Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження методів багатошляхової маршрутизації в безпроводових мережах

Виконав:
студент 2 курсу, групи ТСМм-19-1
Барсук В.О.
(прізвище, ініціали)

Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Телекомунікаціні системи та мережі
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Мельнікова Л.І
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2021р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Телекомунікаціні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ

Зав. кафедри _____
(підпис)

«____» _____2021р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Барсуку Валерію Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів багатошляхової маршрутизації в безпроводових мережах
затверджена наказом по університету від «10» березня 2021р. №343 Ст.

2. Термін подання студентом роботи до екзаменаційної комісії 20.05.2021р.

3. Вихідні дані до роботи: Протоколи маршрутизації OLSRv2 та MP-OLSR, площа обслуговування 1500 мх1500 м, час модулювання 100 с, модель фізичного рівня PHY 802.11 b, частота радіоканалу 2,4 GHz, швидкість передачі 11 Mbps, розмір пакету 512 bytes.

4. Перелік питань, що потрібно опрацювати в роботі:

1) Аналіз існуючих методик маршрутизації
2) Особливості маршрутизації у безпроводових мережах
3) Протоколи багатошляхової маршрутизації в MANET
4) Дослідження протоколів багатошляхової маршрутизації

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент кафедри ІКІ ім. В.В. Поповського Мельнікова Любов Іванівна		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2021	Виконано
2	Збір матеріалів для дослідження	25.02.2021	Виконано
3	Розробка 1 розділу	05.03.2021	Виконано
4	Розробка 2 розділу	15.03.2021	Виконано
5	Розробка 3 розділу	25.03.2021	Виконано
6	Розробка 4 розділу	07.04.2021	Виконано
7	Оформлення кваліфікаційної роботи	18.05.2021	Виконано

Дата видачі завдання 15 лютого 2021 року

Студент _____ Барсук В.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Мельнікова Л.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 88 с., 41 рис., 6 табл., 3 додатки, 27 джерел.

MANET, OLSR, MP-OLSR, AD HOC, БАГАТОШЛЯХОВА МАРШРУТИЗАЦІЯ, БАГАТОШЛЯХОВИЙ АЛГОРИТМ ДЕЙКСТРИ, БЕЗПРОВОДОВІ МЕРЕЖІ

Об'єкт дослідження: дослідження методів багатошляхової маршрутизації в безпроводових мережах.

Предмет дослідження: багатошляхова маршрутизація в безпроводових, мобільних мережах.

Методи досліджень: аналіз, збір, узагальнення результатів та формування висновків, методи імітаційного моделювання.

У кваліфікаційній магістерській роботі проведено дослідження протоколів багатошляхової маршрутизації в безпроводових MANET мережах. Розглянуто принципи організації, основи функціонування та особливості маршрутизації в MANET мережах. Представлені характеристики протоколів всіх груп з точки зору забезпечення мережевої продуктивності. Проведено порівняльний аналіз протоколу OLSR і його модифікації MP-OLSR.

ABSTRACT

The report contains: 88 p., 41 fig., 6 tables, 27 sources.

MANET, OLSR, MP-OLSR, AD HOC, MULTI-WAY ROUTING, MULTI-PATH DIJKSTRA ALGORITHM, WIRELESS NETWORK

Object of research: methods of multi-path routing in wireless networks.

Subject of research: multi-way routing in wireless, mobile networks.

Research methods: analysis, collection, generalization of results and formation of conclusions, methods of simulation modeling.

An aim of work is research of protocols of multipath routing in wireless MANET networks. The principles of organization, basics of functioning and features of routing in MANET networks are considered. The principles of organization, basics of functioning and features of routing in MANET networks are considered. The characteristics of the protocols of all groups in terms of network performance are presented. A comparative analysis of the OLSR protocol and its modification MP-OLSR.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AODV (Ad hoc Ondemand Distance Vector routing) – протокол динамічної маршрутизації для мобільних ad-hoc мереж

ARP (Address Resolution Protocol) – протокол визначення адресу

DSR (Dynamic Source Routing) – динамічна маршрутизація від джерела

ECMP (Equal Cost Multipath) – рівні багатошляхові вартості

EIGRP (Enhanced Interior Gateway Routing Protocol) – покращений IGRP

IGRP (Interior Gateway Routing Protocol) – внутрішній маршрутизуючий протокол шлюзу

IS-IS (Intermediate System To Intermediate System) – взаємодія проміжних систем

MANET (Mobile Ad hoc NETwork) – мобільна однорангова мережа

MP-OLSR (MultiPath OLSR) – багатошляховий оптимізований протокол стану каналу

OLSR (Optimized Link State Routing protocol) – оптимізований протокол стану каналу

OMP (Optimized Multipath) – оптимізований багатошляховый

OSPF (Open Shortest Path First) – відкритий SPF

QoS (Quality of service) – якість обслуговування

RIP (Routing Information Protocol) – протокол маршрутної інформації

RREP (Request Response) – відповідь на запит

RREQ (Route Requests) – запит маршруту

SPF (Shortest Path First) – перший найкоротший шлях

TC (Topology Control) – контроль топології

TCP (Transmission Control Protocol) – протокол керування передачею

ZRP (Zone Routing protocol) – зонний протокол маршрутизації

ВСТУП

Питання маршрутизації стоїть гостро в спеціалізованих мережах Mobile Ad hoc NETwork (MANET). Це тип мережі спонтанний, самоорганізований і самопідтримуваний без будь-якої інфраструктури [1, 2]. Маршрутизація по найкоротшому шляху може призвести до незбалансованого розподілу трафіку – канали, через які проходить найкоротший шлях, стають перевантаженими, у той час як інші ділянки мережі простоюють.

