щодо маршрутизації мають адаптуватися до змін трафіку та довірливості вузла. Методи на основі DRL (Deep Reinforced Learning) можуть вирішувати цю задачу через їх здатність навчатися оптимальній політиці маршрутизації на основі даних про трафік у мережі. Наприклад, протокол DQSP (Deep Q-learning Secure Protocol) використовує такі методи як DDPG (Deep Deterministic Policy Gradient), щоб віддавати перевагу маршрутам, які обходять скомпрометовані вузли, забезпечуючи високу пропускну здатність і низьку затримку в мережах SDN-IoT [12]. Подібні стратегії, такі як алгоритм TBPPO (Trust-Based Proximal Policy Optimization), поєднують нейронні мережі та оцінку довіри на основі розбіжностей ймовірностей, щоб під час вибору маршруту врахувати характеристики QoS та забезпечити безпечне з'єднання [12,13].

Одним перспективних підходів є також багатоплощинна маршрутизація, яка розширює концепцію єдиної логічної таблиці маршрутів шляхом створення кількох площин маршрутизації, кожна з яких має власну систему ваг для каналів зв'язку. У схемах багатоплощинної маршрутизації, таких як метод QoS-aware Multi-Plane Routing (Q-MPR), застосовується попереднє планування мережі в автономному режимі для генерації кількох кандидатних площин. Під час роботи кожна нова сесія класифікується за вимогами до QoS і безпеки, після чого призначається до оптимальної площини, яка найбільше відповідає цим критеріям. Це забезпечує гнучкішу стратегію розподілу трафіку, яка адаптується як до перевантажень, так і до ризиків, пов'язаних з довірою, досягаючи вищої пропускної здатності та зменшення втрат пакетів у порівнянні з одноплощинними підходами [14]. Багатоплощинний підхід доцільно застосовувати в масштабних мережах із неоднорідними шаблонами трафіку та змінним рівнем довіри до вузлів, оскільки він дає змогу забезпечити узгодження вимог до продуктивності та безпеки за умов обмеженого централізованого керування.

Поєднання класичних алгоритмів маршрутизації з передовими методами штучного інтелекту відкриває перспективний напрям для покращення якості обслуговування та забезпечення безпеки у мережі. Це створює передумови для розширення функціональних можливостей мереж наступного покоління на основі протоколу OSPF з урахуванням вимог до якості обслуговування та безпеки в умовах зростаючого навантаження на глобальні комунікаційні системи.

Розлянуті підходи до задачі маршрутизації дають змогу поєднати вимоги до якості обслуговування та безпеки мережі. Інтеграція рейтингів довіри у стандартні метрики маршрутизації, застосування адаптивного прийняття рішень на основі DRL, а також використання стійких і багатоплощинних методів оптимізації дозволяють сформувати нову концепцію маршрутизації. Такий підхід орієнтований на забезпечення безпечної передачі даних у присутності недовірливих вузлів, що набуває особливого значення в умовах зростання загроз у мережевому середовищі.

Традиційно протокол OSPF використовує пропускну здатність як метерику каналів зв'язку. Проте існує можливість використання інших метрик якості облуговування. В такому разі для кожної метрики будується власна таблиця маршрутизації та під час маршрутизації відбувається вибір відповідної таблиці на основі вимог до якості обслуговування [7].

Іншим практичним підходом є модифікація класичного алгоритму протоколу OSPF. У версіях алгоритму з урахуванням довіри недовірливий вузол може бути повністю виключеним з початкового списку доступних вузлів для маршрутизації. Тоді маршрути через цей вузол обираються лише за відсутності альтернативних шляхів [15].

Альтернативно маршрутам через недовірливі вузли може призначатися висока вага, таким чином депріорітезуючи такі маршрути, Наприклад, при побудові таблиці маршрутизації можна виключити маршрути через ненадійні вузли, задавши їм нескінченну вартість. Це дозволяє зберігати зв'язок з такими вузлами як із кінцевими точками, але не використовувати їх для транзиту. Такий підхід є легко реалізовуваним і дозволяє підвищити безпеку в уже наявних мережах без суттєвих змін до протоколу [7].

У цьому контексті доцільним є розгляд підходу до маршрутизації, який поєднує врахування параметрів якості обслуговування із механізмами довіри до мережевих вузлів. З метою забезпечення ефективного використання ресурсів мережі та підвищення її стійкості до потенційно шкідливої активності, пропонується інтеграція показників довіри та характеристик якості обслуговування у процес побудови маршрутних таблиць. Такий підхід дозволяє обмежити обсяг передачі трафіку через недовірливі вузли, водночас забезпечуючи дотримання вимог до пропускної здатності та затримки. Інтеграція зазначених критеріїв є передумовою для побудови гнучкіших та безпечніших мережевих рішень, здатних ефективно функціонувати в умовах сучасних загроз.

