УДК 004.722:004.732 DOI: 10.31673/2412-4338.2026.019016

Джусь Олексій Петрович
аспірант кафедри систем автоматизованого проектування
Національний університет «Львівська політехніка», Львів, Україна
ORCID 0009-0004-0030-6162
oleksii.p.dzhus@lpnu.ua

Лобур Михайло Васильович
доктор технічних наук, професор, завідувач кафедри систем автоматизованого проектування
Національний університет «Львівська політехніка», Львів, Україна
ORCID 0000-0001-7516-1093
mykhaylo.v.lobur@lpnu.ua

ГІБРИДНИЙ ПРОТОКОЛ МАРШРУТИЗАЦІЇ ДЛЯ БЕЗПРОВОДОВИХ MESH-МЕРЕЖ

Анотація. *Ефективність безпроводових mesh-мереж критично залежить від протоколу маршрутизації канального рівня, який працює з MAC-адресами та повинен адаптуватися до змінної топології, інтерференції, характеру трафіку та вимог якості обслуговування. В роботі проаналізовані існуючі методи гібридизації маршрутизації в mesh-мережах, визначено вимоги до L2-протоколурозроблено архітектуру гібридного протоколу, що включає модуль виявлення сусідів, сформулювано оптимізаційну задачу максимізації сумарної корисності маршруту за лінійними обмеженнями QoS, виконано математичний аналіз середньої затримки доставки, контрольного навантаження, часу конвергенції, допустимого навантаження та умов стабільності з використанням експоненційного згладжування метрик для запобігання «мерхтінню» режимів, виявлено слабкі місця протоколу та визначити перспективи вдосконалення. Запропонований протокол обмежує проактивну зону, забезпечуючи лінійне масштабування локального трафіку OGM і квадратичне – лише для періодичних глобальних оновлень. Математичні моделі дозволяють розрахувати середню затримку як зважену суму залежно від ймовірності проактивного режиму, загальне контрольне навантаження, час конвергенції та умови стабільності. Теоретичні розрахунки демонструють зменшення накладних витрат на 50–80% порівняно з BATMAN у великих мережах, швидшу локальну конвергенцію, кращу адаптацію до трафіку та повноцінну підтримку QoS. Порівняння з іншими протоколами підтверджує переваги у мобільних і гетерогенних сценаріях. Можливі тимчасові петлі при перемиканні режимів (ймовірність ~0,1 при високій мобільності), залежність від точності метрик, підвищена складність реалізації, обчислювальні витрати на IoT-пристроях та відсутність вбудованої криптографії (вразливість до атак типу «чорна діра», DoS). Отримані результати свідчать, що HMP є ефективним рішенням для високонавантажених динамічних mesh-мереж.*

Ключові слова: *mesh-мережа, гібридна маршрутизація, BATMAN, HWMP, протокол L2, QoS.*

Dzhus Oleksii
Ph.D. student of the Computer Aided Design Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0009-0004-0030-6162
oleksii.p.dzhus@lpnu.ua

Lobur Mykhaylo
DSc., professor, head of the Computer Aided Design Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0001-7516-1093
mykhaylo.v.lobur@lpnu.ua

HYBRID ROUTING PROTOCOL FOR WIRELESS MESH NETWORKS

Abstract. *The efficiency of wireless mesh networks critically depends on the link-layer routing protocol, which works with MAC addresses and must adapt to changing topology, interference, traffic patterns, and quality of service requirements. The paper analyzes existing methods of hybridizing routing in mesh networks, defines requirements for the L2 protocol, develops an architecture of a hybrid protocol that includes a neighbor discovery module, formulates an optimization problem for maximizing the total utility of a route under linear QoS constraints, performs a mathematical analysis of the average delivery delay, control load, convergence time, allowable load, and stability conditions using*

exponential smoothing of metrics to prevent "flickering" of modes, identifies weaknesses of the protocol, and identifies prospects for improvement. The proposed protocol limits the proactive zone, providing linear scaling of local OGM traffic and quadratic scaling only for periodic global updates. Mathematical models allow calculating the average delay as a weighted sum depending on the probability of proactive mode, the total control load, the convergence time and the stability conditions. Theoretical calculations demonstrate a 50–80% reduction in overhead compared to BATMAN in large networks, faster local convergence, better adaptation to traffic and full QoS support. Comparison with other protocols confirms the advantages in mobile and heterogeneous scenarios. Possible time loops when switching modes (probability ~0.1 at high mobility), dependence on the accuracy of metrics, increased implementation complexity, computational costs on IoT devices and lack of built-in cryptography (vulnerability to black hole attacks, DoS). The results obtained indicate that HMP is an effective solution for highly loaded dynamic mesh networks.

Keywords: *mesh network, hybrid routing, BATMAN, HWMP, L2 protocol, QoS.*

1. Вступ

Безпроводові mesh-мережі представляють собою децентралізовані самоорганізовані мережі, в яких кожен вузол може функціонувати як маршрутизатор для пересилання трафіку інших вузлів. Ефективність таких мереж критично залежить від обраного протоколу маршрутизації, який визначає, як пакети знаходять шлях від джерела до призначення через множину проміжних вузлів. Mesh-мережі забезпечують стійкість, розширюваність та самовідновлення без потреби в централізованій інфраструктурі. Важливим компонентом будь-якої передачі даних є протокол маршрутизації, який визначає, як вузли обмінюються інформацією про топологію та вибирають шляхи для передачі. Фокус робиться на протоколах рівня L2 (канального рівня), оскільки вони дозволяють прозору маршрутизацію на основі MAC-адрес, що є ефективним для безпроводових середовищ.

Аналіз існуючих протоколів виявляє фундаментальний компроміс між проактивними та реактивними підходами [1]. Проактивні протоколи (OLSR, BATMAN-adv) підтримують постійно актуальну інформацію про маршрути, забезпечуючи низьку затримку встановлення з'єднання, але ціною високих накладних витрат на підтримку таблиць маршрутизації. Реактивні протоколи мінімізують накладні витрати, але вносять затримку на пошук маршруту при кожному новому з'єднанні. Оптимальний протокол для mesh-мережі повинен адаптивно поєднувати обидва підходи залежно від динаміки топології мережі (швидкості зміни з'єднань), характеру трафіку (постійний vs епізодичний), щільності вузлів у різних зонах мережі, доступності енергетичних ресурсів і вимог до якості обслуговування 'Quality of Service' (QoS). Ця потреба мотивує розробку гібридних протоколів, які здатні динамічно обирати стратегію маршрутизації на основі поточних умов мережі.

