УДК 004.722 DOI https://doi.org/10.35546/kntu2078-4481.2026.2.52

Л. І. ЦВІРКУН
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та комп'ютерної інженерії
Національний технічний університет «Дніпровська політехніка»
ORCID: 0000-0002-5568-5516

І. О. СОБОЛЕВСЬКИЙ
аспірант кафедри інформаційних технологій та комп'ютерної інженерії
Національний технічний університет «Дніпровська політехніка»
ORCID: 0009-0009-0410-7941

АНАЛІЗ МЕТОДІВ МАРШРУТИЗАЦІЇ ДАНИХ У БАГАТОРІВНЕВИХ ТУМАННИХ МЕРЕЖАХ

У даній роботі розглянута організація маршрутизації даних у багаторівневих туманних мережах, які поєднують велику кількість гетерогенних IoT-пристроїв, проміжні туманні вузли та віддалені хмарні центри обробки. Показано, що традиційні підходи до маршрутизації, розроблені переважно для більш простих і відносно статичних мережних структур, не забезпечують потрібного рівня затримки, надійності та енергоефективності в умовах динамічних туманних інфраструктур з нерівномірним розподілом навантаження. На основі опрацьованих джерел узагальнено основні групи методів маршрутизації для туманних мереж: кластерні рішення з використанням SDN, динамічні підходи, що спираються на машинне та глибинне навчання, метаевристичні багатокритеріальні алгоритми, а також інтегровані підходи, у яких маршрутизація розглядається разом із керуванням ресурсами та забезпеченням безпеки. Окрему увагу приділено аналізу критеріїв, які на практиці найбільше впливають на роботу системи, а саме: затримка передавання, надійність каналів зв'язку, енергоспоживання, пропускна здатність та вимоги до якості обслуговування для різних класів трафіку. На прикладі системи екологічного моніторингу показано, як перехід від повністю хмарної архітектури до багаторівневої туманної дозволяє зменшити затримку доставки критичних даних, знизити навантаження на центральну інфраструктуру, підвищити стійкість до відмов окремих компонентів і краще враховувати локальні особливості середовища. На основі порівняльного аналізу сформульовано орієнтовні практичні рекомендації щодо вибору методів маршрутизації для невеликих IoT-систем з помірними вимогами до затримки, великомасштабних розгортань з нерівномірним трафіком та енергообмежених сенсорних мереж, де критичною є тривалість автономної роботи вузлів. Окреслено перспективні напрями подальших досліджень, пов'язані з уніфікацією протоколів взаємодії між рівнями туманної архітектури, інтеграцією механізмів безпеки без суттєвого погіршення продуктивності, а також розробкою ресурсоефективних алгоритмів машинного навчання, які можуть працювати безпосередньо на туманних вузлах із обмеженими обчислювальними та енергетичними можливостями.

Ключові слова: *туманні мережі, маршрутизація даних, IoT-інфраструктура, SDN, машинне навчання, метаевристичні алгоритми.*

L. I. TSVIRKUN
Candidate of Technical Sciences, Associate Professor,
Professor at the Department of Information Technology
and Computer Engineering
Dnipro University of Technology
ORCID: 0000-0002-5568-5516

I. O. SOBOLEVSKYI
Postgraduate Student at the Department of Information Technologies
and Computer Engineering
Dnipro University of Technology
ORCID: 0009-0009-0410-7941

ANALYSIS OF DATA ROUTING METHODS IN MULTI-LEVEL FOG NETWORKS

This paper considers the organization of data routing in multi-level fog networks that combine a large number of heterogeneous IoT devices, intermediate fog nodes, and remote cloud processing centers.