Багатошляхова маршрутизація була запропонована як альтернатива маршрутизації по єдиному найкоротшому шляху для розподілу навантаження і зменшення ймовірності виникнення перевантаження в мережі [3].

Таким чином, протоколи багатошляхової маршрутизації дозволяють підвищити ефективність маршрутизації, тобто забезпечують підвищення продуктивності мережі [4]. Багатошляхова маршрутизація реалізована в таких протоколах як Open Shortest Path First (OSPF), MultiPath Optimized Link State Routing protocol (MP-OLSR) та ін[2].

Для вирішення задач масштабованості, безпеки, часу життя мережі, нестійкості безпроводових передачі, та адаптації до медіа додатків у розглянутій літературі пропонується впровадження багатошляховий алгоритму Дейкстри в існуючі протоколи маршрутизації Optimized Link State Routing protocol (OLSR)[5, 6]. Одночасно виникає задача сумісності багатошляхового протоколу з існуючими, що дозволить використовувати мережу, яка вже існує.

У кваліфікаційній магістерській роботі проведено дослідження протоколів багатошляхової маршрутизації, які використовуються в MANET мережах, з метою визначення протоколу, що забезпечує найбільш високу продуктивність мережі. Розглядається можливість і досліджується ефективність впровадження багатошляхового алгоритму Дейкстри в протокол маршрутизації для мобільних безпроводових мереж.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДИК МАРШРУТИЗАЦІЇ

1.1 Задача маршрутизації і розподілу інформаційних потоків в сучасних мультисервісних мережах

Задача маршрутизації в загальному випадку полягає в знаходженні оптимального за деякими критеріями шляху або безлічі шляхів для обслуговування трафіку користувачів.

Основні цілі маршрутизації полягають у мінімізації (максимізації) значень обраних показників якості обслуговування (швидкості передачі, середньої затримки, джитера, втрат пакетів й ін.), а також у забезпеченні збалансованого завантаження мережі, її канальних і буферних ресурсів. Тому основними задачами, які належать до галузі маршрутизації, є: контроль і збір інформації про стан мережі (її топології, завантаження мережних ресурсів тощо), розрахунок шуканих шляхів (маршрутів) і реалізація маршрутних рішень.

Мережний рівень за допомогою маршрутизації також реалізує функції об’єднання мереж, побудованих з використанням різнотипних технологій, що використовують різні принципи адресації, пересилання даних, управління (рис. 1.1). Для об’єднання мереж на третьому рівні EMBBC, як правило, використовується спеціальний пристрій — маршрутизатор мережі, який підтримує різні технології канального рівня (на рис. 1.1 технології Frame Relay і Fast Ethernet) і обробляє блоки даних мережного рівня. При такому підключенні протокольні особливості локалізуються в межах однієї ділянки мережі, а пересилання пакетів здійснюється на базі єдиного протоколу мережного рівня, який має бути налаштований на кожному кінцевому пристрої.

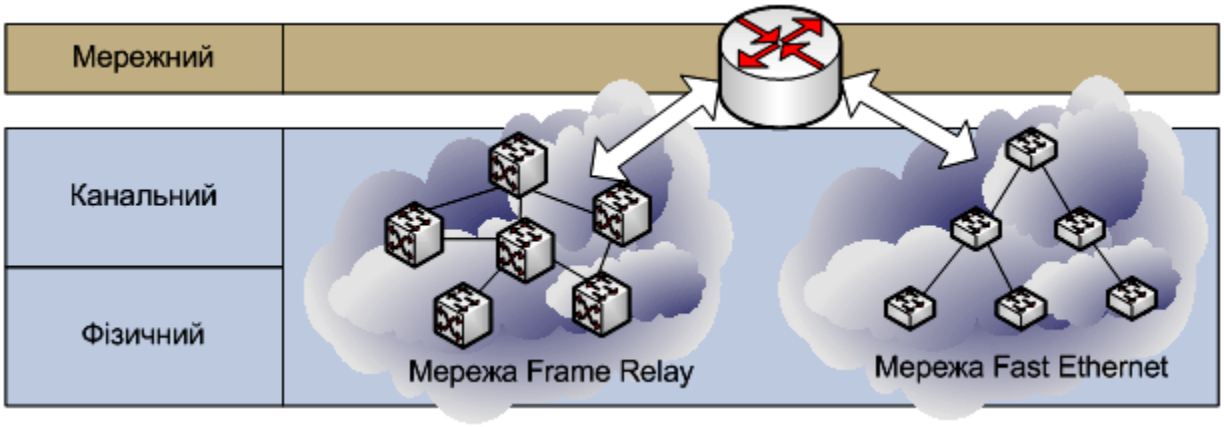


Рисунок 1.1 – Побудова об’єднаної мережі

Інформація про маршрути зберігається на маршрутизаторі у вигляді спеціальних інформаційних структур, які називаються маршрутними таблицями (МТ). Основна робота зі створення таблиць маршрутизації виконується автоматично, але передбачається й можливість корегування або доповнення їх вручну, тобто адміністративно. Для автоматичної побудови таблиць маршрутизатори обмінюються інформацією про топологію об’єднаної мережі у відповідності зі спеціальним службовим протоколом. Протоколи цього типу називаються протоколами маршрутизації або маршрутними протоколами.