2. Постановка проблеми

Сучасні безпроводові mesh-мережі широко застосовуються в системах широкосмугового доступу, розумного міста, промислового IoT та аварійних комунікацій. Їх головною перевагою є саморганізуюча архітектура та стійкість до відмов вузлів. Однак ефективна маршрутизація в таких мережах залишається складною проблемою. Основна проблема полягає в необхідності одночасного забезпечення високої адаптивності до швидких змін топології, мобільності вузлів та мінливих умов радіоканалу при збереженні низьких накладних витрат на службовий трафік і масштабованості мережі до сотень і тисяч вузлів. Існуючі протоколи мають суттєві обмеження. Проактивні рішення (BATMAN, OLSR) забезпечують швидку реакцію, але генерують надмірний контрольний трафік, що знижує корисну пропускну здатність у великих мережах. Реактивні протоколи (AODV) мінімізують службові витрати, проте створюють значну початкову затримку. Гібридні протоколи, зокрема HWMP стандарту IEEE 802.11s, недостатньо ефективні в умовах високої мобільності та гетерогенності мережі.

Особливо гостро проблема проявляється на канальному рівні (L2). Маршрутизація за MAC-адресами дозволяє зменшити накладні витрати та забезпечити прозорість для верхніх рівнів, але ускладнює глобальну оптимізацію маршрутів з урахуванням наскрізних QoS-параметрів (затримка, втрати, пропускна здатність).

Таким чином, актуальним науковим і практичним завданням є розробка гібридного протоколу маршрутизації L2, який динамічно поєднує проактивні та реактивні механізми, використовує локальні метрики якості каналів і забезпечує підтримку QoS при добрій масштабованості в динамічних mesh-мережах. Розв'язання цієї проблеми дозволить суттєво підвищити ефективність, надійність і економічність безпроводових mesh-мереж у сучасних і перспективних застосуваннях.

3. Аналіз останніх досліджень і публікацій

Гібридні методи в безпродових mesh-мережах зазвичай поєднують кілька стратегій маршрутизації, режимів передачі або стеків протоколів на рівні 2 (L2) для покращення пропускної

здатності, надійності та якості обслуговування. Робота охоплює маршрутизацію на основі HWMP стандарту IEEE 802.11s, маршрутизацію на рівні MAC, гібридні безпроводові/BS архітектури та схеми на основі міжрівневих або оптимізаційних схем.

Можна виділити кілька підгодів до гібридизації mesh-мереж:

– гібридний протокол базової станції/ad-hoc дозволяє здійснювати 1- або 2-стрибкові прямі передачі в мережі, орієнтованій на базові станції; двострибковий прямий режим може покращити повну швидкість зв'язку на ~20% порівняно з чистою інфраструктурною маршрутизацією [2];

– гібридні схеми зворотного розсіювання/безпроводового живлення поєднують пасивне зворотне розсіювання та активну радіочастотну передачу зі збором енергії; оптимізоване перемикання режимів значно збільшує пропускну здатність та дальність у сітках, подібних до IoT, та гетерогенних мережах [3], [4];

гібридне кільце-сітчасте мережеве кодування (Hybrid Ring-Mesh Protocol, HRMP) поєднує проводове оптичне кільце та безпроводову сітку з кооперативним мережевим кодуванням, що забезпечує нижчий рівень помилок пакетів та розширене покриття для великих даних через безпроводові мобільні мережі класу 5G [5].

Можна виділити існуючі підходи до адаптації протоколів:

1. Гібридний безпродовий mesh-протокол (Hybrid Wireless Mesh Protocol, HWMP) – це гібридний протокол маршрутизації L2 (проактивне дерево + реактивна маршрутизація на вимогу), що використовує MAC-адреси та радіозалежні метрики; моделювання показують меншу затримку та вищу пропускну здатність, ніж чистий AODV [6].

2. Кооперативний підхід до маршрутизації L2 обмежує проактивну маршрутизацію стабільною магістраллю та використовує реактивну маршрутизацію для мобільних клієнтів, причому обидва протоколи співіснують на рівні MAC, використовуючи окремі таблиці пересилання, зменшуючи втрату пакетів та затримку [7].

3. У гібридних безпродових mesh-мережах (Cooperative Hybrid Routing Protocol, CHRP) поєднує проактивну та реактивну маршрутизацію з метрикою, що враховує вузли (стан каналу, перешкоди, енергія клієнта), для покращення пропускної здатності, затримки та споживання енергії [8].

4. Протокол гібридної маршрутизації за регіональними умовами (Regional Condition Hybrid Routing Protocol, RC-HRP) для гетерогенних WMN масштабує ємність, використовуючи багаторадіомашлюзові маршрутизатори та диференційований трафік шлюзів/клієнтів [9].

5. Гібридний багатошляховий алгоритм маршрутизації та планування, орієнтований на QoS, використовує інформацію про пропускну здатність та затримку для розділення потоків по шляхах, зменшуючи затримку в черзі, тремтіння та втрати [10].

В табл. 1 приведене структуроване порівняння існуючих підходів до гібридизації mesh-мереж.

Таблиця 1

Порівняння підходів до гібридизації mesh-мереж

Підхід	Гібридний аспект	Основні переваги
HWMP (802.11s) [6], [11], [12]	Проактивна, реактивна маршрутизація L2	Збільшення пропускної здатності, зменшення затримка проти AODV
Кооперативна маршрутизація на рівні MAC [7]	Проактивна магістраль, реактивний клієнт на рівні L2	Зменшення втрат, зменшення затримки
CHRP [8], [13]	Проактивна, реактивна, міжрівневі метрики	Зменшення втрат, зменшення затримки, економія енергії
RC HRP [9]	Регіональна гібридна маршрутизація в гетерогенній WMN	Збільшення ємность, збільшення пропускної здатності

Також можна виділити гібриди, орієнтовані на безпеку та надійність:

– secure-GLOR використовує гібридне шифрування (симетричне + асиметричне) у протоколі маршрутизації WMN на основі геолокації, зменшуючи розмір шифротексту та криптографічні накладні витрати, одночасно покращуючи безпеку [14];

– гібридні схеми цілісності і шифрування для ad hoc / mesh-подібних WANET підвищують конфіденційність та стійкість до вторгнень завдяки меншим обчислювальним ресурсам порівняно з традиційними моделями безпеки [15], [16].