Виділення невирішених раніше частин загальної проблеми. Проблема врахування якості обслуговування у мережах OSPF є актуальною та потребує комплексного підходу, що поєднує традиційні протоколи маршрутизації з новітніми технологіями управління трафіком та адаптивними методами розподілу ресурсів, щоб задовольнити зростаючі вимоги сучасних мережевих сервісів. Враховуючи це, актуальною є розробка гібридних рішень, здатних адаптувати стандартний функціонал OSPF до сучасних вимог якості обслуговування, забезпечуючи таким чином високу якість обслуговування в умовах сучасних мережевих інфраструктур з високими вимогами щодо продуктивності та стабільності [16].

Мета дослідження: метою дослідження є розробка методу маршрутизації в OSPF-мережах, який враховує параметри якості обслуговування, такі як пропускна здатність, затримка та рівень довіри до мережевих вузлів.

Завдання дослідження. Програмна реалізація нового методу маршрутизації, що будує дерево шляхів від джерела до всіх вузлів у мережі з урахуванням недовірливих вузлів та вимог до якості обслуговування. Частиною завдання є моделювання мережевих топологій з недовірливими вузлами та тестування різних типів трафіку з вимогами до QoS у порівнянні з класичним алгоритмом Дейкстри. Реалізація завдань дозволить продемонструвати практичну цінність методу для реальних OSPF-мереж з недовірливими вузлами.

Основна частина дослідження. Розглянемо запропонований підхід до маршрутизації в OSPF-мережах для вирішення задачі маршрутизації в OSPF-мережах з урахуванням пропускної здатності, затримок та наявності в мережі недовірливих вузлів.

Розглянемо мережу згенеровану з метою моделювання, що складається з маршрутизаторів (вузлів) та каналів зв'язку (ребер). Нехай мережа задається неорієнтованим графом G=(V,E), де V — множина довірливих та недовірливих вузлів, а E — множина ребер між вузлами мережі.

Кожне ребро $e_{ij} \in E$, що з'єднує вузли v_i та v_j, характеризується вектором показників якості обслуговування, що визначається за формулою:

$$w_{ij} = [d_{ij}, b_{ij}], \quad (1)$$

де: d_{ij} — затримка (delay) на каналі *ij;* b_{ij} — пропускна здатність (bandwidth) каналу *ij*.

Окрім цього, кожен вузол може бути довірливим або недовірливим. Вузол вважається недовірливим через підозру на можливу шкідливу діяльність або неналежне виконання своїх функцій у мережі.

Такі вузли можуть визначатися адміністратором мережі, заздалегідь, на основі політик безпеки, типу обладнання, або історії поведінки вузла. Недовірливі вузли при можливості мають бути виключені з множини можливих маршрутів для забепечення безпечного з'єднання. Рішення про їх виключення приймається з врахуванням типу трафіку, що передається. Зокрема, для пакетів, конфіденційність яких є критичною, недовірливі вузли не повинні бути транзитними. Натомість пакети, які не потребують конфіденційного з'єднання, можуть передаватися через такі вузли.

Важливим етапом реалізації запропонованого методу є процес нормування та обчислення ваг ребер графу мережі. Оскільки параметри, що характеризують фізичні якості каналів зв'язку, мають різні шкали, перед агрегацією приведемо їх до інтервалу [0,1].

У випадках, коли нижчі значення показника вважаються кращими (наприклад, затримка), нормалізоване значення обчислюється як різниця між максимальним і поточним значенням, поділена на діапазон між максимальним і мінімальним значеннями:

$$d_{ij}^{*} = \frac{d_{ij} - d_{min}}{d_{max} - d_{min}}, \quad (2)$$

де: d_{ij}^{*} - нормалізоване значення затримки на ребрі e_{ij}; d_{min} та d_{max} – відповідно мінімальне та максимальне значення затримки серед усіх ребер графу.

У випадках, коли вищі значення є кращими (пропускна здатність), нормалізація виконується таким чином, щоб після перетворення вищі нормалізовані значення відповідали кращим умовам. Для цього від одиниці віднімається результат min-max нормалізації значень показника:

$$b_{ij}^{*} = 1 - \frac{b_{ij} - b_{min}}{b_{max} - b_{min}}, \quad (3)$$

де: b_{ij}^{*} - нормалізоване значення пропускної здатності на ребрі e_{ij}; b_{min} та b_{max} – відповідно мінімальне та максимальне значення пропускної здатності серед усіх ребер графу.