Вибір протоколу маршрутизації (routing protocols) — це досить складне та багатопланова задача. Під час його розв’язання слід враховувати такі основні фактори:

- розмір і зв’язність топології мережі (кількість мережних вузлів і трактів передачі, порядок їхнього з’єднання), а також планове зростання або зміну її структури;
- характер і обсяг мережного трафіка;
- підтримуваний рівень безпеки та надійності;
- вимоги до якості обслуговування;
- необхідність підтримки масок змінної довжини (VLSM).

На сьогодні на практиці паралельно функціонує у різних мережних технологіях ціла низка різноманітних за своїми функціональними можливостями протоколів маршрутизації. У мережах IP успішно застосовуються протоколи RIP (Routing Information Protocol), IGRP (Internet Gateway Routing Protocol), Enhanced

IGRP, OSPF (Open Shortest Path First), IS-IS (Intermediate System-to-Intermediate System), BGP (Border Gateway Protocol) та EGP (Exterior Gateway Protocol). У технології ATM підтримуються протоколи IISP (Interim Inter-Switch Protocol) і PNNI (Private Network — Network Interface). У стеку Novell функції маршрутизації реалізує протокол NLSP (NetWare Link Services (State) Protocol).

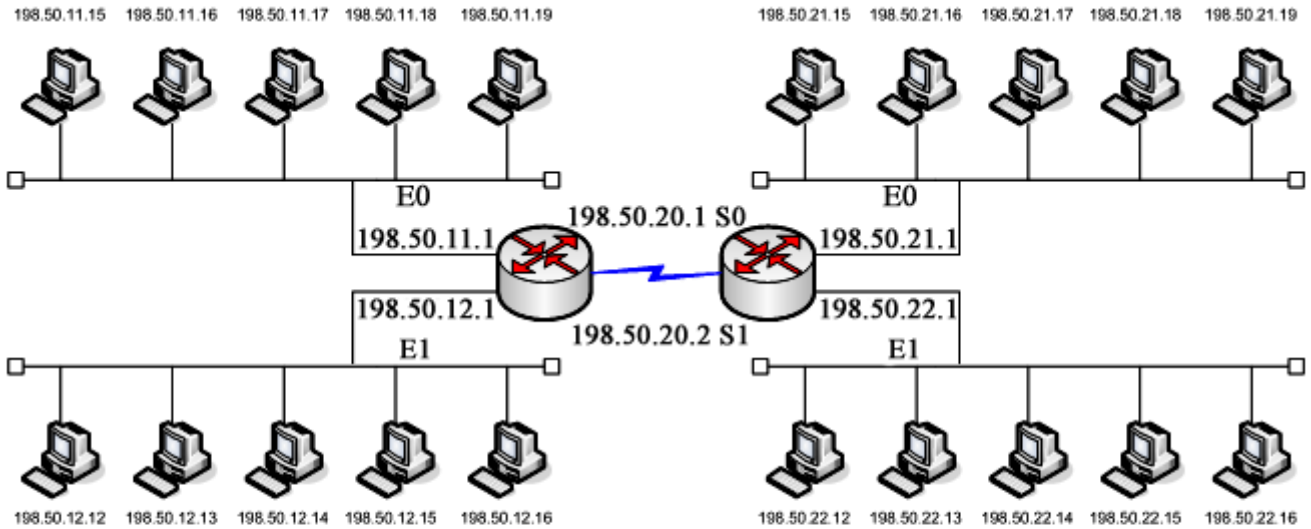
Маршрутні протоколи слід відрізняти від власне мережних протоколів, таких як IP, IPX або AppleTalk. І ті й інші забезпечують функції мережного рівня моделі OSI, тобто беруть участь у доставці пакетів адресатові через різнорідну об'єднану мережу. Але в той час як перші збирають і передають мережею винятково службову інформацію, другі призначені для передачі користувальницьких даних так само, як це роблять протоколи канального рівня. Протоколи маршрутизації використовують мережні протоколи як транспортний засіб. Тому протокол маршрутизації — це протокол, який підтримує мережні протоколи й надає механізми обміну маршрутною інформацією. При обміні маршрутною інформацією пакети протоколу маршрутизації містяться в полі даних пакетів мережного або навіть транспортного рівня, тому з погляду вкладеності пакетів протоколи маршрутизації формально слід було б віднести до більш високого рівня, ніж мережний.

У тому, що маршрутизатори для прийняття рішення щодо транспортування пакета звертаються до адресних таблиць, можна побачити їх подібність із мостами та комутаторами. Однак природа використовуваних ними адресних таблиць значно розрізняється. Замість MAC-адрес у таблицях маршрутизації вказуються номери мереж, які зібрані в об'єднану мережу. Іншою відмінністю таблиць маршрутизації від адресних таблиць мостів є спосіб їхнього створення. У той час як міст будує таблицю, пасивно спостерігаючи за минаючими через нього інформаційними кадрами, що посилають через нього кінцеві вузли мережі один одному, маршрутизатори самі ініціюють обмін спеціальними службовими пакетами, повідомляючи сусідам про відомі їм мережі, маршрутизатори та про зв'язки цих мереж з маршрутизаторами. Крім топології зв'язків враховуватися при розрахунку шляхів може також і їхня пропускна здатність. Це дозволяє маршрутизаторам швидше адаптуватися до змін конфігурації мережі, а також правильно передавати пакети в мережах з довільною топологією, що допускає наявність контурів.