У безпроводових mesh-мережах L2 «гібридна» передача найчастіше означає поєднання проактивної та реактивної маршрутизації, інфраструктурних та ad hoc шляхів або пасивних та активних режимів фізичного рівня для балансування пропускної здатності, затримки, стійкості та енергії. HWMP IEEE 802.11s, гібридна маршрутизація на рівні MAC та схеми зворотного розсіювання/активності демонструють суттєві переваги, тоді як новіші роботи додають багатошляхове планування з урахуванням QoS, мережеве кодування та гібридну криптографію для безпечних, масштабованих mesh-мереж.

Для безпроводових мобільних мереж 802.11s, схеми багатоадресної розсилки L2 (L2M-S/E) повторно використовують стан дерева HWMP та додають розподілену оптимізацію дерева, зменшуючи накладні витрати та покращуючи пропускну здатність багатоадресної розсилки [11]. Тестова робота з BATMAN-adv та HWMP підтверджує нижчі накладні витрати на обробку маршрутизації L2 та підтримку незалежно від протоколу вище L2, що робить її привабливою для високопродуктивних сіток [12].

4. Мета і задачі дослідження

Мета дослідження полягає в розробці та теоретичному обґрунтуванні гібридного протоколу маршрутизації канального рівня для безпроводових mesh-мереж, який динамічно поєднує проактивні механізми з локальними метриками якості каналів і реактивні механізми пошуку маршрутів, забезпечуючи високу адаптивність, підтримку QoS, зменшення накладних витрат та масштабованість у динамічних умовах. Для досягнення поставленої мети визначимо задачі:

1. Визначити ключові вимоги до гібридного L2-протоколу: робота виключно з MAC-адресами, використання локальних метрик (TQ, RSSI, SNR тощо), відсутність необхідності у повній глобальній карті топології, забезпечення масштабованості при великій кількості вузлів.

2. Розробити архітектуру та функціональну структуру протоколу.

3. Сформулювати математичну оптимізаційну задачу вибору маршрутів як задачу максимізації сумарної корисності з лінійними обмеженнями QoS-параметрів, а також моделі оцінки середньої затримки, контрольного навантаження, часу конвергенції та стабільності системи.

4. Виконати теоретичний аналіз ефективності, розрахувати накладні витрати, порівняти протокол з існуючими рішеннями та виявити його сильні та слабкі сторони.

5. Результати дослідження

Вимоги до гібридного методу

Важливим компонентом будь-якої передачі даних є протокол маршрутизації, який визначає, як вузли обмінюються інформацією про топологію та вибирають шляхи для передачі, тому основними вимогами для протоколу канального рівня є:

– оперування адресами другого рівня (наприклад, MAC);

– відсутність потреби у формуванні повної карти топології;

– використання локальних метрик (рівень довіри, якість посилання тощо);

– можливість уникнення великого перевикористання ресурсів при масштабуванні mesh-мережі.

В якості найближчого аналога підходить децентралізований routing-протокол BATMAN, у якому кожен вузол періодично розсилає пакет OGM (Originator Message). На їх основі кожен одержувач визначає найкращий шлях до джерела, вимірюючи якість каналів. Для виявлення якості використовується метрика метрика TQ (Transmission Quality)

$$TQ_{ij} = \frac{N_{success}}{N_{all}}, \quad (1)$$

де $N_{success}$ – успішні передачі, N_{all} – всі передачі.

Після чого оновлення шляхів відбувається локально, без глобальних таблиць маршрутизації, тому протокол добре підходить для великих та динамічних мереж. Але в той самий час він не має суворого обчислення глобальної топології, що ускладнює оптимізацію сценаріїв із великим трафіком. Також слід зазначити, що якість каналів визначається емпірично, без аналітичної моделі об'єктивної оцінки комбінованих шляхів.

Інші протоколи (OLSR, HWMP у 802.11s, AODV у L3) відрізняються механізмом побудови маршрутів (таблиці, карти топологій, реактивні запити маршруту тощо). Часто ці підходи вимагають додаткових метрик, картографічних таблиць, що збільшує трафік контролю.

Структура гібридного mesh-протоколу

Пропонується гібридний mesh-протокол (Hybrid Mesh Protocol, HMP), який поєднує переваги локальних метрик L2 (як у BATMAN) і адаптивної глобальної оптимізації шляхів на основі часткової карти топології для великих і навантажених мереж. Основні особливості нового протоколу:

– локальні метрики (як TQ у BATMAN);

– глобальні епізоди оновлення топології для критичних шляхів;

– модуль QoS, що враховує затримку D, пропускну здатність B та втрати пакетів L.

Запропонований протокол HMP являє собою гібридний протокол другого рівня OSI, який інтегрує проактивні та реактивні механізми маршрутизації з адаптивним переключенням між ними на основі характеристик мережі.

Протокол HMP складається з наступних ключових компонентів (див. рис. 1):

1. Модуль виявлення сусідів (neighbor discovery) періодично розсилає beacon-повідомлення для виявлення та моніторингу доступних сусідніх вузлів. Відстежує якість каналів до кожного сусіда через вимірювання RSSI, SNR та packet loss rate.

2. Проактивний модуль (proactive core): підтримує таблиці маршрутизації для критичних напрямків (gateway вузли, інфраструктурні маршрутизатори). Використовує модифікований алгоритм на основі BATMAN-adv з періодичними OGM.

3. Реактивний модуль (reactive module): виконує пошук маршрутів за запитом для рідкісних або тимчасових з'єднань. Використовує механізм Route Request (RREQ) і Route Reply (RREP) з локальним кешуванням.