Після нормалізації показників якості обслуговування обчислюється агрегована вага ребра як зважена сума:

$$W_{ij} = \alpha \cdot \mathrm{d_{ij}} + \beta \cdot \mathrm{b_{ij}}, \quad (4)$$

де параметри α та β виконують роль коефіцієнтів ваги критеріїв пропускної здатності та затримок відповідно, сума яких має дорівнювати 1.

Значення коефіцієнтів ваг критеріїв можуть варіюватися залежно від класу трафіку, що заданий в полі DSCP (Differentiated Services Code Point) пакету, що маршрутизується. Наприклад, для даних реального часу можна задати високу вагу затримки, а для інших завантажень пріоритизувати пропускну здатність.

Задача полягає у знаходженні маршруту, який одночасно задовольняє критерії якості обслуговування та уникає недовірливих вузлів.

Для розв'язку задачі маршрутизації з врахуванням пропускної здатності, затримок та недовірливих вузлів було розроблено метод маршрутизації, що працює на основі модифікованого алгоритму Дейкстри.

Оптимальний маршрут визначається як шлях з мінімальною агрегованою вагою P_{min}:

$$P_{min} = \min \sum W_{ij}. \quad (5)$$

В залежності від вимог до конфіденційності з'єднання недовірливі вузли можуть використовуватися для трафіку, безпека якого не є важливою. Вони не включаються до множини допустимих вузлів для маршрутизації, якщо тип трафіку вимагає конфіденційного з'єднання. У цьому режимі формується підграф, що складається лише з довірливих вузлів та відповідних ребер, і на його основі визначаються довірливі маршрути з урахуванням вимог якості обслуговування.

Якщо безпека пакетів є важливою, то виконується повторне проходження графа. Воно дозволяє знайти маршрути до вузлів, що знаходяться за недовірливими вузлами, тобто до вузлів, що не з'єднані з відправником жодним довірливим шляхом. У такій ситуації система повторно розглядає граф уже з урахуванням недовірливих вузлів, щоб сформувати маршрути, використовуючи і недовірливі маршрутизатори.

У випадку якщо конфіденційність не є пріорітетом, запропонований підхід працюватиме як класичний алгоритм протоколу OSPF.

Можна виділити наступні випадки, в яких маршрути через недовірливі вузли можуть бути використані:

- якщо не існує жодного маршруту від початковго вузла до вузла призначення, що не включає недовірливі вузли;
- якщо трафік не потребує конфіденційності, а недовірливий шлях забезпечує кращі значення пропускної здатності та затримок порівняно з використанням довірливих маршрутів.

Застосування розглянутого підходу дає можливість забезпечити гнучкість у виборі маршрутів, балансуючи між вимогами до безпеки та ефективністю передачі залежно від типу трафіку.

Для демонстрації запропонованого підходу було реалізовано три сценарії.

Сценарій І. У мережі відсутні недовірливі вузли. Розглянемо зважений граф на Рис. 1, що зображує досліджувану мережу. Мережа складається з 7-ми маршрутизаторів A-G, серед яких немає недовірливих маршрутизаторів. На ребрах графу позначено умовні фізичні величини параметрів, що

характеризують канал і використовуються для визначення ваги каналу. Пропускна здатність позначена літерою B, затримки позначені літерою D. Для визначення агрегованих ваг ребер враховуються метрики якості обслуговування та значення відповідних коефіцієнтів для них відповідно до типу трафіку. На початковому етапі, для некритичного трафіку, вважається, що обидві метрики мають однакову вагу, яка становить 0,5. Значення вагових коефіцієнтів для маршрутних метрик сценарію I, що використовуються на Рис. 1, наведено в Табл. 1.

У початковій конфігурації мережі наявні лише довірливі вузли, тому розглянутий метод будує дерево найкоротших шляхів за аналогією з класичним алгоритмом, за умови що класичний алгоритм використовує нормалізовані значення показників якості обслуговування як ваги ребер графу. Таким чином усі шляхи будуть проходити виключно через довірливі вузли.