За допомогою протоколів маршрутизації маршрутизатори складають карту зв'язків мережі того чи іншого ступеня детальності. На підставі цієї інформації

для кожного номера мережі приймається рішення про те, якому наступному маршрутизатору слід передавати пакети, що направляються за даною адресою, щоб маршрут виявився раціональним. Результати таких рішень заносяться в таблицю маршрутизації (рис. 1.2). Маршрутизатори зберігають і оновлюють таку важливу інформацію в таблицях маршрутизації:

- тип протоколу, тобто інформацію про протокол маршрутизації, який зробив запис у таблиці маршрутизації;
- зв'язку одержувач/наступний вузол, яка повідомляє маршрутизатору про те, що вузол-одержувач або підключений безпосередньо, або може бути досягнутий через інший маршрутизатор — наступний транзитний вузол (next hop), що перебуває на шляху до пункту призначення. Маршрутизатор аналізує адресу одержувача у вхідних пакетах і порівнює її на відповідність із записами в таблиці маршрутизації;
- метрики маршрутизації (див. нижче);
- вихідний інтерфейс — інтерфейс, через який мають бути відправлені дані, щоб досягти пункту призначення.



Таблиця маршрутизації

Звідки отримано	Мережна адреса	Лічильник вузлів	Інтерфейс
C	192.50.11.0	0	E0
C	192.50.12.0	0	E1
C	192.50.13.0	0	S0
R	192.50.14.0	1	S0
R	192.50.15.0	1	S0

Таблиця маршрутизації

Звідки отримано	Мережна адреса	Лічильник вузлів	Інтерфейс
C	192.50.21.0	0	E0
C	192.50.22.0	0	E1
C	192.50.23.0	0	S1
R	192.50.24.0	1	S1
R	192.50.25.0	1	S1

Рисунок 1.2 - Приклад маршрутної таблиці

Метрики протоколів маршрутизації. Критерієм вибору того чи іншого шляху між заданою парою вузлів мережі є мінімум або максимум його «довжини» (ваги, вартості), поданої у вигляді суми «довжин» трактів передачі, які цей шлях утворює. «Довжина» тракту передачі в термінах протоколів маршрутизації називається його метрикою (routing metric). В існуючих протоколах маршрутизації залежно від особливостей розв'язуваної маршрутної задачі використовується досить широкий перелік метрик, які характеризують різні за своєю природою властивості того чи іншого тракту передачі, а саме його фізичну довжину, надійність, пропускну здатність, завантаженість, вартість й ін. (рис. 1.3).

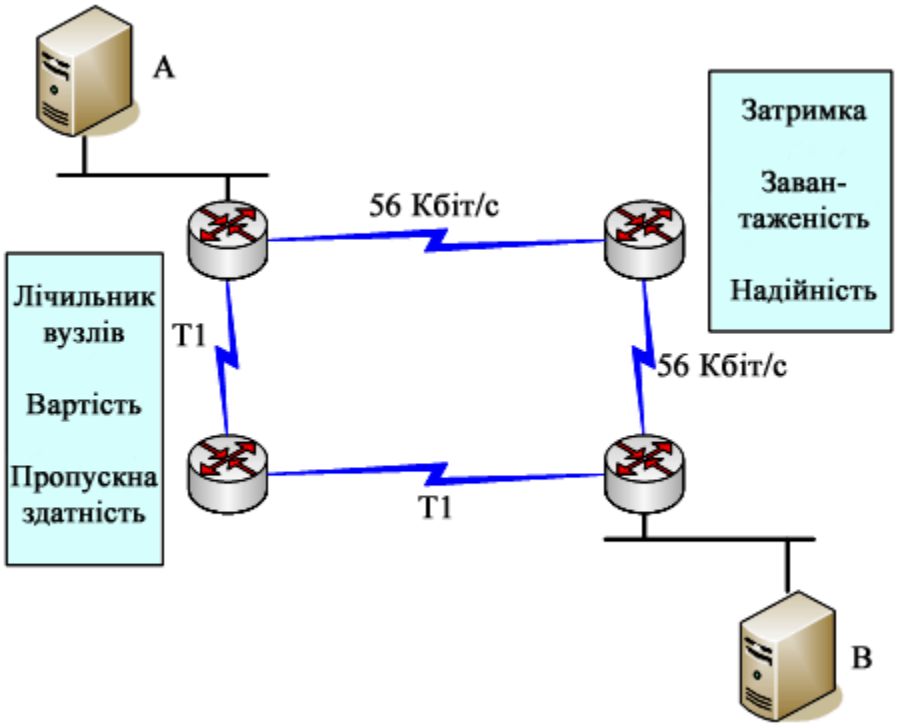


Рисунок 1.3 - Метрики маршрутизації

Окрім того, що метрика тракту передачі може автоматично обчислюватися засобами того чи іншого протоколу маршрутизації, вона також може встановлюватися й адміністративно.

