https://doi.org/10.31891/2307-5732-2026-365-3
УДК 004.056.53(045)

БІЛОУС ВІТАЛІЙ
Вінницький національний технічний університет
https://orcid.org/0009-0001-2350-1583
e-mail: pydev@ukr.net
КАТАЄВ ВІТАЛІЙ
Вінницький національний технічний університет
https://orcid.org/0000-0002-7458-7807
e-mail: kataev@vntu.net
ГУМЕНЮК В'ЯЧЕСЛАВ
Вінницький національний технічний університет
https://orcid.org/0009-0004-0348-7616
e-mail: hvv@vntu.edu.ua
ШЕНДЕРУК ОЛЕГ
Вінницький національний технічний університет
https://orcid.org/0009-0000-5218-4137
e-mail: shenderuk2002@ukr.net

БАГАТОРІВНЕВА ПРОКСІ-СЕРВЕРНА СИСТЕМА З ДИНАМІЧНИМ КОНТРОЛЕМ МАРШРУТИЗАЦІЇ ТА ГІБРИДНИМ СТОХАСТИЧНИМ ПЕРЕМІШУВАННЯМ МАРШРУТІВ

У статті описано підхід до побудови багаторівневої проксі-системи з динамічним маршрутизаційним контролем, котра орієнтована на підвищення рівня захищеності інформаційних ресурсів та оптимізацію керування мережевим трафіком. Запропонована авторами архітектура ґрунтується на ієрархічній організації проксі-серверів, у межах якої кожен рівень виконує спеціалізовані функції. Зокрема, реалізується первинна фільтрація з'єднань, поглиблений аналіз безпеки, кешування даних, контроль доступу та фінальна маршрутизація. Такий підхід забезпечує поетапну обробку мережевих запитів, підвищує надійність системи та сприяє її масштабованості за умов зростання навантаження.

Особливу увагу приділено моделі динамічної маршрутизації, що реалізується на основі гібридного стохастичного алгоритму. Запропонований алгоритм поєднує ймовірнісний вибір маршрутів із детермінованим аналізом історичних характеристик трафіку та стану мережі. Стохастичний компонент дозволяє знизити передбачуваність маршрутів і мінімізувати ризик локальних перевантажень, тоді як детермінований складник забезпечує стабільність функціонування та підвищує ефективність використання мережевих ресурсів. Алгоритм враховує поточні параметри мережі, зокрема затримки, пропускну здатність і рівень завантаженості серверів, та здійснює динамічне коригування вагових коефіцієнтів маршрутів у режимі реального часу. Це забезпечує адаптивне балансування навантаження та автоматичне перенаправлення трафіку у разі виникнення перевантажень або змін топології мережі.

Запропонований підхід підвищує стійкість багаторівневих проксі-систем до мережевих атак і забезпечує стабільну передачу даних в умовах інтенсивного та змінного трафіку. Отримані результати свідчать про доцільність використання гібридних стохастичних методів маршрутизації в сучасних інформаційних мережах.

Ключові слова: *багаторівнева проксі-система; динамічна маршрутизація; гібридний стохастичний алгоритм; балансування мережевого трафіку; інформаційна безпека; адаптивні мережі.*

BILOUS VITALII, KATAIEV VITALII, HUMENIUK VIACHESLAV, SHENDERUK OLEG
Vinnytsia National Technical University

MULTI-LEVEL PROXY SERVER SYSTEM WITH DYNAMIC ROUTING CONTROL AND HYBRID STOCHASTIC ROUTE SHUFFLING

The article considers an approach to designing a multi-tiered proxy system with dynamic routing control, aimed at enhancing information resource security and optimizing network traffic management. The proposed architecture is based on a hierarchical organization of proxy servers, where each tier performs specialized functions. Specifically, it implements initial connection filtering, deep security analysis, data caching, access control, and final routing. This approach provides phased processing of network requests, increases system reliability, and promotes its scalability under conditions of increasing load.

Particular attention is paid to the dynamic routing model, which is implemented based on a hybrid stochastic algorithm. The proposed algorithm combines probabilistic route selection with deterministic analysis of historical traffic characteristics and network status. The stochastic component allows reducing the predictability of routes and minimizing the risk of local overloads, while the deterministic component ensures stable operation and increases the efficiency of using network resources.