It is shown that traditional routing approaches, originally designed for simpler and mostly static network topologies and focused on a limited set of quality-of-service metrics, fail to provide the required levels of latency, reliability and energy efficiency in highly dynamic fog infrastructures with uneven traffic distribution. Based on a review of recent

 ISSN 2078-4481

research, the paper summarizes the main groups of routing methods used in fog-based IoT systems: cluster-based solutions employing software-defined networking (SDN), dynamic approaches relying on machine and deep learning, metaheuristic multi-objective optimization algorithms, and integrated approaches in which routing is considered together with resource management and security mechanisms. Particular attention is paid to the criteria that have the greatest practical impact on system behaviour, namely end-to-end latency, link reliability, energy consumption, throughput and quality-of-service requirements for different traffic classes. Using an environmental monitoring system as an example, the paper illustrates how a migration from a purely cloud-centric architecture to a multi-tier fog architecture can reduce the latency of critical data delivery, decrease the load on central infrastructure, increase resilience to node and link failures and better reflect local characteristics of the monitored environment. On the basis of the comparative analysis, the paper formulates practical recommendations for choosing routing methods in small-scale IoT systems with moderate latency requirements, large-scale deployments with highly non-uniform traffic patterns and energy-constrained sensor networks, where the lifetime of battery-powered nodes is a key constraint. Finally, several promising directions for further research are outlined, including the unification of interaction protocols between architectural layers, tighter integration of security mechanisms into routing without significant performance degradation, and the design of resource-efficient machine-learning algorithms that can be executed directly on fog nodes with limited computational and energy resources.

Key words: *fog networks, data routing, IoT infrastructure, SDN, machine learning, metaheuristic algorithms.*

Постановка проблеми

Кількість підключених до мережі пристроїв постійно зростає, і разом з цим збільшується обсяг даних, які потрібно передавати та обробляти майже в режимі реального часу. Традиційні алгоритми маршрутизації, розроблені для більш простих мережних структур, часто не дають потрібного результату в туманних мережах. Такі мережі складаються з великої кількості різнорідних вузлів, працюють в умовах обмежених ресурсів і змінної топології, а до якості обслуговування (затримка, втрата пакетів, пропускна здатність) висуваються жорсткі вимоги.

Туманна мережа зазвичай має кілька рівнів: кінцеві IoT-пристрої, проміжні туманні вузли [1] та хмарні центри обробки. Кожен із рівнів має свої обмеження за обчислювальними можливостями та енергоспоживанням, а також різні вимоги до затримки. Для практичних систем − наприклад, розумного міста, автономного транспорту чи промислового моніторингу − важливо не лише доставити дані, а й зробити це в допустимі строки та без перевантаження мережі.

Через це при маршрутизації в туманних мережах потрібно одночасно враховувати кілька різних параметрів. Серед них − затримка, енергоефективність, пропускна здатність, надійність каналів зв'язку та можливість швидко пристосовуватися до змін структури мережі. У цій роботі основна увага зосереджується на порівнянні кластерних, SDN-орієнтованих, методів на основі машинного навчання, метаевристичних та інтегрованих підходів до маршрутизації й на тому, як їх доцільно застосовувати в багаторівневих туманних архітектурах з різними вимогами до затримки, енергоефективності та надійності.

Аналіз останніх досліджень і публікацій

При аналізі сучасних робіт з маршрутизації в туманних IoT-мережах можна виділити кілька основних напрямів. Дослідження зосереджуються на кластерних та SDN-орієнтованих підходах до керування трафіком, методах на основі машинного навчання, метаевристичних алгоритмах багатокритеріальної оптимізації, а також інтегрованих рішеннях, де маршрутизація поєднується з керуванням ресурсами та забезпеченням безпеки.

До першого напряму належать роботи, у яких маршрутизація організовується за допомогою кластеризації та програмно-керованих мереж. Наприклад, у праці [2] запропоновано кластерний двофазний протокол для транспортних мереж, де туманні обчислення поєднуються з SDN-контролером. Експерименти демонструють зростання пропускної здатності та зменшення затримки порівняно зі статичними протоколами, що підтверджує доцільність гібридних підходів у динамічних умовах. Подібні ідеї використання SDN для гнучкого керування маршрутами в туманних мережах розвиваються й в інших роботах [3, 4].

Окремий напрям пов'язаний із застосуванням машинного та глибинного навчання для планування маршрутів і керування ресурсами. У роботі [5] глибокі моделі використовуються для прогнозування оптимальних шляхів у транспортних туманних обчисленнях, що дає змогу зменшити затримку та підвищити стабільність роботи системи в умовах високої мобільності. Подібні підходи зустрічаються й у інших дослідженнях [3, 6, 7], де машинне навчання застосовують для класифікації задач, кластеризації ресурсів і динамічного налаштування пріоритетів трафіку.