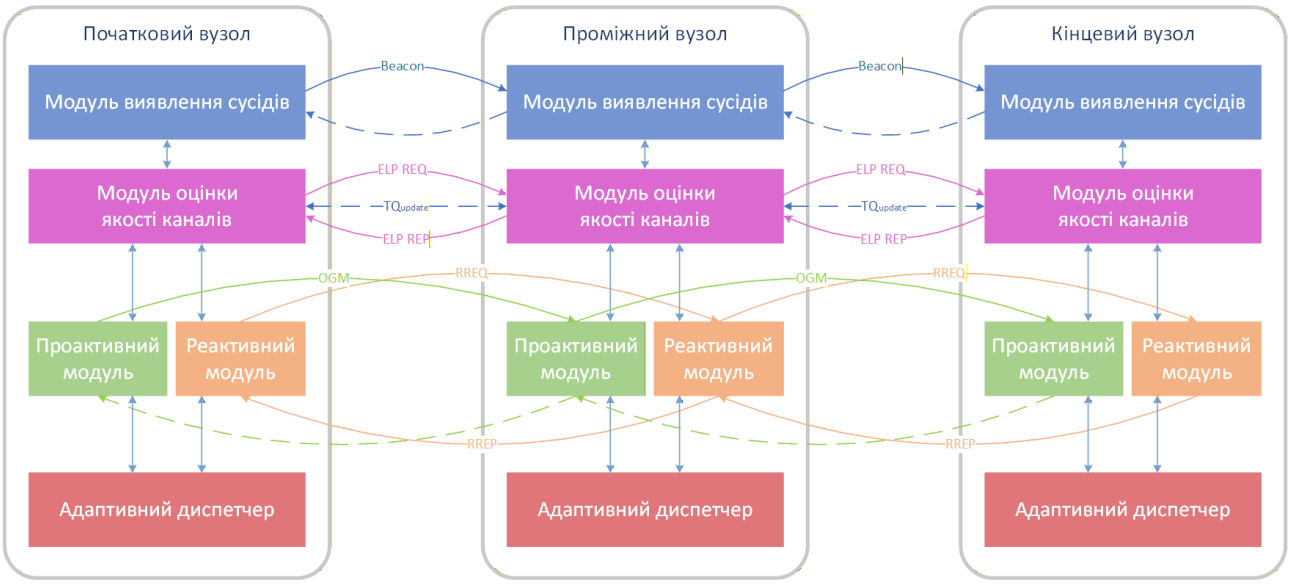

Рис. 1. Схема взаємодії компонентів гібридного mesh-протоколу

4. Адаптивний диспетчер (adaptive manager): приймає рішення про використання проактивного або реактивного режиму на основі аналізу метрик мережі, історії трафіку та прогнозування поведінки.

5. Модуль оцінки якості каналів (link quality estimator): обчислює комплексну метрику якості на основі декількох параметрів: затримка, пропускна здатність, стабільність, енергоефективність.

Mesh-мережу моделюємо як граф $G(V, E)$ із множиною вузлів V і множиною безпроводових зв'язків E. Ребро $e_{ij} \in E$ існує, якщо вузол i може напряму обмінюватися кадрами з вузлом j, якість сигналу перевищує поріг і канал вважається доступним для маршрутизації. Тобто кожне ребро – це

реальний радіоканал між двома сусідами. А тому для кожного ребра e_{ij} визначаємо $q_{ij} \in [0,1]$ – якість каналу (чим ближче до 1, тим краще), Δ_{ij} – середня затримка, l_{ij} – відсоток втрат. HMP можна розділити на етапи:

1. *Ініціалізація*. Кожен вузол створює віртуальний L2-інтерфейс, подібно до BATMAN. Визначається параметр k (глибина проактивної зони, типово 3–5 переходи). Кожен вузол i періодично вимірює якість прямого каналу q_{ij} до сусіда j і затримку Δ_{ij} та втрати l_{ij}.

2. *Проактивна (локальна) фаза*. Періодично (інтервал T_{loc} в межах 1–2 сек.) вузли розсилають OGM з інформацією про сусідів і метриками TQ, після чого будуються таблиці маршрутів для вузлів у радіусі k переходів. Якщо посилання асиметричне, використовується ELP (Echo Location Protocol) для перевірки. Так локальна метрика для ребра $i \to j$ визначається як

$$M_{ij} = \alpha q_{ij} - \beta \Delta_{ij} - \gamma l_{ij}, \tag{2}$$

де α, β і γ – вагові коефіцієнти для пріоритетів QoS.

3. *Реактивна (глобальна) фаза*. Якщо призначення за межами k хопів, вузол-джерело надсилає RREQ, аналогічно до AODV, але на L2 з MAC-адресами. RREQ поширюється з накопиченням метрик (затримка, втрати пакетів), а вузол-призначення відповідає RREP по найкращому шляху, який кешується на час T_{glob}. В результаті глобальні оновлення дозволяють раз на T_{glob} узгоджувати вузлам часткові карти топології суміжних вузлів та обчислювати глобальні метрики для довгих маршрутів.

4. *Передача даних* для локальних – за проактивними таблицями, для глобальних – за реактивними шляхами. Якщо шлях розривається, ініціюється локальне відновлення або новий запит.

5. Періодичні OGM *оновлюють локальні таблиці*; реактивні запити активуються за потребою. Конструювання маршруту – вибір шляху $P_{u \to v}$ між довільними вузлами u і v із максимальним сумарним значенням

$$M(P_{u \to v}) = \sum_{(u,v) \in P_{u \to v}} M_{uv}, \tag{3}$$

за умови, що

$$M(P_{u \to v}) > \theta, \tag{4}$$

де θ – поріг прийнятної якості маршруту.

Ця гібридна модель зменшує флудинг OGM у великих мережах, обмежуючи проактивність локальною зоною.

Визначення оптимізаційної задачі між проактивною та реактивною фазами

Для маршруту між вузлами u і v

$$\sum_{(i,j) \in P} \alpha q_{ij} - \beta \Delta_{ij} - \gamma l_{ij}\,, \tag{5}$$

за умов:

$$q_{ij} \geq q_{min}, \Delta_{ij} \leq \Delta_{max}, l_{ij} \leq l_{max}. \tag{6}$$

Це задача на знаходження шляху з максимальною сумарною корисністю з лінійними обмеженнями.

Середня затримка доставки пакета в HMP залежить від режиму маршрутизації:

$$D_{avg} = p_{proact} \cdot D_{proact} + p_{react} \cdot (D_{discov} + D_{react}), \quad (7)$$

де p_{proact} – ймовірність використання проактивного режиму, D_{proact} – затримка при наявності готового маршруту, D_{discov} – затримка пошуку маршруту, D_{react} – затримка передачі після знаходження маршруту.