The algorithm takes into account current network parameters, including latency, bandwidth, and server load, and dynamically adjusts route weights in real time. This provides adaptive load balancing and automatic traffic redirection in the event of overloads or changes in network topology.

The proposed approach increases the resistance of multi-level proxy systems to network attacks and ensures stable data transmission in conditions of intensive and variable traffic. The results obtained indicate the feasibility of using hybrid stochastic routing methods in modern information networks.

Keywords: *multi-level proxy system; dynamic routing; hybrid stochastic algorithm; network traffic balancing; information security; adaptive networks.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий розвиток інформаційних технологій в усіх сферах життя людей, а також зростанням обсягів трафіку, що циркулює в мережі формує задачу підвищення вимог до ефективності та надійності сучасних комп'ютерних систем. Разом з цим змінюється характер загроз, зокрема, мережеві атаки стають дедалі складнішими, збільшується кількість DDoS-атак, що спрямовані на інфраструктурні вузли, частішими стають спроби несанкціонованого доступу до ресурсів. За таких умов традиційні підходи до забезпечення мережевої безпеки не завжди дають очікуваний результат. Аналогічна проблема виникає із статичними алгоритмами маршрутизації, котрі в більшості випадків не враховують поточний стан мережі, а також рівень завантаженості її компонентів, що непрактично в реальному застосуванні.

Варто звернути увагу також на багаторівневі проксі-системи, що широко застосовуються для фільтрації трафіку, контролю доступу та організації взаємодії між користувачами й сервісами. В таких ситуаціях наведена проблема явно прослідковується, оскільки використання фіксованих маршрутів часто призводить до локальних перевантажень, зниження продуктивності, а також підвищує вразливість системи до цільових атак.

Таким чином, актуальним практичним завданням для подальшої роботи є необхідність розробки адаптивного підходу в динамічній маршрутизації. Очікується, що такий підхід забезпечить балансування трафіку, підвищить стійкість до атак і, водночас, дозволить ефективніше використовувати мережеві ресурси. Такі результати, у свою чергу, є корисними для проєктування сучасних захищених мережевих інфраструктур, які працюють в умовах інтенсивного та нестабільного трафіку.

Аналіз досліджень та публікацій

Сьогодні актуальним є питання захисту комп'ютерних мереж, оскільки з часом кількість можливих загроз та важливість потенційних негативних наслідків лише зростає. Рішенням даного питання є постійне вдосконалення та розвиток систем захисту, що спрямовані перш за все на захист даних користувачів та безпечну роботу в мережевому середовищі.

Для більш детального ознайомлення із можливими загрозами та ризиками, що становлять небезпеку для комп'ютерних мереж, проаналізуємо деякі дослідження. За результатами аналізу слід відзначити, що одним із ключових засобів захисту є маршрутизаційний контроль. Зокрема, приділяється увага між доменній маршрутизації та протоколу BGP, оскільки він є вразливим до атак, що орієнтовані на перехоплення маршрутів, витік префіксів і підміну маршрутної інформації. Хоча, незважаючи на це, протокол є широко використовуваним.

Помітна частина досліджень спрямована на застосування криптографічних механізмів захисту маршрутизації. Зокрема, у стандарті BGPsec реалізовано перевірку цілісності AS-шляху на основі цифрових підписів, що дозволяє підтверджувати достовірність маршрутних оголошень і запобігати їх несанкціонованій зміні. Далі цей підхід був розвинений через впровадження інфраструктури RPKI та механізмів валідації походження маршрутів (Route Origin Validation), які забезпечують перевірку відповідності оголошених префіксів авторизованим джерелам [1, 2]. Паралельно розвивається напрям, пов'язаний з управлінням політиками маршрутизації та фільтрацією маршрутів. У низці робіт і стандартів підкреслюється, що використання списків дозволених префіксів, фільтрація AS-path і обмеження маршрутних політик на практиці суттєво знижують ризики як цілеспрямованих атак, так і конфігураційних помилок [3]. Водночас у звітах європейських експертних органів зазначається, що відсутність навіть базових механізмів фільтрації досі залишається однією з причин масштабних інцидентів маршрутизації в мережі Інтернет [4].

Окремо слід відзначити підходи до захисту BGP-сесій. Сучасні стандарти пропонують, зокрема, використання механізму TCP-AO, який забезпечує захист транспортного рівня під час обміну маршрутною інформацією та дозволяє протидіяти атакам, пов'язаним із підміною з'єднання або відмовою в обслуговуванні [5]. Це позитивно впливає на стабільність процесів маршрутизації та знижує ризик порушення роботи мережі.