Під час розробки протоколів маршрутизації необхідно задовольнити ряду важливих, але іноді суперечливих вимог:

1. Оптимальність, яка характеризує здатність протоколу забезпечувати вибір найкращого в рамках певних критеріїв шляху (множини шляхів), напри-

клад, шлях з мінімальною кількістю переприйомів або шлях, який має максимальну пропускну здатність.

2. Простота апаратно-програмної реалізації та мінімальні обсяги створюваного службового трафіка при зборі даних про стан ТКС або розсиланні інформації управління.

3. Стійкість, яка характеризує здатність протоколу забезпечувати ефективне розв'язання маршрутних задач в умовах непередбаченої зміни умов функціонування мережі, наприклад, при відмові мережного обладнання, сплеску абонентського навантаження та ін..

4. Висока оперативність одержання остаточних маршрутних рішень, особливо в умовах реалізації розподіленої маршрутизації, пов'язаної із забезпеченням збіжності відповідних обчислювальних алгоритмів з розрахунку шуканих шляхів.

5. Адаптивність, пов'язана зі здатністю протоколу постійно (періодично) відстежувати та своєчасно реагувати на поточні зміни топології мережі, параметрів мережних вузлів (розміри черг) і трактів передачі (пропускна здатність, затримки, втрати пакетів), а також характеристик абонентського навантаження.

6. Масштабованість, яка характеризує здатність протоколу виконувати визначені функції із заданою якістю при збільшенні розмірності мережі (числа мережних вузлів, трактів передачі та ін.).

Найбільш повно вимогам щодо простоти та масштабованості, відповідає статична маршрутизація, у ході якої маршрутні таблиці формуються адміністративно й у процесі функціонування мережі залишаються незмінними. Динамічна маршрутизація, у ході якої зміст маршрутних таблиць автоматично корегується відповідно до зміни стану (наприклад, топології та/або завантаженості) мережі, є засобом задоволення вимог, пов'язаних із забезпеченням стійкості, адаптивності та оптимальності рішень [6].

Традиційні схеми (або алгоритми) динамічної маршрутизації виробляють пошук єдиного найкоротшого шляху на підставі інформації, отриманої в результаті обміну з сусідніми пристроями. Найбільш популярні математичні алгоритми, використовувані для знаходження найкоротшого шляху, Беллмана-Форда і Дейкстри, званого в західній літературі SPF (Shortest Path First)

алгоритмом. Практична реалізація цих математичних алгоритмів отримала розвиток в протоколах RIP і OSPF відповідно. Надалі в протоколах RIP і OSPF була реалізована ідея знаходження безлічі найкоротших шляхів з однаковою вартістю. Незважаючи на те, що вищенаведені протоколи знаходять єдиний або безліч найкоротших за вартістю шляхів, відсутність обліку обмежень і доступних мережевих ресурсів не дозволяють використовувати ці протоколи в класичному вигляді для маршрутизації в сучасних інформаційно-комунікаційних мережах.

1.2 Класичні протоколи маршрутизації по найкоротшому шляху

Для вирішення задачі знаходження найкоротшого шляху було запропоновано кілька аналітичних алгоритмів, найбільш відомі і часто вживані на практиці - алгоритми Беллмана-Форда і Дейкстри.

Промислова реалізація алгоритму Беллмана-Форда - це протоколи RIPvl і RIPv2 (Routing Information Protocol) для IP мереж. Завдяки простоті настройки, ці протоколи вже протягом 20 років широко використовується для маршрутизації в невеликих і середніх мережах. У ряді фірмових реалізацій підтримується багатоколійні режим роботи, максимальна кількість використовуваних шляхів в цьому випадку дорівнює шести. Недоліками цього протоколу вважається неможливість працювати в великих мережах, оскільки в якості метрики протокол використовує кількість переходів.

Як наслідок, маршрут, обраний таким протоколом, буде оптимальним з точки зору використовуваної метрики (кількості проміжних вузлів), але може не бути оптимальним з точки зору доступності мережевих ресурсів на всіх ділянках обраного шляху.

Інший, широко використовуваний на практиці, спосіб пошуку найкоротшого шляху - алгоритм Дейкстри. Він дозволяє побудувати дерево найкоротших відстаней і шляхів із заданої вершини до всіх інших. Алгоритм застосуємо для орієнтованих, неорієнтованих і змішаних мережевих графів. Згідно з цим алгоритмом, найкоротшим серед всіх найкоротших шляхів від вузла 1 є шлях, що складається з однієї дуги, що з'єднує вузол 1 з найближчим сусіднім вузлом, так як будь-який шлях, що складається з декількох дуг, буде завжди довше довжини першої дуги, внаслідок припущення про позитивності всіх дугових довжин. Наступним найкоротшим серед найкоротших шляхів повинен

бути шлях з однієї дуги до наступного найближчого сусіда вузла 1, або найкоротший шлях з двох дуг, що проходить через вузол, обраний на першому кроці, і т.д.

Так як число операцій, виконуваних алгоритмом Дейкстра на кожному кроці, пропорційно N, а кроки ітеріруются N-1 раз, то обсяг обчислень в гіршому випадку дорівнює O (N2), а не O (N3), як у алгоритму Беллмана-Форда [8].