Для частих з'єднань $p_{proact} \approx 1$ середня затримка HMP наближається до D_{proact}, що забезпечує продуктивність на рівні повністю проактивних протоколів. Для нечастих з'єднань домінує реактивний компонент, що зменшує накладні витрати.

Визначення допустимого навантаження на мережу

Нехай $N = |V|$ для множини вузлів mesh-мережі V, а їх кількості N. Тоді можна визначити локальне навантаження. Кожен вузол періодично розсилає повідомлення своїм сусідам. Якщо період локальних оновлень T_{loc} і кількість сусідів d_i для вузла i, то кількість локальних повідомлень за один період, із класичної леми про суму степенів, в якій кожне ребро з'єднує два вузли, отже воно враховується двічі при підрахунку степенів:

$$\sum_{i=1}^{N} d_i = 2|E|, \quad (8)$$

а в безпроводових мережах середній ступінь вузла зазвичай обмежений (мережа розріджена), то:

$$|E| = O(N), \quad (9)$$

тобто локальний контрольний трафік масштабується лінійно з кількістю вузлів $C_{loc} = O(N)$. Це одна з причин, чому L2-підходи добре масштабуються.

Глобальні оновлення відбуваються раз на T_{glob}, тому у найгіршому випадку кожен вузол може розповсюджувати частину інформації про топологію лише в обмежані періоди. З цього формується глобальне навантаження, тоді кількість потенційних пар взаємодій складає $O(N^2)$. Отже середній контрольований трафік $C_{glob} = O\left(\frac{N^2}{T_{glob}}\right)$.

Таким чином можна визначити загальне контрольне навантаження

$$C_{ctrl} = O\left(N + \frac{N^2}{T_{glob}}\right) \quad (10)$$

при умові інтенсивність контрольного трафіку

$$\frac{N^2}{T_{glob}} \leq \epsilon \lambda_{data}, \quad (11)$$

де λ_{data} – інтенсивність корисного трафіку, $\varepsilon \ll 1$ – допустима частка контрольного трафіку. Тому якщо глобальна частина стає незначною, то система поводиться подібно до BATMAN, який є проактивним, що призводить до високих накладних у великих мережах $O(n^2)$, тоді як HMP обмежує це k-перехід, зменшуючи O на 50–80% для $d > 10$. Конвергенція швидша для локальних шляхів, але повільніша для глобальних порівняно з реактивними як AODV. HWMP також гібридний, але фокусується на деревах для фіксованих топологій, тоді як HMP адаптований для динамічних з BATMAN-подібними метриками. HMP кращий у мобільних сценаріях (швидше оновлення локальних зон), але HWMP ефективніший у статичних з меншою затримкою ($C_{react} \approx d \cdot \tau$ проти стандартних $2d \cdot \tau$).

Аналіз накладних витрат протоколу

Теоретичний аналіз HMP базується на оцінці накладних витрат, часу конвергенції та пропускної здатності. Розглянемо мережу з n вузлами, діаметром D (максимальна кількість переходів), щільністю ρ (вузлів на одиницю площі). Накладні витрати складаються з витрат на проактивну та реактивну частини. Для проактивної частини кожен вузол розсилає OGM з частотою $1/T_{loc}$. Для зони k переходів, кількість OGM на вузол $\approx \pi k^2 \rho$ (за моделлю дискового графа)

$$O_{loc} = \frac{n}{T_{loc}} \cdot \pi k^2 \rho \cdot sizeof(OGM). \quad (12)$$

Для реактивної частини для m запитів, кожен RREQ поширюється на $O(D^2)$ вузлів

$$O_{glob} = m \cdot D^2 \cdot sizeof(RREQ). \quad (13)$$

Загальні максимальні накладні витрати розраховуються

$$O_{max} \leq O_{loc} + O_{glob}. \quad (14)$$

Порівнюючи із BATMAN ($O \approx n^2/T_{glob}$), HMP зменшує O за рахунок обмеження $k << D$.

Час конвергенції для проактивної частини становить

$$C_{loc} = k \cdot \tau, \quad (15)$$

де τ – середня затримка переходу.

Для реактивної частини час конвергенції становить

$$C_{glob} = 2d \cdot \tau\ (RREQ + RREP). \quad (16)$$

Так як одночасна робота не можлива, тому можна розрахувати середній час конвергенції

$$C_{avg} = \left(p_{local} \cdot C_{loc} + \ (1 - p_{local}) \cdot C_{glob}\right), \quad (17)$$

де p_{local} – ймовірність локальної комунікації (залежить від додатка, наприклад, 0,7 для IoT).

Пропускну здатність можна визначити через смугу прокускання безпродового каналу:

$$S = S_{max} \cdot (1 - O_{max}/B), \quad (18)$$

де B – доступна смуга пропускання.

Метрика шляху для кожного переходу:

$$TQ = \prod(1 - p_i) \cdot S_i, \quad (19)$$

де p_i – втрати на i-му переході.

HMP оптимізує баланс між проактивністю (швидка локальна реакція) та реактивністю (економія ресурсів для рідкісних глобальних комунікацій).

Визначення умов стабільності роботи протоколу

Також слід зазначити, що стабільність для mesh-мережі означає відсутність флуктуацій маршрутів (route flapping), збіжність алгоритму і обмежений час реакції на зміну топології. Тому маршрут вибирається як

$$P^* = arg\ arg \sum_{(u,v)\in P} M_{uv} \ . \tag{20}$$

Для $M_{uv}(t)$, яка змінюється в часі, система стабільна, якщо

$$|M_{uv}(t+1) - M_{uv}(t)| < \varepsilon, \tag{21}$$

де ε – це допустиме відхилення, яке визначає, наскільки може змінитися метрика каналу між двома послідовними моментами часу без ініціювання перебудови маршруту. Тобто зміни метрики обмежені. Якщо варіація перевищує поріг, маршрути починають часто перебудовуватись. Для уникнення цього вводиться експоненційне згладжування

$$M'_{uv}(t) = \lambda M_{uv}(t) + (1-\lambda) M'_{uv}(t-1), \tag{22}$$

де λ – це коефіцієнт згладжування, який визначає, наскільки сильно нове вимірювання впливає на оновлену метрику каналу, $0 < \lambda < 1$. Її введення зменшує осциляції мережі.