Ще один важливий напрям – моніторинг і виявлення аномалій маршрутизації. Аналіз змін топології, нетипових AS-шляхів або різких змін у префіксах дає змогу оперативно виявляти атаки та обмежувати їх вплив [6]. У цьому контексті все активніше застосовуються методи машинного та глибокого навчання, які дозволяють автоматизувати обробку великих обсягів маршрутних даних і підвищити точність виявлення складних атак [7-8].

У сучасних дослідженнях окрему увагу також приділяють архітектурним підходам до реалізації маршрутизаційного контролю, зокрема із застосуванням програмно-керованих мереж (SDN). Використання SDN-контролерів дозволяє централізовано керувати маршрутами, що, на практиці, спрощує впровадження політик безпеки, дає змогу ізолювати підозрілі або небезпечні маршрути та загалом підвищує рівень керованості мережевої інфраструктури [9-10].

Узагальнюючи результати аналізу наукових праць, можна відзначити, що сучасні підходи до підвищення захищеності мереж інформаційних систем зазвичай базуються не на одному рішенні, а на їх поєднанні. Йдеться, зокрема, про криптографічний захист маршрутизації, механізми валідації походження маршрутів, застосування політик і фільтрації, захист BGP-сесій, а також засоби моніторингу аномалій. Окремо варто відзначити використання інтелектуальних методів і програмно-керованих підходів, які розширюють можливості контролю мережі. Саме комплексне застосування таких рішень дозволяє підвищити стійкість мереж до сучасних маршрутних атак.

Водночас, попри значну кількість наукових результатів у цій сфері, проблему не можна вважати повністю вирішеною. Сучасні кіберзагрози відрізняються складністю та різноманітністю, що на практиці

дозволяє зловмисникам обходити навіть досить ефективні механізми захисту. За таких умов система інформаційної безпеки має бути не просто надійною, а й адаптивною – здатною швидко реагувати на зміни у загрозовому середовищі.

Саме з цієї причини в даній роботі пропонується підхід до підвищення захищеності інформаційних систем, зокрема комп'ютерних мереж, який базується на використанні сукупності взаємопов'язаних проксі-серверів із динамічною маршрутизацією та гібридним стохастичним перемішуванням маршрутів.

Формулювання цілей статті

Метою роботи є розробка та обґрунтування комплексного підходу, що базується на використанні групи взаємодіючих проксі-серверів із механізмами динамічної маршрутизації та гібридного стохастичного перемішування маршрутів. Такий підхід передбачає підвищення рівня захищеності комп'ютерних мереж інформаційних систем.

Виклад основного матеріалу

В даній роботі авторами пропонується багаторівнева архітектура проксі-серверів. Підхід ґрунтується на механізмах динамічного маршрутизаційного контролю та є інтегрованим рішенням, що дозволяє підвищити рівень захисту інформаційних ресурсів і оптимізувати керування мережевим трафіком.

Опишемо запропоновану архітектуру, структура якої наведена на діаграмі (рис. 1). Відповідно до наведеної структури, в системі буде забезпечена послідовна обробка мережевого трафіку на кожному етапі. Це забезпечить адаптованість до динамічних змін мережевого середовища, а також дозволить досягти оптимального балансу між навантаженням на продуктивністю.

Передбачається, що така система має логічну послідовність та відповідає класичним моделям secure proxy та service chaining, а також є сумісною з сучасними підходами Zero Trust / defense-in-depth. Окрім того, архітектура охоплює декілька ієрархічних рівнів проксі-серверів, де кожен виконує певні функції. Такими функціями є фільтрація, аналіз, маршрутизація, кешування та контроль доступу. Як наслідок, такій системі буде властива стійкість до значних навантажень, підвищена захищеність і надійний фунціонал.

Опишемо більш детальніше запропонований авторами підхід. Весь зовнішній трафік спочатку потрапляє у вхідний вузол. На цьому етапі виконується базова перевірка запитів: аналізуються IP-адреси, типи протоколів, окремі поля заголовків пакетів і джерело звернення. Повноцінної глибокої інспекції тут немає, але цього достатньо, щоб відсіяти частину небажаних або потенційно загрозливих з'єднань ще на початку. Паралельно вузол виконує розподіл трафіку між проксі-серверами першого рівня, щоб уникнути локальних перевантажень.