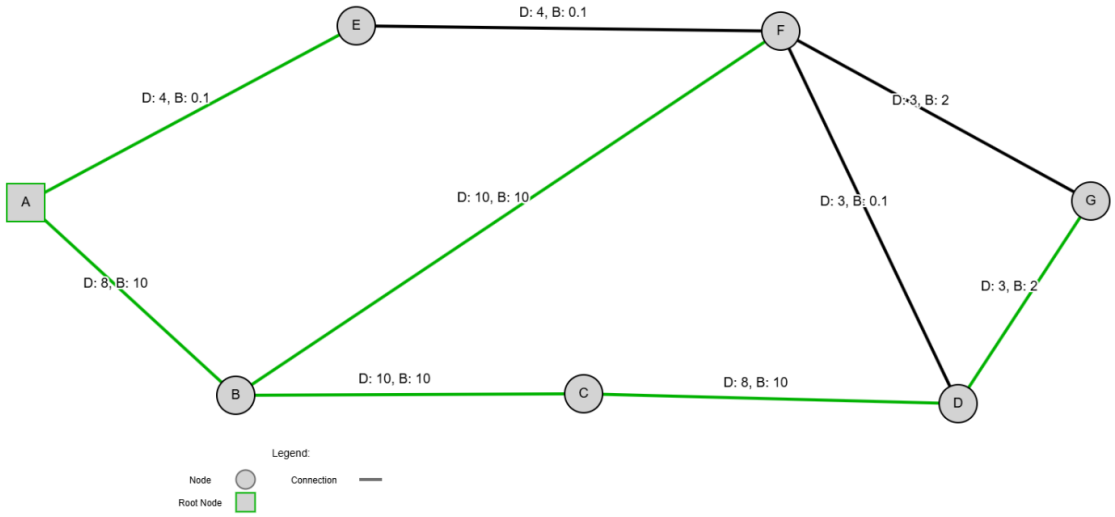

Рис. 1. Сценарій I. Дерево найкоротших шляхів побудоване за допомогою запропонованого підходу для мережі без недовірливих вузлів для α=0,5 і β=0,5

Таблиця 1. Значення вагових коефіцієнтів для метрик у розглянутих сценаріях

Сценарій	Коефіцієнт	Значення
I і II	α	0,5
	β	0,5
III	α	0,75
	β	0,25
IV	α	0,2
	β	0,8

Зв'язки між вузлами, що формують дерево найкоротших шляхів від вузла A до інших вузлів мережі, позначено на рисунку зеленим кольором. Всі інші зв'язки не будуть використовуватися під час маршрутизації пакетів, на рисунку вони позначені чорним кольором.

Сценарій II. Для ілюстрації гнучкості запропонованого підходу розглянемо сценарій II, де до мережі було додано новий вузол H, який є недовірливим (Рис. 2). На рисунку він позначений шестикутником з червоним контуром. Недовірливий вузол з'єднаний з мережею через канали покращеної якості, що в результаті забезпечує їм нижчі значення сумарної ваги каналів. Вагові коефіцієнти метрик якості обслуговування в сценарії II залишаються такими ж як у сценарії I.

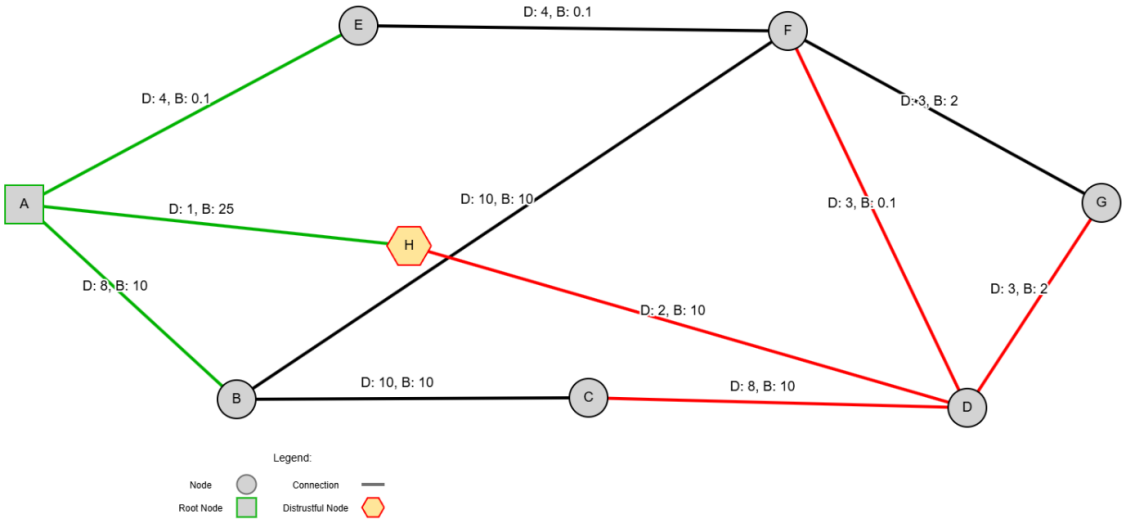

Рис. 2. Сценарій II. Дерево найкоротших шляхів побудоване без урахування критерію довіри до недовірливого вузла для α=0,5 і β=0,5

Без урахування довіри до вузла, найкоротший шлях, наприклад, від вузла A до вузла G проходить через недовірливий вузол H. Це є наслідком того, що канали зв'язку, які сполучають його з мережею мають мінімальні затримки та високу пропускну здатність. Проте розроблений метод відкидає цей маршрут, оскільки вузол H має статус недовірливого. У результаті обирається довший маршрут через довірливі вузли A→B→C→D→G, що гарантує безпечну передачу даних (Рис. 3). Такий механізм дозволяє уникнути ситуацій, коли маршрут з оптимальними характеристиками якості обслуговування проходить через потенційно недовірливі або скомпрометовані вузли, що може призвести до витоку або модифікації інформації.