Для задач, де одночасно враховується кілька суперечливих критеріїв (затримка, енергоспоживання, надійність, завантаженість каналів), усе частіше застосовуються метаевристичні багатокритеріальні алгоритми. Наприклад, у роботі [8] показано, що такі методи дають змогу знаходити прийнятні компромісні рішення при розгортанні IoT-сервісів у туманних мережах і краще масштабуються порівняно з детерміністичними підходами. Подібні ідеї оптимізації енергоефективної маршрутизації з урахуванням якості обслуговування розвиваються й у роботі [7].

Ще один важливий напрям стосується інтеграції безпеки та маршрутизації. У роботах [6, 9−12] розглядаються моделі автентифікації вузлів, виявлення вторгнень і побудови доказово безпечних протоколів для туманних і транспортних систем. Характерною особливістю цих досліджень є намагання поєднати забезпечення безпеки

з прийнятними затримками та помірними витратами обчислювальних ресурсів.

Узагальнюючи результати аналізу, можна відзначити, що більшість робіт зосереджуються або на окремих аспектах маршрутизації (SDN, машинне навчання, метаевристика, безпека), або на конкретних класах систем (транспортні мережі, VANET, толерантні до затримок IoT-мережі). Водночас питання порівняння цих підходів саме в контексті багаторівневих туманних архітектур та формування практичних рекомендацій щодо вибору методу маршрутизації для різних типів IoT-застосувань опрацьовано менш детально. Саме на цьому аспекті зосереджується дана робота.

Формулювання мети дослідження

Метою дослідження є порівняльний аналіз методів маршрутизації даних у багаторівневих туманних мережах, визначення їх переваг і недоліків та формування практичних рекомендацій щодо вибору методу маршрутизації залежно від типу IoT-застосування і вимог до роботи системи. Для досягнення цієї мети необхідно розв'язати такі завдання:

– узагальнити сучасні підходи до маршрутизації у туманних мережах і виконати їх класифікацію за ключовими ознаками;

– проаналізувати переваги та обмеження основних груп методів маршрутизації в контексті багаторівневих туманних архітектур;

– сформувати орієнтовні практичні рекомендації щодо вибору методів маршрутизації для різних типів IoT-застосувань з урахуванням вимог до затримки, енергоефективності та надійності.

Викладання основного матеріалу дослідження

Для подальшого аналізу методів маршрутизації у багаторівневих туманних мережах необхідно спочатку розглянути їх класифікацію за ключовими ознаками, що дозволить чітко співвіднести конкретні підходи з вимогами практичних сценаріїв використання IoT та обмеженнями інфраструктури.

Перш за все розглянемо наскільки метод маршрутизації здатний підлаштовуватися під зміну умов роботи мережі, а також те, як саме приймаються рішення про вибір маршруту.

За ступенем адаптивності методи маршрутизації можна умовно розділити на статичні та динамічні. Статичні методи працюють з наперед визначеними маршрутами і майже не враховують поточний стан мережі. Вони відносно прості в реалізації, але погано підходять для туманних мереж, де навантаження та топологія змінюються. Динамічні методи, навпаки, орієнтуються на актуальну інформацію про затримку, пропускну здатність і завантаженість вузлів. Завдяки цьому маршрути можна змінювати «на льоту», коли з'являються затори або проблеми з окремими каналами.

Ще один важливий критерій − це спосіб керування маршрутизацією. Тут виділяють три варіанти організації маршрутизації: централізовану, розподілену та гібридну. У централізованих рішеннях основні рішення приймає контролер (наприклад, SDN-контролер), який має загальне уявлення про стан мережі. Це зручно для глобальної оптимізації, але створює залежність від роботи контролера і збільшує вимоги до каналів зв'язку. У розподілених підходах рішення приймаються на рівні окремих вузлів, що підвищує стійкість до відмов і дає кращу масштабованість, але глобально оптимальну конфігурацію знайти складніше. Гібридні методи поєднують обидва підходи: частина рішень приймається централізовано, а частина − локально, що добре підходить для багаторівневих туманних архітектур.