Далі запити передаються на перший рівень проксі-серверів, де вже відбувається більш детальний аналіз з точки зору безпеки. Рівень складається з кількох паралельних серверів, тому обробка залишається стабільною навіть при зростанні навантаження. Тут використовуються міжмережеві екрани та системи виявлення вторгнень, які аналізують мережеві потоки в режимі реального часу. Основна задача – виявлення аномальної поведінки, характерної, наприклад, для DDoS-атак або розповсюдження шкідливого трафіку.

Після проходження цього етапу запити переходять на другий рівень проксі. Його функції вже більше пов'язані з оптимізацією. Зокрема, застосовується кешування часто використовуваних даних, що дозволяє зменшити кількість повторних звернень до ресурсів. Це знижує загальне навантаження на мережу і, в більшості випадків, скорочує час відповіді. Важливо, що цей рівень має зв'язки як з попереднім, так і з наступним, тому маршрути можуть змінюватися динамічно, без жорсткої прив'язки до одного шляху.

На третьому рівні реалізовано контроль доступу та автентифікацію. Кожен запит проходить перевірку, яка може включати кілька факторів, після чого визначається роль користувача і відповідні права доступу. Це не окремий ізольований етап, а частина загальної логіки обробки, яка впливає на те, які ресурси будуть доступні далі.

Після цього трафік потрапляє у вихідний вузол. Тут виконується фінальна маршрутизація, перевіряється цілісність передаваних даних і здійснюється передача до кінцевого адресата. Також ведеться журналювання запитів, що використовується для подальшого аналізу або аудиту.

Маршрутизація в системі не є фіксованою. Вона залежить від поточного стану мережі: враховується завантаженість серверів, затримки передачі, а також попередні характеристики трафіку. За рахунок цього система може змінювати маршрут навіть для однотипних запитів, якщо умови в мережі змінюються.

Для вибору маршрутів використовується комбінований підхід. Імовірнісна складова дозволяє розподіляти трафік між кількома доступними шляхами, зменшуючи ризик перевантаження окремих вузлів. Водночас детермінована частина базується на накопичених статистичних даних про стан мережі, що допомагає уникати різких коливань у роботі системи.

У структурі передбачено кілька альтернативних маршрутів між вузлами, і вибір наступного вузла відбувається з урахуванням поточного стану мережі. Якщо один із маршрутів перевантажується, трафік може бути автоматично перенаправлений іншим шляхом без зупинки обробки.

Загалом алгоритм маршрутизації побудований як гібридний: поєднує стохастичні та детерміновані підходи. Така схема дозволяє системі адаптуватися до змін мережевого середовища і більш рівномірно розподіляти навантаження, без жорсткої прив'язки до наперед визначених маршрутів.

Далі наведемо та опишемо загальну структуру основних компонентів алгоритму та послідовність його роботи (рис. 2). Це дозволяє краще зрозуміти, як саме реалізується динамічна маршрутизація на практиці. Окремо слід звернути увагу на механізм коригування маршрутів у режимі реального часу. Ймовірнісні ваги не залишаються сталими – вони змінюються залежно від поточного стану мережі. Враховуються такі фактори, як завантаження вузлів або зміни у топології, якщо вони виникають під час роботи системи.

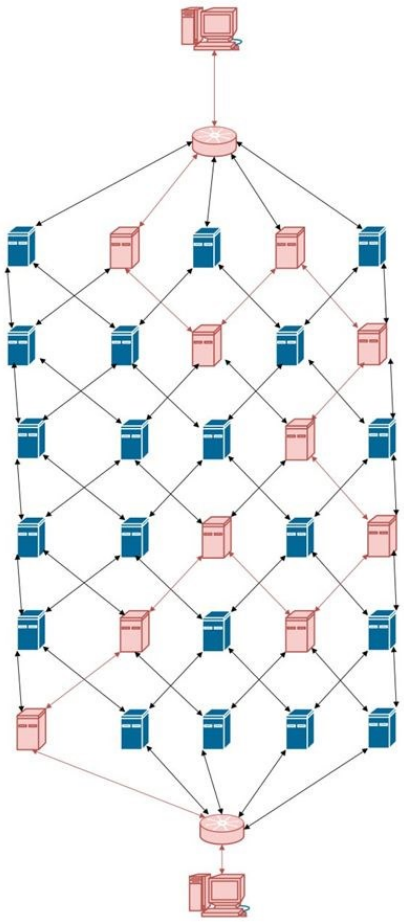

Рис. 1. Діаграма динамічної маршрутизації з використанням гібридного підходу

За рахунок цього проксі-сервери можуть досить швидко реагувати на перевантаження або інші зміни, не чекаючи накопичення критичних проблем. Перебудова маршрутів відбувається поступово, без різких переходів, але достатньо часто, щоб не виникали “вузькі місця”.