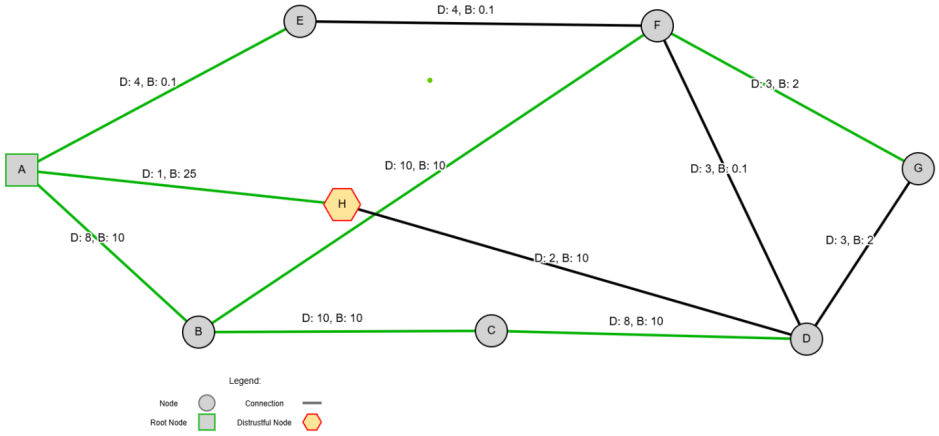

Рис. 3. Сценарій II. Дерево найкоротших шляхів побудоване за допомогою запропонованого методу для мережі з одним недовірливим вузлом для α=0,5 і β=0,5

У випадку, коли трафік не містить конфіденційних даних (наприклад, відеопотік без доступу до персональних відомостей) відповідними налаштуваннями адміністратор або політика маршрутизації може дозволити використання маршруту через вузол H. Для цього атрибут довіри ігнорується. Тоді маршрути через недовірливі вузли розглядаються нарівні з іншими.

Таким чином, запропонований метод підтримує адаптивну маршрутизацію залежно від типу трафіку та дозволяє динамічно балансувати між вимогами до безпеки та якістю обслуговування.

Сценарій III. Цей сценарій передбачає випадок коли передається критичний трафік, що потребує як мінімізації затримки, так і забезпечення конфіденційності. Така ситуація характерна, наприклад, для систем керування в режимі реального часу, безпекових застосувань або служб, що обробляють чутливі дані. У цьому випадку запропонований метод не використовує недовірливі вузли під час формуваня таблиці маршрутизації вузла A, навіть якщо вони забезпечують значно кращі показники якості обслуговування. Алгоритм формує маршрут виключно через довірливі

вузли. Якщо такого шляху не існує, то виконується повторне проходження графа, яке дозволяє сформувати маршрут через недовірливі сегменти, враховуючи ваги каналів та мінімізуючи вагу результуючого шляху. Такий підхід мінімізує можливість передачі критичних даних через вузли, які можуть бути джерелом витоку або компрометації інформації.

Приклад використання запропонованого методу для сценарію III з ваговими коефіцієнтами, що відповідають трафіку систем реального часу зображено на Рис. 4, вагові коефіцієнти для сценарію III наведені у Табл. 1.

Сценарій IV. Сценарій розглядає випадок з некритичними даними, для яких затримка має менший пріоритет, ніж пропускна здатність. Це можуть бути службові повідомлення, потоковий мультимедійний контент або деякі дані моніторингу мережі.

На Рисунку 5 показано ту саму мережу для сценарію IV в умовах маршрутизації трафіку, для якого вибрані змінені вагові коефіцієнти метрик якості обслуговування (Табл. 1). У цьому випадку розроблений метод використав сегмент F-G, що має кращу пропускну здатність. Сегмент F-G було використано для формування найкоротшого шляху з вузла A до вузла G.

Отримані результати демонструють ефективність запропонованого підходу до маршрутизації в OSPF-мережах з урахуванням якості обслуговування та наявності в мережі недовірливих вузлів. Метод передбачає, що інформація про довірливість вузлів визначається адміністративно на етапі конфігурації мережі, що дозволяє всім вузлам мати актуальну інформацію про рівень довіри до інших вузлів у мережі. З метою урахування параметрів якості обслуговування запропонований метод дозволяє адаптувати маршрути до різних типів трафіку, балансуючи між вимогами до пропускної здатності та затримок.