Окремо розглядаються основні критерії оптимізації, які враховують під час вибору маршруту. У туманних мережах зазвичай доводиться враховувати не одну, а кілька цілей: затримку, енергоспоживання, пропускну здатність, надійність каналів, рівень безпеки та витрати на обслуговування. Для систем реального часу першочерговою є затримка, для енергообмежених сенсорних мереж − економія енергії, а для критичних застосувань (наприклад, медичних) на перше місце виходять надійність та захист даних.

Динамічні SDN-орієнтовані методи. Окрему групу становлять методи, у яких динамічна маршрутизація поєднується з можливостями програмно-керованих мереж. У такій архітектурі SDN-контролер отримує інформацію про стан каналів та вузлів і на основі цих даних змінює таблиці маршрутизації. Це дозволяє швидко реагувати на зміну навантаження, появу нових вузлів або відмову існуючих. Якщо контролер тимчасово недоступний, гібридні рішення дають змогу вузлам працювати за локальними правилами, щоб мережа продовжувала функціонувати [2−4].

Методи на основі машинного навчання. Частина сучасних робіт пропонує будувати маршрути з використанням машинного та глибинного навчання. Основна ідея в тому, щоб не просто реагувати на поточний стан мережі, а й намагатися передбачити, як зміниться навантаження в майбутньому. Такі методи аналізують історію трафіку, зміни в топології та інші параметри, а потім пропонують маршрути, які мають бути більш стійкими до типових сценаріїв. У SDN-архітектурах це дозволяє контролеру гнучкіше налаштовувати ваги зв'язків, пріоритети для різних типів трафіку та розподіл запитів між туманними вузлами [3, 5−7]. Для цього використовуються як алгоритми класифікації (розподіл задач за пріоритетами), так і алгоритми кластеризації (групування ресурсів за характеристиками).

Безпека та автентифікація у процесі маршрутизації. У туманних мережах безпека напряму пов'язана з тим, як саме організована маршрутизація. Якщо вузол скомпрометований або канал ненадійний, є ризик втрати чи підміни даних. Тому частина рішень пропонує спочатку переконатися в надійності вузлів (автентифікація), а вже потім допускати їх до участі в маршрутизації. Для цього можуть використовуватися нейронні мережі та інші інтелектуальні методи, які виявляють аномальну поведінку. Додатково застосовуються гібридні оптимізаційні алгоритми, які намагаються знайти баланс між рівнем безпеки, витратами енергії та продуктивністю [6, 9−11].

Метаевристичні підходи та багатокритеріальна оптимізація. У складних туманних IoT-мережах часто доводиться враховувати одразу кілька суперечливих вимог. Класичні алгоритми оптимізації у таких умовах або працюють занадто повільно, або дають не дуже хороші результати. Тому в роботах усе частіше використовують метаевристичні методи: генетичні алгоритми, популяційні підходи та інші підходи до пошуку компромісних рішень. Такі методи дозволяють одночасно враховувати затримку, енергоспоживання, завантаженість каналів і надійність, а також застосовуються для задач розміщення сервісів на туманних вузлах та планування використання кеш-пам'яті [7, 8].

Інтегровані підходи. Остання група робіт робить акцент на тому, що маршрутизацію потрібно розглядати разом із керуванням ресурсами та безпекою. У таких рішеннях шлях для пакета даних − це тільки частина більшої картини, де одночасно враховуються продуктивність, енергетичні витрати, надійність, захист даних та вартість інфраструктури. Зазвичай у таких системах комбінують кілька ідей: SDN для глобального керування, машинне навчання для прогнозування та прийняття рішень, метаевристику для пошуку компромісу між різними цілями і механізми автентифікації для захисту від зловмисних або некоректних вузлів. Зараз у туманних мережах усе частіше переходять від окремої оптимізації одного параметра до підходів, у яких маршрутизація, розміщення сервісів і політики безпеки налаштовуються разом: для кожного маршруту задаються допустима затримка, граничне енергоспоживання та вимоги до захисту, а оптимізаційний алгоритм підбирає конфігурації, які задовольняють ці обмеження. У таких системах маршрутизація розглядається не лише як задача вибору шляху, а як невід'ємна частина загальної стратегії керування ресурсами туманної архітектури. Поєднання SDN, машинного навчання, метаевристики та механізмів автентифікації дозволяє будувати гнучкі, адаптивні та стійкі до відмов інфраструктури [4, 8, 10].