Час збіжності визначається:

$$T_{conv} = D \cdot T_{loc}, \tag{23}$$

де D – діаметр графа (максимальна кількість переходів), T_{loc} – період локальних оновлень. Отже збіжність масштабується лінійно з діаметром мережі.

Система лишається стабільною, якщо:

$$\frac{dM_{uv}}{dt} < \frac{\vartheta}{D}, \tag{24}$$

де ϑ – поріг зміни маршруту. Інакше система переходить у режим постійної перебудови.

Виходячи з цього можна визначити компроміс стабільності та адаптивності системи. Отже маємо фундаментальний баланс для:

– малого T_{glob} притаманна краща оптимізація, але породжуєть великий контрольний трафік;

– великого T_{glob} притаманне менше навантаження, але з'являється повільніша реакція на зміни системи.

Таким чином можна визначити оптимальне значення:

$$\frac{N^2}{T_{glob}} \ll \lambda_{data}. \tag{25}$$

У порівняння стабільності з іншими підходами треба зазначити, що У BATMAN стабільність вища через відсутність глобальних перерахунків, у OLSR стабільність нижча через повну карту топології, тому запропонований HMP займає проміжну позицію.

6. Слабкі місця протоколу та напрямки вдосконалення.

Аналіз показує, що локальна частина протоколу масштабується лінійно, а глобальна частина – квадратично, але керується періодом оновлення. В той самий час стабільність залежить від швидкості зміни каналу, діаметра мережі, коефіцієнта згладжування і порогу зміни маршруту. Таким чином HMP можна налаштувати або як більш стабільний (наближений до BATMAN) або більш оптимізуючий (наближений до глобальних протоколів). Можна також виділити слабкі місця нового протоколу:

1. Контрольні додаткові витрати (хоча обмежений настройкою T_{glob}, глобальні оновлення створюють додатковий трафік порівняно з BATMAN). Перехід між проактивною та реактивною фазами може спричинити несумісності таблиць, призводячи до тимчасових петель (ймовірність ~0,1 при високій мобільності). Успадкована від BATMAN реактивна частина може ігнорувати асиметрію, збільшуючи втрати пакетів на 10–15%.

2. Ефективність адаптивного механізму HMP критично залежить від точності вимірювання мережевих метрик (RSSI, ETX, затримок). Неточні або зашумлені вимірювання можуть призвести до неоптимальних рішень про вибір режиму. Проблема особливо гостра в умовах високої інтерференції в безпроводовому середовищі, швидкої зміни умов поширення радіохвиль, обмежених можливостей вимірювального обладнання та асинхронності вимірювань на різних вузлах. Складність налаштування вагових коефіцієнтів α, β і γ або їх неправильний вибір може призвести до субоптимальних маршрутів. Неправильний вибір k також призводить до неоптимальної роботи мережі: занадто малий – часті реактивні запити; занадто великий – високі накладні.

3. Гібридна природа протоколу вимагає підтримки двох окремих підсистем маршрутизації (проактивної та реактивної), що збільшує складність імплементації та обсяг коду. Необхідність синхронізації між модулями та управління переходами між режимами додає додаткові точки потенційних помилок. Це може ускладнити тестування, налагодження та підтримку протоколу порівняно з простішими монолітними рішеннями. Затримка в адаптації (при швидких змінах топології глобальні оновлення можуть запізнюватись). У надвеликих мережах (для $N > 1000$) реактивний флудинг може перевантажити мережу, подібно до AODV. Хоча HMP теоретично має кращу масштабованість за повністю проактивні протоколи, в мережах з тисячами вузлів можуть виникати проблеми зростання розміру таблиць маршрутизації навіть для обмеженого набору проактивних призначень, збільшення часу конвергенції при масштабних змінах топології, проблеми з синхронізацією версій протоколу між великою кількістю вузлів і потенційні «шторми» RREQ повідомлень при масових реактивних запитах. Для надвеликих мереж може знадобитися впровадження ієрархічної структури або кластеризації.

4. Адаптивний диспетчер потребує постійного моніторингу мережевих метрик та обчислення функцій корисності для прийняття рішень про вибір режиму. Це створює додаткові обчислювальні витрати, які можуть бути значними на ресурсообмежених пристроях (IoT вузли, сенсорні мережі). Процесор та пам’ять, використані для аналізу метрик, не можуть бути задіяні для обробки корисного трафіку. Вразливість до шуму вимірювань (вимірювання QoS параметрів, таких як затримки і втрати, можуть бути нестабільними).

5. Відсутність вбудованої криптографії робить вразливим до атак на OGM або RREQ/RREP. HMP успадковує вразливості як проактивних, так і реактивних протоколів можливість атак типу «чорна діра» через маніпуляцію метриками якості, вразливість до DoS атак через флуд RREQ повідомлень, потенційна підробка OGM повідомлень для захоплення трафіку, складність впровадження наскрізного шифрування на рівні L2, можливість витоку інформації про топологію мережі через beacon повідомлення. Необхідна розробка додаткових механізмів автентифікації та перевірки цілісності для захисту службових повідомлень протоколу.

Крім того в умовах швидко змінюваної топології або граничних значень метрик, система може постійно переключатися між проактивним та реактивним режимами, викликаючи «мерехтіння» всієї мережі або окремих її сегментів. Часті переключення призводять до нестабільності маршрутів, додаткових накладних витрат на реорганізацію таблиць маршрутизації, ускладнення прогнозування поведінки мережі та зниження ефективності кешування маршрутів. Для зменшення вливу цієї особливості роботи необхідно впроваджувати механізми гістерезису в функції корисності, яка запобігає частим переключенням при незначних коливаннях метрик.

Незважаючи на адаптивність, в умовах критично низького заряду батареї на більшості вузлів, протокол може не мати достатньо інформації для прийняття оптимальних рішень. Постійна робота модуля виявлення сусідів споживає енергію навіть коли вузол не бере активної участі в передачі даних, що може бути неприйнятним для вузлів з дуже обмеженими енергетичними ресурсами.

HMP забезпечує кращу якість маршрутів та гнучкість завдяки комбінуванню локальних і глобальних метрик, але це дається ціною певного додаткового контролю у порівнянні із аналогічними протоколами (табл. 2).