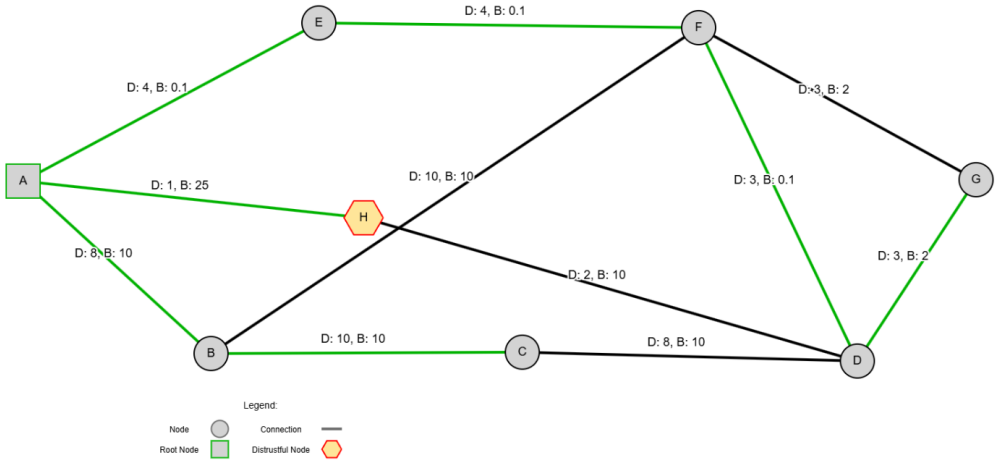

Рис. 4. Сценарій III. Дерево найкоротших шляхів побудоване за допомогою запропонованого методу для мережі з недовірливим вузлом для α=0,75 і β=0,25

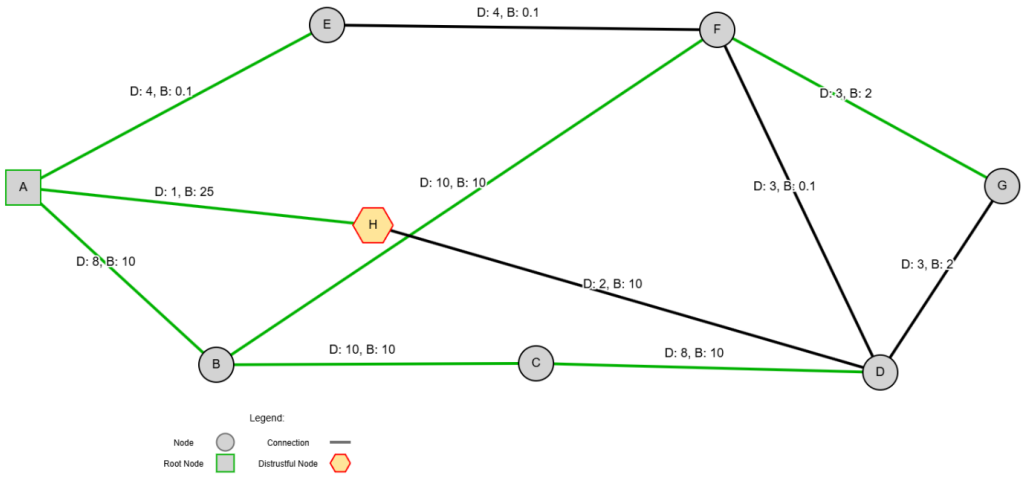

Рис. 5. Сценарій IV. Дерево найкоротших шляхів побудоване за допомогою запропонованого методу для мережі з недовірливим вузлом для α=0,2, і β=0,8

Проведене моделювання на прикладі мережі з одним недовірливими вузлом ілюструє, що у випадку конфіденційного трафіку метод коректно виключає маршрути через недовірливі вузли навіть за наявності у них кращих характеристик. Це дозволяє гарантувати захист даних від потенційного витоку або модифікації, зберігаючи водночас доступність сервісів. При цьому шляхи формуються через довірливі вузли, хоч і з вищою сумарною вартістю. Вища сумарна вартість виступає обґрунтованим компромісом в інтересах забезпечення безпеки.

У випадку некритичного трафіку запропонований метод демонструє гнучкість завдяки можливості використанню змінених вагових коефіцієнтів метрик для конкретного типу трафіку, зокрема з пріоритетом на пропускну здатність. Це дає змогу формувати маршрути з урахуванням доступності ресурсів, покращуючи показники якості обслуговування.

Особливо перспективним є подальше вдосконалення механізмів оцінки довіри шляхом інтеграції даних з різнорідних джерел, зокрема систем виявлення вторгнень, історії взаємодії між вузлами та поведінкового аналізу трафіку. Такий підхід дозволить підвищити точність і динамічність визначення довірливості вузла, адаптуючи маршрутизацію до змін у безпековому середовищі. Крім того, перспективним є впровадження методів машинного навчання для прогнозування ризиків та автоматичного коригування маршрутів у режимі реального часу. Це створює підґрунтя для побудови самонавчальних мережевих систем, здатних динамічно реагувати на нові загрози та оптимізувати трафік з урахуванням змін у структурі мережі та в моделі загроз.