Цей алгоритм знаходить найкоротший шлях з мінімальними накладними витратами, що є привабливим для реалізації протоколів маршрутизації. Однак в алгоритмі передбачається, що вага дуг заздалегідь відомий. У реальних мережах, обмін сигнальної інформацією значних обсягів може викликати перевантаження, особливо в великих мережах. Тому протоколи, які реалізують алгоритм Дейкстри, працюють в межах певної замкнутої області, яка зазвичай називається автономною системою, а обмін між автономними системами проводиться узагальненими, сумарними маршрутами.

Найбільш відома реалізація алгоритму Дейкстри - протокол OSPF, який по суті є єдиним (за винятком IS-IS) протоколом для внутрішньої маршрутизації в середніх і великих мережах. Як було зазначено вище, великий обсяг сигнальної інформації, необхідний для адекватного вибору маршрутів, визначив ієрархічну структуру побудови мережі на підставі областей. При цьому в кожній мережі повинна бути особлива область, яка називається магістральної, через яку відбувається обмін інформацією з усіма іншими областями.

У загальному випадку розглянуті алгоритми знаходять найкоротший маршрут по мінімуму метрики

$$D_{ij} = \min \sum d_{mk} \qquad (1.1)$$

де D_{ij} - сумарна метрика обраного шляху, d_{mk} - вартість пересилки по ділянці mk, що входить в шлях ij. Однак при виборі цього найкоротшого шляху не враховуються обмеження, які можуть бути накладені з одного боку вимогами до обслуговування трафіку (наприклад, максимальним значенням затримки, SLA), з іншого боку, адміністраторами мережі (наприклад, обмеження системної політики). Крім того, протоколи маршрутизації, реалізовані на базі алгоритмів Беллмана-Форда і Дейкстри, не можуть бути використані для вирішення задачі трафік інжинірингу [9]. У сучасних мережах такі алгоритми повинні використовуватися лише для знаходження доступних найкоротших шляхів і бути одним з елементів більш складної системи маршрутизації, а остаточний вибір

шляху або сукупності шляхів проводиться на підставі комплексних даних, зібраних за допомогою протоколів маршрутизації, сигналізації і з урахуванням оцінки передбачуваної завантаження.

1.3 QoS маршрутизація

Протоколи маршрутизації, які використовуються на сьогоднішній день, підтримують тільки один клас обслуговування, званий best-effort (обслуговування в міру можливості). На відміну від традиційних підходів до вибору шляху, алгоритми QoS маршрутизації при розрахунку оптимального шляху враховують вимоги трафіку і доступність мережевих ресурсів. QoS маршрутизація визначається як механізм вибору шляху, при якому маршрути для потоків визначаються на підставі деяких даних про доступність ресурсів в мережі і QoS вимог потоків. Виходячи з визначення, очевидні дві групи задач, від яких залежить оптимальність вибору маршрутів:

• загальномережеві задачі - збір і аналіз інформації про доступність мережевих ресурсів шляхом обміну сигнальними повідомленнями; критерії вибору оптимальних маршрутів на підставі зібраних даних, алгоритми їх знаходження;

• задачі, пов'язані з визначенням характеристик (середня і пікові швидкості надходження пакетів) і вимог потоків до QoS.

З точки зору збору статистики, аналізу та прийняття рішень маршрутизації, виділяють два підходи QoS маршрутизації - глобальний і локальний. Глобальні (або централізовані) схеми QoS маршрутизації створюють узагальнений вигляд мережі і доступних ресурсів з даного вузла (рис. 1.4).

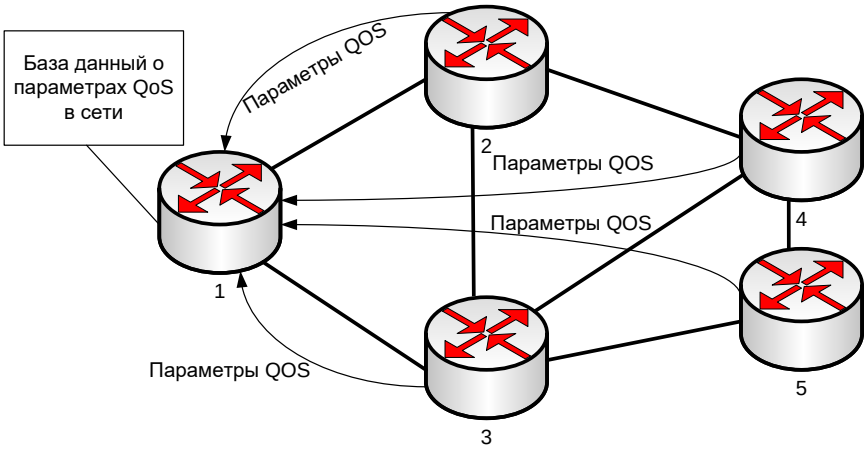


Рисунок 1.4 – Централізований збір інформації про параметри якості обслуговування

Стан і доступність окремих ресурсів визначається на підставі періодичного обміну службовою інформацією між усіма маршрутизаторами в мережі. На противагу цьому, в разі використання локальної схеми QoS маршрутизації, обмін параметрами між маршрутизаторами не проводиться, а оптимальний маршрут формується на підставі QoS статистики, зібраної локальним вузлом. В цьому випадку, оптимальність маршруту буде визначатися адекватністю інформації, отриманої від сусідів і доступності локальних ресурсів.