Новий гібридний протокол HMP поєднує сильні сторони L2 підходів (низький оверхед, локальні рішення) з глобальною оптимізацією шляхів та підтримкою QoS. Математичні моделі дозволяють формалізувати вибір найкращих шляхів з урахуванням якості зв’язків, затримки та втрат. Порівняння із BATMAN та іншими рішеннями показало, що HMP досягає кращої адаптивності та якості маршрутизації за помірного контролю. Проте існують слабкі місця, пов’язані з оверхедом та необхідністю тонкого налаштування параметрів.

Таблиця 2

Порівняння запропонованого протоколу до існуючих протоколів

Характеристика	BATMAN	OLSR/HWMP	HMP (запропонований)
Локальні метрики	так	ні	так
Глобальна оптимізація	Ні	так	так
Підтримка QoS	ні	обмежено	так
Контрольні додаткові витрати	низький	високий	середній
Адаптація до трафіку	середня	середня	висока
Складність реалізації	низька	висока	середня

7. Висновки та перспективи подальших досліджень

У роботі розроблено та теоретично обґрунтовано гібридний протокол маршрутизації HMP рівня L2 для безпроводових mesh-мереж. Запропоноване рішення ефективно поєднує локальні метрики якості каналів BATMAN-подібного типу для проактивної маршрутизації в обмежених зонах (глибина 3–5 переходів) з реактивними механізмами пошуку маршрутів і модулем QoS, що дозволяє динамічно адаптуватися до змін топології, характеру трафіку та вимог до затримки, пропускної здатності й втрат пакетів. Математичні моделі, сформульовані в роботі, дають змогу точно оцінювати середню затримку доставки, загальне контрольне навантаження, час конвергенції та умови стабільності системи з використанням експоненційного згладжування для запобігання флуктуаціям маршрутів. Теоретичний аналіз підтвердив зменшення накладних витрат на 50–80% порівняно з BATMAN у великих мережах, лінійне масштабування локального трафіку, кращу адаптивність до мобільних сценаріїв і повноцінну підтримку QoS. Порівняння з відомими гібридними протоколами показало переваги HMP у динамічних і гетерогенних mesh-мережах, хоча в статичних умовах HWMP може зберігати певну перевагу завдяки фокусу на деревоподібних структурах. Разом з тим виявлено низку слабких місць: потенційні тимчасові петлі при перемиканні режимів, висока залежність від точності вимірювання метрик, підвищена складність реалізації та обчислювальні витрати на ресурсообмежених пристроях, а також відсутність вбудованих механізмів безпеки (вразливість до атак маніпуляції метриками, DoS через флуд RREQ).

Перспективи подальших досліджень охоплюють імітаційне моделювання протоколу в середовищах NS-3 та OMNeT++ для оцінки продуктивності в реалістичних сценаріях (висока мобільність, щільна інтерференція, гетерогенне обладнання) і розробку та експериментальну верифікацію програмної реалізації HMP на реальному тестовому стенді mesh-мережі.

Внесок авторів. Михайло Лобур – концептуалізація; методика; Олексій Джусь – програмне забезпечення; Олексій Джусь – збір і перевірка емпіричних даних; Олексій Джусь – емпіричне дослідження; Олексій Джусь – аналіз джерел, підготовка огляду літератури або теоретичних основ дослідження.

Декларація про штучний інтелект

Під час підготовки цієї роботи автори використовували програми штучного інтелекту Grammarly Pro для виправлення граматики тексту та Strike Plagiarism для пошуку можливого плагіату. Після використання цього інструменту автори переглянули та відредагували контент за потреби й взяли на себе повну відповідальність за зміст публікації.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Джусь, О., & Лобур, М. (2025). Аналіз стану та проблем функціонування безпроводових ad hoc та mesh мереж. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 727–751. https://doi.org/10.28925/2663-4023.2025.30.914

2. Chang, R., Chen, W., & Wen, Y. (2003). Hybrid Wireless Network Protocols. IEEE Trans. Veh. Technol., 52, 1099–1109. https://doi.org/10.1109/tvt.2002.807126

3. Long, Y., Huang, G., Tang, D., Zhao, S., & Liu, G. (2021). Achieving High Throughput in Wireless Networks With Hybrid Backscatter and Wireless-Powered Communications. IEEE Internet Things J., 8, 10896–10910. https://doi.org/10.1109/jiot.2021.3051344

4. Kim, S., & Kim, D. (2017). Hybrid Backscatter Communication for Wireless-Powered Heterogeneous Networks. IEEE Trans. Wirel. Commun., 16, 6557–6570. https://doi.org/10.1109/twc.2017.2725829

5. Attar, H., Solyman, A., Alrosan, A., Chakraborty, C., & Khosravi, M. (2021). Deterministic Cooperative Hybrid Ring-Mesh Network Coding for Big Data Transmission over Lossy Channels in 5G Networks. EURASIP J. Wirel. Commun. Netw., 2021. https://doi.org/10.1186/s13638-021-02032-z

6. Yang, K., J., & Miao, Z. (2009). Hybrid Routing Protocol for Wireless Mesh Network. In 2009 Int. Conf. on Computational Intelligence and Security, 1, 547–551. https://doi.org/10.1109/cis.2009.48

7. Triviño, A., Ariza, A., Casilari, E., & Cano, J. (2013). Cooperative Layer-2 based Routing Approach for Hybrid Wireless Mesh Networks. China Commun., 10, 88–99. https://doi.org/10.1109/cc.2013.6633748

8. Chai, Y., Shi, W., Shi, T., & Yang, X. (2017). An Efficient Cooperative Hybrid Routing Protocol for Hybrid Wireless Mesh Networks. Wirel. Netw., 23, 1387–1399. https://doi.org/10.1007/s11276-016-1229-8

9. Gunasekaran, K., Verma, S., Johnsana, J., Tamilarasan, N., & Sahayaraj, J. (2024). An Innovative Regional Condition Hybrid Routing Protocol Accessing in Wireless Networks. In 2024 9th Int. Conf. on Communication and Electronics Systems (ICCES), 647–652. https://doi.org/10.1109/icces63552.2024.10860076

10. Huang, T., & Li, Y. (2021). Quality of Service (QoS)-based Hybrid Optimization Algorithm for Routing Mechanism of Wireless Mesh Network. Sens. Mater. https://doi.org/10.18494/sam.2021.3383