Висновки та перспективи подальших досліджень. Запропонований метод трьохкритеріальної маршрутизації для OSPF-мереж демонструє ефективність у врахуванні пропускної здатності та затримок у середовищі з недовірливими вузлами. Його ключовими перевагами є:

– можливість адаптації до типу трафіку, зокрема ізоляція недовірливих вузлів для критичного трафіку та їх використання для неконфіденційних даних;

– зниження ризику витоку або компрометації даних шляхом автоматичного виключення або обмеження використання недовірливих вузлів;

– маршрути вибираються з урахуванням як технічних, так і безпекових критеріїв.

Подальші дослідження можуть бути спрямовані на динамічне формування оцінок довіри, інтеграцію з системами моніторингу безпеки та використання машинного навчання для прогнозування загроз і оптимізації маршрутів у реальному часі. Запропонований метод може стати основою для застосування нових підходів до маршрутизації.

Список бібліографічного опису:

1. Karamela, Noelia, and Dimitrios A. Karras. "A Comparative Analysis of OSPF and EIGRP Routing Protocol Evaluation." Journal of Transactions in Systems Engineering 1.2 (2023): 73-103.
2. Al-Musawi, Bahaa & Branch, Philip & Hassan, Mohammed & Pokhrel, Shiva. "Identifying OSPF LSA falsification attacks through non-linear analysis." Computer Networks 167 (2020): 107031.
3. Bi, Yuanguo & Han, Guangjie & Lin, Chuan & Peng, Yan & Pu, Huayan & Jia, Yazhou. "Intelligent quality of service aware traffic forwarding for software-defined networking/open shortest path first hybrid industrial internet." IEEE Transactions on Industrial Informatics 16.2 (2019): 1395-1405.
4. Jaron, Alexandre, Andrej Mihailovic, and Abdol-Hamid Aghvami. "Qos-aware multi-plane routing method for OSPF-based IP access networks." Computer Networks 99 (2016): 1-14.
5. Simson, Fransiskus, and Indrastanti R. Widiasari. "Comparative Analysis of Quality of Service Performance of Video Streaming Services Using OSPF and EIGRP Networks." JIKO (Jurnal Informatika dan Komputer) 6.1 (2023).
6. Simson, Fransiskus, and Indrastanti R. Widiasari. "Comparative Analysis of Quality of Service Performance of Video Streaming Services Using OSPF and EIGRP Networks." JIKO (Jurnal Informatika dan Komputer) 6.1 (2023).
7. Дрєєва, Г., Мелешко, Є., Дрєєв, О., Міхав, В. (2022). Програмна імітаційна модель комп'ютерної мережі з фрактальним трафіком для тестування алгоритмів маршрутизації. *Сучасні інформаційні системи*, *6*(4), 11–18. https://doi.org/10.20998/2522-9052.2022.4.02
8. Obelovska, K.; Snaichuk, Y.; Liskevych, O.; Mitoulis, S.-A.; Liskevych, R. Mitigation of Risks Associated with Distrustful Routers in OSPF Networks—An Enhanced Method. Computers 2025, 14, 43. https://doi.org/10.3390/computers14020043
9. Nurhaida, Ida, Desi Ramayanti, and I. Nur. "Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks." Commun. Appl. Electron 7.31 (2019): 12-25.
10. M. Alsaeedi, M. M. Mohamad and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey," in IEEE Access, vol. 7, pp. 107346-107379, 2019, doi: 10.1109/ACCESS.2019.2932422
11. Keshari, S.K., Kansal, V. & Kumar, S. A Systematic Review of Quality of Services (QoS) in Software Defined Networking (SDN). Wireless Pers Commun 116, 2593–2614 (2021). https://doi.org/10.1007/s11277-020-07812-2
12. X. Guo, H. Lin, Z. Li and M. Peng. "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT." IEEE Internet of things journal 7.7 (2019): 6242-6251.