Основними цілями QoS маршрутизації є:

1. Динамічне визначення шляхів на підставі інформації про доступність ресурсів в мережі і QoS вимог потоків. При виборі шляху можуть враховуватися обмеження системної політики, такі як вартість, використання або виключення з маршруту певних вузлів і т.д.

2. Оптимізація використання ресурсів - QoS маршрутизація повинна ефективно використовувати мережеві ресурси, збільшуючи загальну пропускну здатність. Така схема маршрутизації може бути основою для ефективного мережевого інжинірингу.

3. Компенсація деградації обслуговування трафіку - QoS маршрутизація може компенсувати короткочасну брак ресурсів, дозволяючи отримати більше ресурсів у порівнянні зі схемами маршрутизації, заснованими на виборі найкоротшого шляху.

Запропоновано алгоритми для реалізації алгоритмів QoS маршрутизації IP мережах. Для опису характеристик шляхів вводиться поняття «прийнятного»

шляху (feasible path) [11]. Шлях вважається «прийнятним», якщо вільна пропускна здатність на всіх ділянках шляху більше, ніж запитувана. Задача QoS маршрутизації в цьому сенсі є вибір «прийнятного» шляху, якщо такий існує. Для цього шляху p = (i1, i2, ..., ik) максимально можливе значення резервованій пропускної здатності (що позначається mrb) визначається як

$$mrbp = \min\{R_{ij}, ij \notin p\} \tag{1.2}$$

Отже, шлях *p* може бути прийнятним, якщо *mrbp* не менш, ніж необхідне значення пропускної здатності *b*:

$$mrbp \geq b \tag{1.3}$$

Для пошуку найкоротших шляхів може застосовуватися один з відомих алгоритмів, наприклад, алгоритм Беллмана-Форда або Дейкстри. Ми можемо визначити в якості вартості переходу по ділянці *ij*, як R_{ij} - залишкову пропускну здатність каналу і вартість шляху *p* рівну *mrbp*. Якщо значення *mrb* не менш, ніж запитувана пропускна здатність *b*, прийнятний шлях знайдений.

Для вибору прийнятних шляхів запропоновано чотири алгоритму:

• Найкоротший шлях з максимальною кількістю доступних ресурсів (widest-shortest path) - шлях з мінімальною кількістю переходів серед всіх «прийнятних» шляхів. Якщо існує кілька «прийнятних» шляхів з однаковою пропускною спроможністю, випадковим чином вибирається один.

• Шлях з максимальною кількістю доступних ресурсів (shortest-widest path) - шлях з максимальною кількістю доступних ресурсів вибирається серед всіх «прийнятних» шляхів. Якщо існує декілька таких шляхів, випадковим чином вибирається один.

• Шлях з найкоротшим відстанню (shortest distance path) - «прийнятний» шлях визначається за мінімальним відстані. Відстань є функцією доступної пропускної здатності і визначається як:

$$dist(p) = \sum_{j=1}^{k} \frac{1}{R_{ij}}, \tag{1.4}$$

Де R_{ij} – пропускна здатність, доступна на ділянці шляху *ij*.

• Динамічний альтернативний шлях (dynamic alternative path) - нехай *n* - шлях з мінімальною кількістю переходів, коли мережа простоює, динамічний альтернативний шлях - найкоротший маршрут з максимальною кількістю доступних ресурсів, довжиною не більше ніж *n+1*.

В більшості подібних алгоритмів спочатку передбачається, що можливо знайти, як мінімум, один шлях, що задовольняє вимогам трафіку. Така ситуація властива для мереж, які обслуговують невелику навантаження. У той же час при збільшенні навантаження, можлива ситуація, коли не вдасться знайти єдиний шлях для обслуговування трафіку. У такій ситуації доречним є перехід до багатоколійні схемами маршрутизації і використанні незадіяних шляхів з великим значенням метрики. Тому використання даних алгоритмів в наведеному вигляді є недоцільним. Однак в поєднанні з технікою багатоколійні маршрутизації подібні рішення можуть використовуватися на практиці.

1.4 Багатошляхова маршрутизація по шляхах з однаковою і різною вартістю

Як було показано, маршрутизація по найкоротшому шляху може привести до незбалансованого розподілу трафіку - канали, через які проходить найкоротший шлях, стають перевантаженими, у той час як інші ділянки мережі простоюють. Багатоколійні маршрутизація (рис. 1.5) була запропонована як альтернатива маршрутизації по єдиному найкоротшому шляху для розподілу навантаження і зменшення ймовірності виникнення перевантаження в мережі.

У загальному випадку для реалізації багатоколійні схеми маршрутизації з підтримкою QoS необхідно вирішити три задачі:

1. Отримати інформацію про характеристики трафіку для визначення вимог до обслуговування;

2. Відібрати один або кілька шляхів, за якими буде передаватися даний трафік;

3. Підтримувати інформацію про використовувані ресурси на даному шляху.