Для наочності розглянемо приклад системи екологічного моніторингу, яка використовує багаторівневу туманну архітектуру. Початкові вимірювання параметрів навколишнього середовища (температура, вологість, концентрація шкідливих речовин тощо) виконуються великою кількістю сенсорних вузлів, розміщених на досить великій території.

Якщо всі ці сенсори безпосередньо передаватимуть дані до хмарного центру, маємо класичну централізовану архітектуру. Для невеликої зони моніторингу з помірними вимогами до затримки цього може бути достатньо: реалізація проста, а всі дані зберігаються в одному місці. Але зі збільшенням площі та кількості вузлів з'являються типові проблеми: зростають затримки передачі даних від віддалених сенсорів, важче оперативно реагувати на зміну показників, а потік даних від тисяч пристроїв перевантажує канали зв'язку та центральний сервер.

Щоб зменшити вплив цих недоліків, одним із можливих рішень є перехід від повністю хмарної до багаторівневої туманної архітектури. У такій архітектурі на проміжному рівні розміщуються туманні вузли, які можна умовно сприймати як регіональні центри обробки. До них надходять дані від сенсорів певної зони. Ці вузли виконують попередню фільтрацію, узагальнення та аналіз інформації і, за потреби, самостійно формують локальні сповіщення, якщо параметри виходять за допустимі межі. У хмару в цьому випадку надсилаються переважно узагальнені показники та події, а не «сирі» дані від кожного сенсора, що помітно зменшує обсяг трафіку й розвантажує центральну інфраструктуру.

Маршрутизація між туманними вузлами та хмарою може будуватися з використанням SDN-контролера, який збирає інформацію про стан каналів, затримки та завантаженість окремих сегментів мережі. На основі цих даних контролер змінює маршрути, перенаправляє трафік у разі погіршення якості зв'язку або виходу з ладу окремих вузлів. Якщо додатково застосовувати методи машинного навчання, можна враховувати сезонні або добові зміни трафіку (наприклад, збільшення кількості даних у промисловій зоні в робочий час) і заздалегідь планувати розподіл навантаження.

Питання безпеки в такій системі теж є важливими. Перед тим як допустити туманний вузол або критичний сенсорний пункт до участі в маршрутизації, їх доцільно перевірити. Для цього можуть використовуватися алгоритми виявлення аномалій, які аналізують поведінку вузла та допомагають виявити підозрілу активність, що може свідчити про компрометацію або несанкціоноване втручання. Тільки після успішної перевірки вузол отримує право передавати й обробляти дані.

Навантаження між туманними вузлами зручно розподіляти за допомогою метаевристичних алгоритмів багатокритеріальної оптимізації. У такій постановці враховується поточне завантаження, споживання енергії, вартість обробки й допустима затримка для різних типів даних. Дані про перевищення граничних рівнів забруднення обробляються з вищим пріоритетом, тоді як фонові статистичні вимірювання можуть передаватися та аналізуватися

при наявності вільних ресурсів. Окрема задача − це вибір місць розміщення сенсорних вузлів і туманних центрів. Якщо враховувати географію, доступність енергоживлення та якість зв'язку, можна побудувати таку топологію, яка дає потрібну щільність моніторингу за прийнятних витрат.

На практиці така архітектура дає зменшення затримок доставки критичних даних, підвищення надійності та стабільності роботи системи, зниження навантаження на хмарний центр та збільшення часу автономної роботи сенсорів, що живляться від батарейок. Якщо додатково аналізувати історичні дані з використанням методів машинного навчання, можна заздалегідь виділяти зони підвищеного ризику та підвищувати пріоритет повідомлень від сенсорів у цих зонах, щоб швидше реагувати на можливі екологічні загрози.

Висновки

Аналіз кластерних, SDN-орієнтованих, методів на основі машинного навчання, метаевристичних та інтегрованих підходів до маршрутизації у багаторівневих туманних мережах показує, що вибір конкретного підходу суттєво впливає на роботу IoT-інфраструктури. На практиці немає універсального рішення, яке однаково добре підходило б для будь-якого сценарію.