13. Zhang, Y.; Qiu, L.; Xu, Y.; Wang, X.; Wang, S.; Paul, A.; Wu, Z. "Multi-path routing algorithm based on deep reinforcement learning for SDN." Applied Sciences 13.22 (2023): 12520.
14. Jaron, Alexandre, Andrej Mihailovic, and Abdol-Hamid Aghvami. "Qos-aware multi-plane routing method for OSPF-based IP access networks." Computer Networks 99 (2016): 1-14.
15. Kvitoslava Obelovska, Yaromyr Snaichuk, Julius Selecky, Rostyslav Liskevych, Tetiana Valkova. "An Approach Toward Packet Routing in the OSPF-based Network with a Distrustful Router." WSEAS Transactions on Information Science and Applications 20 (2023): 432-443.
16. Ostojic, Zivka Slepcevic. Comparative Studies of Link-State Routing Protocols in Wired IP and Ad-Hoc Wireless Network: OSPF, IS-IS and OLSR. Diss. Ph. D. Thesis, University of Applied Sciences Technikum Wien, Vienna, Austria, 2022. Available online: https://resolver. obvsg. at/urn: nbn: at: at-ftw: 1-15934 (accessed on 31 January 2025), 2022.

References:

1. Karamela, Noelia, and Dimitrios A. Karras. "A Comparative Analysis of OSPF and EIGRP Routing Protocol Evaluation." Journal of Transactions in Systems Engineering 1.2 (2023): 73-103.
2. Al-Musawi, Bahaa & Branch, Philip & Hassan, Mohammed & Pokhrel, Shiva. "Identifying OSPF LSA falsification attacks through non-linear analysis." Computer Networks 167 (2020): 107031.
3. Bi, Yuanguo & Han, Guangjie & Lin, Chuan & Peng, Yan & Pu, Huayan & Jia, Yazhou. "Intelligent quality of service aware traffic forwarding for software-defined networking/open shortest path first hybrid industrial internet." IEEE Transactions on Industrial Informatics 16.2 (2019): 1395-1405.
4. Jaron, Alexandre, Andrej Mihailovic, and Abdol-Hamid Aghvami. "Qos-aware multi-plane routing method for OSPF-based IP access networks." Computer Networks 99 (2016): 1-14.
5. Simson, Fransiskus, and Indrastanti R. Widiasari. "Comparative Analysis of Quality of Service Performance of Video Streaming Services Using OSPF and EIGRP Networks." JIKO (Jurnal Informatika dan Komputer) 6.1 (2023).
6. Simson, Fransiskus, and Indrastanti R. Widiasari. "Comparative Analysis of Quality of Service Performance of Video Streaming Services Using OSPF and EIGRP Networks." JIKO (Jurnal Informatika dan Komputer) 6.1 (2023).
7. Drieieva, H., Meleshko, Y., Drieiev, O., Mikhav, V. (2022). Computer simulation model of a computer network with fractal traffic for testing routing algorithms. Advanced Information Systems, 6(4), 11–18. https://doi.org/10.20998/2522-9052.2022.4.02
8. Obelovska, K.; Snaichuk, Y.; Liskevych, O.; Mitoulis, S.-A.; Liskevych, R. Mitigation of Risks Associated with Distrustful Routers in OSPF Networks—An Enhanced Method. Computers 2025, 14, 43. https://doi.org/10.3390/computers14020043
9. Nurhaida, Ida, Desi Ramayanti, and I. Nur. "Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks." Commun. Appl. Electron 7.31 (2019): 12-25.
10. M. Alsaeedi, M. M. Mohamad and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey," in IEEE Access, vol. 7, pp. 107346-107379, 2019, doi: 10.1109/ACCESS.2019.2932422
11. Keshari, S.K., Kansal, V. & Kumar, S. A Systematic Review of Quality of Services (QoS) in Software Defined Networking (SDN). Wireless Pers Commun 116, 2593–2614 (2021). https://doi.org/10.1007/s11277-020-07812-2
12. X. Guo, H. Lin, Z. Li and M. Peng. "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT." IEEE Internet of things journal 7.7 (2019): 6242-6251.
13. Zhang, Y.; Qiu, L.; Xu, Y.; Wang, X.; Wang, S.; Paul, A.; Wu, Z. "Multi-path routing algorithm based on deep reinforcement learning for SDN." Applied Sciences 13.22 (2023): 12520.
14. Jaron, Alexandre, Andrej Mihailovic, and Abdol-Hamid Aghvami. "Qos-aware multi-plane routing method for OSPF-based IP access networks." Computer Networks 99 (2016): 1-14.
15. Kvitoslava Obelovska, Yaromyr Snaichuk, Julius Selecky, Rostyslav Liskevych, Tetiana Valkova. "An Approach Toward Packet Routing in the OSPF-based Network with a Distrustful Router." WSEAS Transactions on Information Science and Applications 20 (2023): 432-443.
16. Ostojic, Zivka Slepcevic. Comparative Studies of Link-State Routing Protocols in Wired IP and Ad-Hoc Wireless Network: OSPF, IS-IS and OLSR. Diss. Ph. D. Thesis, University of Applied Sciences Technikum Wien, Vienna, Austria, 2022. Available online: https://resolver. obvsg. at/urn: nbn: at: at-ftw: 1-15934 (accessed on 31 January 2025), 2022.