У результаті система поводиться стабільніше при нерівномірному навантаженні. Різкі стрибки трафіку не так сильно впливають на загальну роботу, оскільки маршрути не фіксуються жорстко. Це, в свою чергу, дозволяє підтримувати більш надійну передачу даних навіть за умов інтенсивної мережевої активності.

Алгоритм реалізується за такою послідовністю кроків:

Крок 1. Збір метрик про стан мережі.

На початковому етапі відбувається збір відомостей про актуальні параметри функціонування мережі, зокрема значення затримок на окремих маршрутах, інтенсивність трафіку, доступну пропускну спроможність, а також історичні показники завантаження кожного маршруту. Отримана інформація використовується для подальшого аналітичного опрацювання та визначення найбільш доцільного маршруту обслуговування кожного запиту.

Крок 2. Формування множини всіх допустимих маршрутів.

Система здійснює пошук усіх потенційних шляхів передавання даних від вихідного до цільового вузла з урахуванням наявної інфраструктури проксі-серверів. Кожен маршрут описується набором параметрів, зокрема кількістю проміжних вузлів, прогнозованою затримкою та рівнем пропускної здатності. Отримані характеристики використовуються для формування множини допустимих маршрутів, що надалі слугує основою для процедури вибору оптимального шляху.

Крок 3. Формування ймовірнісних ваг для кожного з маршрутів.

Кожному допустимому маршруту надається ймовірнісна вага, що визначається на основі проаналізованих показників. Зокрема, маршрути з нижчими значеннями затримки та більшою пропускною здатністю отримують підвищену ймовірність вибору. Застосування такого підходу забезпечує побудову початкової системи пріоритетів для всіх маршрутів.

Крок 4. Стохастичний вибір маршруту (первинна фаза).

З урахуванням попередньо визначених ймовірнісних ваг система здійснює випадкову селекцію маршруту. Запровадження стохастичного механізму формує контрольований рівень випадковості, що запобігає систематичному використанню одного й того самого шляху передавання даних та зменшує ймовірність його перевантаження. Такий підхід сприяє більш рівномірному розподілу мережевого трафіку між доступними маршрутами.