Тому при проєктуванні таких систем доводиться комбінувати кілька методів маршрутизації та налаштовувати їх з урахуванням топології, обмежень за ресурсами та вимог до якості обслуговування.

Динамічні методи маршрутизації на основі SDN показують помітне покращення пропускної здатності та зменшення затримки в умовах змінного трафіку й топології [1, 2, 4]. Вони добре підходять для середніх і великих мереж з нерівномірним розподілом навантаження, де важливо мати загальну картину стану мережі й можливість швидко перенаправляти трафік у разі проблем з окремими вузлами чи каналами.

Методи на основі машинного навчання дають найкращий результат у складних і динамічних сценаріях, де класичні алгоритми вже не справляються з кількістю параметрів і залежностей між ними [3, 5−7]. Вони дозволяють точніше прогнозувати стан мережі, налаштовувати ваги зв'язків та пріоритети для різних типів трафіку. Разом з тим такі рішення потребують більших обчислювальних ресурсів і досвіду впровадження, тому їх складніше застосовувати безпосередньо на ресурсно обмежених туманних вузлах.

Кластерні підходи з використанням двофазних протоколів маршрутизації та резервних механізмів на основі традиційних протоколів дають змогу зберігати роботу системи навіть у разі відмови окремих централізованих компонентів [2, 7]. Такі підходи мають сенс у великомасштабних розгортаннях, де потрібно поєднати централізоване керування з локальною стійкістю до відмов.

Інтеграція безпеки, конфіденційності та ефективності використання ресурсів в одній системі маршрутизації на практиці є обов'язковою умовою для побудови надійних IoT-інфраструктур. Якщо намагатися покращити тільки продуктивність, тільки енергоефективність або тільки безпеку, то система в цілому працює гірше, ніж могла б. Тому на етапі проєктування маршрутизації доцільно одразу задавати обмеження на затримку, споживання енергії та рівень безпеки й підбирати маршрути та місця розміщення вузлів так, щоб ці вимоги виконувалися одночасно. Інтелектуальні методи автентифікації вузлів і виявлення аномалій у такому разі дозволяють підвищити рівень захисту без помітного погіршення продуктивності [6, 9−11].

Метаевристичні методи багатокритеріальної оптимізації особливо корисні при розгортанні IoT-сервісів у туманних мережах, коли потрібно одночасно враховувати затримку, енергоспоживання, пропускну здатність, вартість обробки та надійність маршрутів. Вони допомагають знаходити компромісні рішення у складних просторах пошуку й краще масштабуються порівняно з детерміністичними підходами [7, 8].

Багаторівнева туманна архітектура загалом дає відчутні переваги порівняно з повністю централізованими хмарними рішеннями, коли потрібно обробляти дані майже в режимі реального часу. Перенесення частини обробки даних ближче до джерел їх виникнення дозволяє зменшити затримки, знизити навантаження на центральні сервери та підвищити стійкість системи до відмов окремих компонентів. Водночас такі архітектури складніші в керуванні: потрібно координувати роботу різних рівнів і окремо стежити за безпекою на кожному з них.

На основі проведеного аналізу сформульовано такі орієнтовні рекомендації щодо вибору методів маршрутизації для різних типів систем. Для відносно невеликих за масштабом IoT-систем з помірними вимогами до затримки можуть бути достатніми спрощені динамічні або кластерні рішення без складних механізмів машинного навчання. У великих туманних мережах із нерівномірним навантаженням та високими вимогами до адаптивності більш доцільними є SDN-орієнтовані та інтегровані підходи, які забезпечують глобальне керування і гнучкий перерозподіл трафіку. Там, де критичною є енергоефективність і тривалість автономної роботи вузлів, маршрути варто будувати так, щоб якомога більше попередньої обробки виконувалося локально, а в мережу передавалися вже агреговані або стиснені дані.