11. Bae, S., & Ko, Y. (2010). Efficient Layer-2 Multicasting for IEEE 802.11s based Wireless Mesh Networks. In 2010 2nd Int. Conf. on Ubiquitous and Future Networks (ICUFN), 109–114. https://doi.org/10.1109/icufn.2010.5547223

12. Singh, M., & Talasila, V. (2015). A Practical Evaluation for Routing Performance of BATMAN-ADV and HWMN in a Wireless Mesh Network Test-Bed. In 2015 Int. Conf. on Smart Sensors and Systems (IC-SSS), 1–6. https://doi.org/10.1109/smartsens.2015.7873617

13. Jiang, H., Lu, L., Han, G., Wang, H., S., & Sun, R. (2018). Routing Algorithm for Supporting Data-Differentiated Service in Hybrid Wireless Mesh Networks in Underground Mines. Int. J. Distrib. Sens. Netw., 14. https://doi.org/10.1177/1550147718812024

14. Nanda, A., Nanda, P., He, X., Jamdagni, A., & Puthal, D. (2020). A Hybrid Encryption Technique for Secure-GLOR: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks. Future Gener. Comput. Syst., 109, 521–530. https://doi.org/10.1016/j.future.2018.05.065

15. Ganta, S., Malleswara, N., & Nallamothu, R. (2025). A Dynamic Integrity and Data Confidentiality based Wireless N2N Data Communication and Security Protocol on Large Networks. Int. J. Comput. Exp. Sci. Eng. https://doi.org/10.22399/ijcesen.720

16. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M., Rahimova, I., Kravchenko, V., & Cherniavskiy, O. (2024). Development of Functionality Principles for the Automated Data Transmission System through Wireless Communication Channels to Ensure Information Protection. East.-Eur. J. Enterpr. Technol. https://doi.org/10.15587/

References

1. Dzhus, O., & Lobur, M. (2025). Analysis of the Status and Problems of the Operation of Wireless Ad Hoc and Mesh Networks. Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(30), 727–751. https://doi.org/10.28925/2663-4023.2025.30.914

2. Chang, R., Chen, W., & Wen, Y. (2003). Hybrid Wireless Network Protocols. IEEE Trans. Veh. Technol., 52, 1099–1109. https://doi.org/10.1109/tvt.2002.807126

3. Long, Y., Huang, G., Tang, D., Zhao, S., & Liu, G. (2021). Achieving High Throughput in Wireless Networks With Hybrid Backscatter and Wireless-Powered Communications. IEEE Internet Things J., 8, 10896–10910. https://doi.org/10.1109/jiot.2021.3051344

4. Kim, S., & Kim, D. (2017). Hybrid Backscatter Communication for Wireless-Powered Heterogeneous Networks. IEEE Trans. Wirel. Commun., 16, 6557–6570. https://doi.org/10.1109/twc.2017.2725829

5. Attar, H., Solyman, A., Alrosan, A., Chakraborty, C., & Khosravi, M. (2021). Deterministic Cooperative Hybrid Ring-Mesh Network Coding for Big Data Transmission over Lossy Channels in 5G Networks. EURASIP J. Wirel. Commun. Netw., 2021. https://doi.org/10.1186/s13638-021-02032-z

6. Yang, K., J., & Miao, Z. (2009). Hybrid Routing Protocol for Wireless Mesh Network. In 2009 Int. Conf. on Computational Intelligence and Security, 1, 547–551. https://doi.org/10.1109/cis.2009.48

7. Triviño, A., Ariza, A., Casilari, E., & Cano, J. (2013). Cooperative Layer-2 based Routing Approach for Hybrid Wireless Mesh Networks. China Commun., 10, 88–99. https://doi.org/10.1109/cc.2013.6633748

8. Chai, Y., Shi, W., Shi, T., & Yang, X. (2017). An Efficient Cooperative Hybrid Routing Protocol for Hybrid Wireless Mesh Networks. Wirel. Netw., 23, 1387–1399. https://doi.org/10.1007/s11276-016-1229-8

9. Gunasekaran, K., Verma, S., Johnsana, J., Tamilarasan, N., & Sahayaraj, J. (2024). An Innovative Regional Condition Hybrid Routing Protocol Accessing in Wireless Networks. In 2024 9th Int. Conf. on Communication and Electronics Systems (ICCES), 647–652. https://doi.org/10.1109/icces63552.2024.10860076

10. Huang, T., & Li, Y. (2021). Quality of Service (QoS)-based Hybrid Optimization Algorithm for Routing Mechanism of Wireless Mesh Network. Sens. Mater. https://doi.org/10.18494/sam.2021.3383

11. Bae, S., & Ko, Y. (2010). Efficient Layer-2 Multicasting for IEEE 802.11s based Wireless Mesh Networks. In 2010 2nd Int. Conf. on Ubiquitous and Future Networks (ICUFN), 109–114. https://doi.org/10.1109/icufn.2010.5547223

12. Singh, M., & Talasila, V. (2015). A Practical Evaluation for Routing Performance of BATMAN-ADV and HWMN in a Wireless Mesh Network Test-Bed. In 2015 Int. Conf. on Smart Sensors and Systems (IC-SSS), 1–6. https://doi.org/10.1109/smartsens.2015.7873617

13. Jiang, H., Lu, L., Han, G., Wang, H., S., & Sun, R. (2018). Routing Algorithm for Supporting Data-Differentiated Service in Hybrid Wireless Mesh Networks in Underground Mines. Int. J. Distrib. Sens. Netw., 14. https://doi.org/10.1177/1550147718812024

14. Nanda, A., Nanda, P., He, X., Jamdagni, A., & Puthal, D. (2020). A Hybrid Encryption Technique for Secure-GLOR: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks. Future Gener. Comput. Syst., 109, 521–530. https://doi.org/10.1016/j.future.2018.05.065

15. Ganta, S., Malleswara, N., & Nallamothu, R. (2025). A Dynamic Integrity and Data Confidentiality based Wireless N2N Data Communication and Security Protocol on Large Networks. Int. J. Comput. Exp. Sci. Eng. https://doi.org/10.22399/ijcesen.720

16. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M., Rahimova, I., Kravchenko, V., & Cherniavskiy, O. (2024). Development of Functionality Principles for the Automated Data Transmission System through Wireless Communication Channels to Ensure Information Protection. East.-Eur. J. Enterpr. Technol. https://doi.org/10.15587/

Надійшла до редакції: 05.12.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26