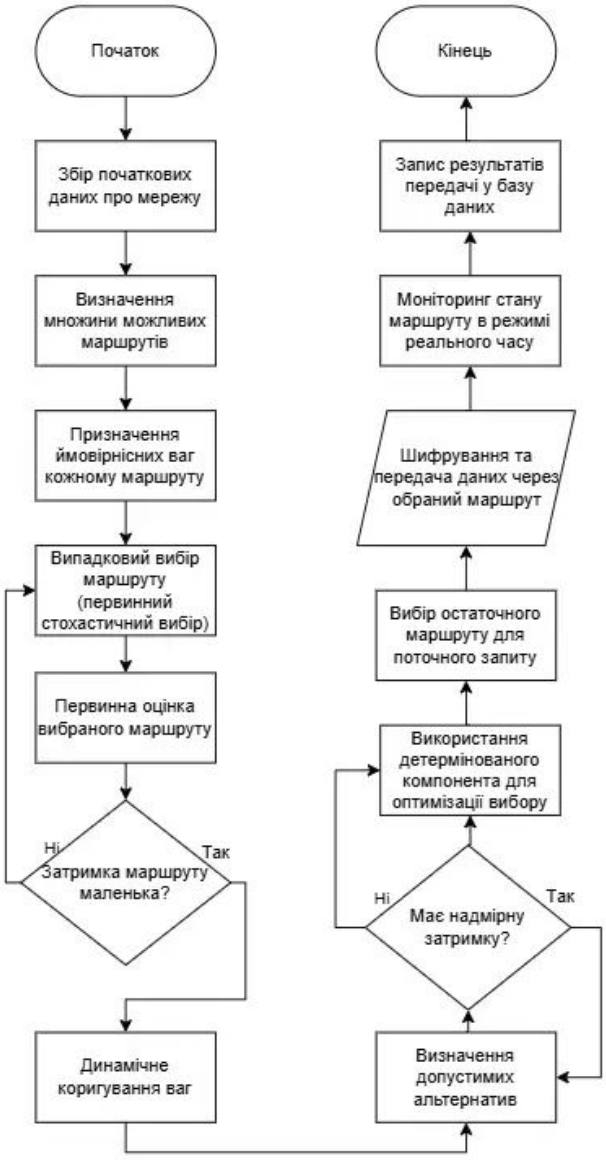

Рис. 2. Схема алгоритму гібридного стохастичного перемішування маршрутів

Крок 5. Початкова оцінка обраного маршруту.

Після визначення маршруту система здійснює його початковий аналіз з метою перевірки відповідності заданим критеріям. У разі, якщо рівень затримки або ступінь завантаженості обраного маршруту перевищують допустимі порогові значення, система ініціює процедуру повторного вибору маршруту.

Крок 6. Оцінювання затримки маршруту.

У разі перевищення затримкою маршруту допустимого рівня алгоритм повертається до кроку 4. Якщо ж значення затримки є незначним, виконується перехід до наступного етапу.

Крок 7. Динамічне коригування вагових коефіцієнтів.

З урахуванням інформації про актуальний стан мережі система здійснює оновлення ймовірнісних коефіцієнтів для кожного маршруту. У разі виявлення ознак перевантаження окремого маршруту його вага зменшується, що відповідно скорочує ймовірність його подальшого вибору. Такий механізм динамічного коригування забезпечує в реальному часі більш ефективну оптимізацію маршрутизації.

Крок 8. Формування набору допустимих альтернатив.

У разі, якщо вибраний маршрут характеризується перевищенням рівня завантаженості або значними затримками, система здійснює відбір альтернативних маршрутів із тієї самої множини. Такий підхід дозволяє виконувати перенаправлення трафіку на менш навантажені шляхи, що сприяє підтриманню стабільної роботи та належного рівня продуктивності системи.

Крок 9. Оцінювання наявності затримки.

У разі виявлення затримки алгоритм повертається до попереднього етапу коригування маршруту (крок 8). За відсутності затримок процес переходить до наступного кроку алгоритму.

Крок 10. Залучення детермінованого компонента для оптимального вибору.

Алгоритм, користуючись детермінованим компонентом, здійснює аналіз накопичених історичних даних щодо раніше використаних маршрутів і на цій основі визначає найбільш ефективні варіанти. Зокрема, маршрути, які стабільно демонстрували мінімальні затримки, отримують підвищений пріоритет.

Крок 11. Формування остаточного маршруту.

Остаточний вибір маршруту для поточного запиту виконується з урахуванням результатів стохастичного відбору, механізмів динамічного налаштування ваг та детермінованого аналізу накопичених показників. Обраний маршрут характеризується найвищою ймовірністю забезпечення ефективної передачі даних, де затримки і навантаження будуть мінімальними.

Крок 12. Шифрування та передавання даних обраним маршрутом.

Передавання інформації здійснюється через визначений маршрут із застосуванням криптографічного захисту. Для забезпечення конфіденційності та цілісності даних використовуються протоколи SSL/TLS, що гарантують безпечну взаємодію між проксі-серверами завдяки шифруванню даних при передачі.

Крок 13. Моніторинг параметрів маршруту.

При передачі даних система відстежує основні характеристики маршруту, зокрема затримку, рівень навантаження та стабільність з'єднання. У випадку виявлення ознак перевантаження здійснюється оперативне коригування маршруту.

Крок 14. Збереження результатів передавання у базі даних.

Всі зібрані параметри маршруту, включаючи показники затримки, пропускної здатності та надійності, фіксуються в базі даних для подальшого використання.

Крок 15. Оцінювання ефективності обраного маршруту.

Виконується аналіз результативності використаного маршруту з подальшим коригуванням імовірнісних ваг. Маршрути з високими показниками ефективності отримують підвищені вагові коефіцієнти, тоді як менш результативні будуть знижені.