У роботі можна виділити кілька пов'язаних між собою напрямів подальшого розвитку систем маршрутизації для туманних мереж:

– розробка алгоритмів машинного навчання, які ефективно використовують ресурси і можуть працювати безпосередньо на туманних вузлах з обмеженими енергетичними та обчислювальними можливостями;

– створення узгоджених протоколів та інтерфейсів міжрівневої взаємодії у багаторівневих архітектурах, щоб рішення різних виробників могли коректно працювати разом;

– дослідження методів спільного налаштування показників QoS, енергоспоживання, надійності та безпеки як єдиної задачі маршрутизації, а не окремих незалежних цілей;

– розробка зручних інструментів для моделювання, тестування та порівняльної оцінки продуктивності різних методів маршрутизації на наборах сценаріїв, наближених до реальних умов роботи мережі;

– створення адаптивних систем, які можуть змінювати стратегію маршрутизації та набір застосовуваних методів залежно від поточного стану мережі, пріоритетів трафіку та заданих обмежень.

У сучасних IoT-інфраструктурах та розумних містах ефективна маршрутизація у багаторівневих туманних мережах стає одним із ключових чинників успішності таких систем. Раціональний вибір і поєднання методів маршрутизації в конкретному проєкті дають змогу досягти не лише прийнятних технічних показників, а й обґрунтованих витрат на експлуатацію інфраструктури у довгостроковій перспективі.

Список використаної літератури

1. Tsvirkun L., Myronov Y. Challenges and Specificities of Adopting Continuous Integration within Scalable Cloud Environments // *2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*. IEEE, 2023. DOI: 10.1109/csit61576.2023.10324010.

2. ICDRP-F-SDVN: An innovative cluster-based dual-phase routing protocol using fog computing and software-defined vehicular network [Electronic resource] / Khalid A. Darabkh [et al.] // *Vehicular Communications*. 2022. Vol. 34. P. 100453. Access mode: https://doi.org/10.1016/j.vehcom.2021.100453.

3. Sarma B., Kumar R., Tuithung T. Machine learning enabled network and task management in SDN based Fog architecture [Electronic resource] // *Computers and Electrical Engineering*. 2023. Vol. 108. P. 108705. Access mode: https://doi.org/10.1016/j.compeleceng.2023.108705.

4. Valizadeh P., Yaghmaee M. H., Sedaghat Y. Reliability and bandwidth aware routing in SDN-based fog computing for IoT applications [Electronic resource] // *Ad Hoc Networks*. 2025. – Vol. 172. P. 103803. Access mode: https://doi.org/10.1016/j.adhoc.2025.103803.

5. Gao Y., Ji K., Gao T. Route planning model based on multidimensional eigenvector processing in vehicular fog computing [Electronic resource] // *Computer Communications*. 2023. Access mode: https://doi.org/10.1016/j.comcom.2023.10.019.

6. Alwasi Frimpong S. [et al.] An adaptive collaborative intrusion detection system for vehicular fog computing networks [Electronic resource] // *Engineering Applications of Artificial Intelligence*. 2025. Vol. 158, Part B. Access mode: https://doi.org/10.1016/j.engappai.2025.111563.

7. Bhavani A., Venkataramana A., Chakravarthy A. S. N. Multi-Objective Hybrid Green Anaconda Skill Optimization Enabled Energy and Cache Based QoS Aware Routing in Delay Tolerant–IoT Network [Electronic resource] // *Sustainable Computing: Informatics and Systems*. 2025. P. 101158. Access mode: https://doi.org/10.1016/j.suscom.2025.101158.

8. Wu B. [et al.] Optimal Deploying IoT Services on the Fog Computing: A Metaheuristic-Based Multi-Objective Approach [Electronic resource] // *Journal of King Saud University – Computer and Information Sciences*. 2022. Access mode: https://doi.org/10.1016/j.jksuci.2022.10.002.

9. Gowri V., Baranidharan B. Adaptive probabilistic neural network based edge data center authentication for secure load balancing in fog computing [Electronic resource] // *Applied Soft Computing*. 2025. Vol. 169. P. 112567. Access mode: https://doi.org/10.1016/j.asoc.2024.112567.

10. Javanmardi S. [et al.] An integration perspective of security, privacy, and resource efficiency in IoT-Fog networks: A comprehensive survey [Electronic resource] // *Computer Networks*. 2025. P. 111470. Access mode: https://doi.org/10.1016/j.comnet.2025.111470.