Запропонований підхід поєднує два різних способи вибору маршрутів – випадковий і більш визначений. За рахунок цього вдається тримати баланс: з одного боку рівномірно розподіляється навантаження, з іншого – не втрачається стабільність у передачі даних. Стохастична частина зменшує ймовірність появи перевантажених ділянок, тоді як використання накопичених результатів роботи системи дозволяє точніше оцінювати, як поводитиметься мережа далі. Така комбінація виглядає виправданою саме для середовищ, де характеристики трафіку постійно змінюються.

Для підвищення надійності в алгоритмі передбачено постійний моніторинг активних маршрутів під час передавання даних. Якщо окремі ділянки починають перевантажуватись, система не чекає критичної ситуації, а поступово перенаправляє трафік іншими шляхами. Це дозволяє зменшити затримки і уникнути розривів у передачі.

У таких умовах динамічна маршрутизація працює помітно ефективніше, ніж фіксовані схеми, особливо коли навантаження змінюється нерівномірно або непередбачувано.

Контроль маршрутизації реалізований на всіх рівнях системи. При виборі маршрутів враховується не лише поточний стан мережі, але й завантаженість серверів та попередні характеристики трафіку. У підсумку система може адаптивно змінювати напрямок передавання даних і автоматично обходити перевантажені ділянки, не порушуючи загальної стабільності роботи.

Аналізуючи отримані результати дослідження відповідно до запропоновано підходу, слід зазначити, що описане рішення орієнтоване на кілька типових проблем, які виникають у багаторівневих системах маршрутизації. Насамперед, це обмеження статичних алгоритмів. Коли маршрути задаються наперед і фактично не змінюються, система негативно реагує на поточний стан мережі. У результаті частина вузлів може перевантажуватись, тоді як інші залишаються недовикористаними.

Окрема проблема – передбачуваність маршрутів. Якщо шляхи передачі даних стабільні, їх відносно просто ідентифікувати. Це створює додаткові ризики, оскільки такі маршрути можуть цілеспрямовано використовуватись для атак, зокрема DDoS. У випадку, коли маршрути змінюються і вибираються не завжди однаково, така передбачуваність знижується, відповідно ускладнюється і сама атака.

Наступний момент – це балансування навантаження. При інтенсивному трафіку навіть незначна нерівномірність розподілу запитів між серверами може швидко призводити до локальних перевантажень. У запропонованому підході це частково компенсується тим, що під час вибору маршруту враховується поточна завантаженість серверів. Імовірності не є фіксованими, вони коригуються в процесі роботи, тому розподіл трафіку виходить більш рівномірним.

При цьому не ігнорується обчислювальна складність. Частина адаптивних методів дає задовільний результат, проте вимагає значних ресурсів. В запропонованому підході використовується більш спрощена схема: стохастичні механізми поєднуються з відносно нескладними обчисленнями, щоб алгоритм залишався придатним для систем з обмеженими ресурсами.

В основі самого алгоритму лежить кілька базових ідей. Вибір маршруту не є жорстко визначеним – використовується імовірнісна модель. Кожному можливому шляху відповідає певна вага, і саме на її основі формується вибір. Це не означає повну випадковість, але структура трафіку стає менш передбачуваною.

Під час роботи враховуються поточні характеристики мережі (завантаженість вузлів, затримки передачі та інші подібні показники). На основі цих параметрів ваги маршрутів змінюються досить оперативно.

За рахунок цього система підлаштовується під ситуацію, а не працює за наперед заданою схемою.

Окремо використовується аналіз накопичених даних. Маршрути оцінюються з точки зору ефективності, і ті, що раніше показували гірші результати (наприклад, через затримки або перевантаження), отримують менший пріоритет. Це не жорстке виключення, але певне обмеження їх подальшого використання.

У підсумку алгоритм забезпечує динамічне керування маршрутами в межах багаторівневої проксі-системи. Він не фіксує єдиний "кращий" шлях, а постійно перебирає допустимі варіанти з урахуванням поточного стану мережі. Це дозволяє уникати перевантажених ділянок, більш рівномірно розподіляти трафік і зберігати стабільну пропускну здатність навіть при зростанні навантаження.

Таким чином, запропонований підхід поєднує два підходи: стохастичний вибір маршрутів і використання статистики попередньої роботи. Перший додає варіативність і зменшує передбачуваність, другий вирівнює поведінку системи, що унеможливлює її хаотичну роботу.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У роботі розглянуто підхід до побудови багаторівневої проксі-архітектури з динамічним керуванням маршрутизацією. Ідея в тому, щоб поєднати кілька рівнів обробки трафіку з адаптивним балансуванням навантаження і базовими механізмами безпеки. Такий підхід частково відповідає сучасним моделям захисту мереж, зокрема Zero Trust і defense-in-depth, де перевірка і контроль розподілені між різними рівнями системи, а не зосереджені в одному місці.

Архітектура складається з ієрархії проксі-вузлів, і кожен рівень виконує свою функцію. На початковому рівні – це фільтрація запитів і первинне виявлення загроз, далі йде кешування і оптимізація доступу, окремо – автентифікація користувачів, і вже потім фінальна маршрутизація трафіку. У такій структурі простіше розділити навантаження між компонентами, і система в цілому краще витримує пікові навантаження.

Окремо виділяється модель динамічної маршрутизації. Вона побудована як гібридний алгоритм, де є імовірнісний вибір маршрутів і використання історичних даних про роботу мережі. Це не дає системі працювати лише на фіксованих шляхах, але й не робить її повністю випадковою. В результаті маршрути менш передбачувані, а навантаження розподіляється більш рівномірно.

Система може реагувати на зміни стану мережі в реальному часі: перенаправляти трафік, якщо певні ділянки перевантажені, і підлаштовувати вибір маршрутів під поточні умови. При цьому алгоритм не стає занадто складним з точки зору обчислень, що важливо для практичного використання.

У підсумку, слід зазначити, що такий підхід є доцільним для багаторівневих проксі-систем, де одночасно важливі безпека, стабільність і масштабованість. Подальшу роботу з даної теми доцільно продовжувати над тестуванням моделі в реальних умовах і адаптацію до програмно-керованих мереж та хмарних середовищ.

References

1. Mirdita D., Schulmann H., Waidner M. SoK: An Introspective Analysis of RPKI Security. arXiv preprint arXiv:2408.12359v1. 2024. URL: https://doi.org/10.48550/arXiv.2408.12359

2. Schulmann H., Zhao S. Learning to identify conflicts in RPKI. arXiv preprint arXiv:2502.03378. 2025. URL: https://doi.org/10.48550/arXiv.2502.03378

3. Kowalski M., Nowak P., Zieliński K. Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. Computer Networks. 2023. URL: https://doi.org/10.1016/j.comnet.2023.109778

4. Reuter A., Birge-Lee H., Chi A. et al. Securing BGP ASAP: ASPA and other post-ROV defenses. Proceedings of the Network and Distributed System Security (NDSS) Symposium. 2025. URL: https://dx.doi.org/10.14722/ndss.2025.240675

5. Cameron Morris C., Herzberg A, Wang B., Secondo S. BGP-iSec: Improved Security of Internet Routing Against Post-ROV Attacks. Network and Distributed System Security (NDSS) Symposium. 2024, URL: https://dx.doi.org/10.14722/ndss.2024.241035

6. Sermpezis P., Kotronis V., Arakadakis K., & Vakali A. Estimating the Impact of BGP Prefix Hijacking. In 2021 IFIP Networking Conference (IFIP Networking). P. 1-10 IEEE. URL: https://doi.org/10.23919/IFIPNetworking52078.2021.9472813

7. Alshamrani A., Myneni S., Chowdhary A., & Huang D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. In 2019 IEEE Communications Surveys & Tutorials. P. 1851-1877 IEEE. URL: https://doi.org/10.1109/COMST.2019.2891891

8. Shen C., Wang R., Li X., Zhang P., Liu K., Tan L. Border Gateway Protocol Route Leak Detection Technique Based on Graph Features and Machine Learning. Electronics 2024, 13, 4072. URL: https://doi.org/10.3390/electronics13204072

9. Jafarian T., Ghaffari A., Seyfollahi A., Arasteh B. Detecting and mitigating security anomalies in Software-Defined Networking (SDN) using Gradient-Boosted Trees and Floodlight Controller characteristics, Computer Standards & Interfaces, Volume 91, 2025, 103871, ISSN 0920-5489, URL: https://doi.org/10.1016/j.csi.2024.103871

10. Junjie O., Yanai N., Takemura T. APVAS: Reducing memory size of AS_PATH validation by using aggregate signatures. arXiv preprint arXiv.2008.13346. 2020. URL: https://doi.org/10.48550/arXiv.2008.13346