11. Awais S. M. [et al.] Provably secure fog-based authentication protocol for VANETs [Electronic resource] // *Computer Networks*. 2024. Vol. 246. P. 110391. Access mode: https://doi.org/10.1016/j.comnet.2024.110391.

12. Цвіркун Л., Соболевський І. Аналіз особливостей використання туманних комп'ютерних середовищ для побудови IoT інфраструктури // *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. № 1. С. 238–243.

References

1. Tsvirkun L., Myronov Y. (2023) Challenges and Specificities of Adopting Continuous Integration within Scalable Cloud Environments. *Proceedings of the 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, IEEE, DOI: 10.1109/csit61576.2023.10324010.

2. Darabkh K. A., et al. (2022) ICDRP-F-SDVN: An innovative cluster-based dual-phase routing protocol using fog computing and software-defined vehicular network. *Vehicular Communications (electronic journal),* vol. 34, p. 100453. Retrieved from: https://doi.org/10.1016/j.vehcom.2021.100453.

3. Sarma B., Kumar R., Tuithung T. (2023) Machine learning enabled network and task management in SDN based Fog architecture. *Computers and Electrical Engineering (electronic journal),* vol. 108, p. 108705. Retrieved from: https://doi.org/10.1016/j.compeleceng.2023.108705.

4. Valizadeh P., Yaghmaee M. H., Sedaghat Y. (2025) Reliability and bandwidth aware routing in SDN-based fog computing for IoT applications. *Ad Hoc Networks (electronic journal),* vol. 172, p. 103803. Retrieved from: https://doi.org/10.1016/j.adhoc.2025.103803.

5. Gao Y., Ji K., Gao T. (2023) Route planning model based on multidimensional eigenvector processing in vehicular fog computing. *Computer Communications (electronic journal).* Retrieved from: https://doi.org/10.1016/j.comcom.2023.10.019.

6. Frimpong S. A., et al. (2025) An adaptive collaborative intrusion detection system for vehicular fog computing networks. *Engineering Applications of Artificial Intelligence (electronic journal),* vol. 158, Part B. Retrieved from: https://doi.org/10.1016/j.engappai.2025.111563

7. Bhavani A., Venkataramana A., Chakravarthy A. S. N. (2025) Multi-Objective Hybrid Green Anaconda Skill Optimization Enabled Energy and Cache Based QoS Aware Routing in Delay Tolerant–IoT Network. *Sustainable Computing: Informatics and Systems (electronic journal),* p. 101158. Retrieved from: https://doi.org/10.1016/j.suscom.2025.101158

8. Wu B., et al. (2022) Optimal Deploying IoT Services on the Fog Computing: A Metaheuristic-Based Multi-Objective Approach. Journal of King Saud University – Computer and Information Sciences (electronic journal). Retrieved from: https://doi.org/10.1016/j.jksuci.2022.10.002

9. Gowri V., Baranidharan B. (2025) Adaptive probabilistic neural network based edge data center authentication for secure load balancing in fog computing. *Applied Soft Computing (electronic journal),* vol. 169, p. 112567. Retrieved from: https://doi.org/10.1016/j.asoc.2024.112567

10. Javanmardi S., et al. (2025) An integration perspective of security, privacy, and resource efficiency in IoT-Fog networks: A comprehensive survey. *Computer Networks (electronic journal),* p. 111470. Retrieved from: https://doi.org/10.1016/j.comnet.2025.111470

11. Awais S. M., et al. (2024) Provably secure fog-based authentication protocol for VANETs. *Computer Networks (electronic journal),* vol. 246, p. 110391. Retrieved from: https://doi.org/10.1016/j.comnet.2024.110391

12. Tsvirkun L., Sobolevskyi I. (2025) Analiz osoblyvostei vykorystannia tumannykh kompiuternykh seredovyshch dlia pobudovy IoT infrastruktury *[Analysis of the features of using fog computer environments for building IoT infrastructure]*. Information Technology: Computer Science, Software Engineering and Cyber Security, no. 1, pp. 238–243

Дата першого надходження статті до видання: 20.02.2026
Дата прийняття статті до друку після рецензування: 27.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026