Вирішенню першої задачі присвячена така область технічних наук, як теорія телетрафіка. Обгрунтування вибору характеристик трафіку в роботі робиться на підставі результатів, отриманих в рамках цієї теорії. Для вирішення задач в роботі приймається те, що характеристики трафіку, що надходить на обслуговування, можуть бути описані відомим законом розподілу. Наприклад, агрегований мультимедійний трафік з деякою точністю може апроксимувати рівномірним розподілом, з огляду на той факт, що інтервали часу між надходженнями заявок

однакові. Для апроксимації трафіку даних може використовуватися експоненціальне розподіл.

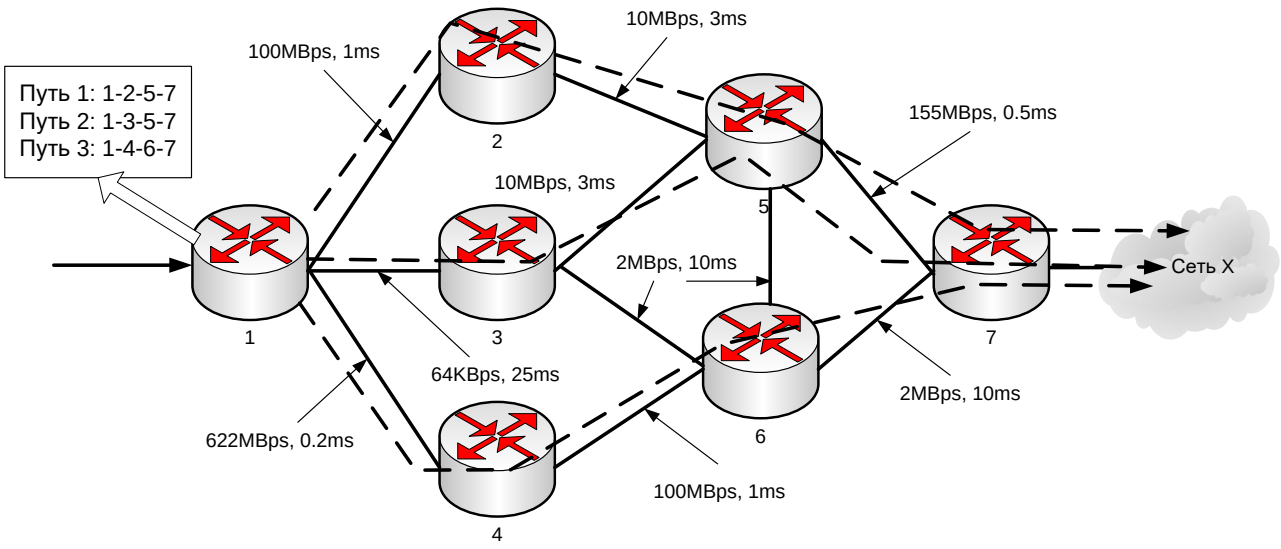


Рисунок 1.5 – Реалізація багатошляхової маршрутизації

Очевидно, що «якість» обраних шляхів визначає корисну продуктивність багатошляхової схеми маршрутизації. Існує кілька причин, за якими бажано зменшити кількість шляхів, використовуваних для маршрутизації. Перш за все, це пов'язано з великою надмірністю встановлення, підтримки і видалення шляху. По-друге, складність схеми розподілу трафіку по множинним шляхах зростає пропорційно збільшенню числа для розподілу трафіку каналів. По-третє, може існувати явне обмеження на кількість шляхів між двома вузлами як, наприклад, в технології MPLS. Тому необхідно використовувати певні процедури, що гарантують знаходження оптимального числа шляхів.

Для адекватного вибору шляхів необхідні відомості про стан мережі. Це відомості про доступність ресурсів, звані QoS-станом, в вузлах мережі, які можуть бути отримані, наприклад, шляхом періодичного обміну інформацією між маршрутизаторами в мережі. Оскільки доступність мережевих ресурсів змінюється в міру надходження і обслуговування потоків, для підтримки точних відомостей про доступність мережевих ресурсів потрібно інтенсивний обмін інформацією між вузлами і високі процесорні витрати на обробку службових даних. Тому важливо передбачити схему маршрутизації, яка б стабільно працювала, навіть якщо оновлення не періодичні або в разі їх втрат.

Було запропоновано кілька багатошляхових схем маршрутизації для балансування навантаження в мережі. ECMP (Equal Cost Multipath) і OMP (Optimized Multipath) приймають рішення про пересилання пакетів на мережевому рівні. Перший підхід реалізований в протоколі OSPF. ECMP розділяє трафік еквівалентно по безлічі шляхів з рівною вартістю. За визначенням, вартість шляху в протоколі OSPF є функцією пропускної здатності:

$$\cos t = \frac{10^8}{Bw}, \tag{1.5}$$

де Bw - пропускна здатність каналу. Іншими словами в даній реалізації розподіл трафіку відбувається по шляхам з однаковою пропускною спроможністю. Однак ці шляхи визначені статично і не відображають поточний стан мережі. Більш того, бажано розділяти трафік відповідно до поточного завантаження кожного каналу. Крім цього, «по-пакетний" підхід (рис. 1.6а) розподілу ресурсів, вимагає значних процесорних витрат. У разі високошвидкісних магістральних мереж більш привабливим є потоковий (flow-based) підхід (рис. 1.6б).

Процедури, реалізовані в алгоритмі ECMP, мають істотним обмеженням - навантаження розподіляється тільки по шляхах з однаковою вартістю без урахування динаміки зміни навантаження, хоча на практиці зміст двох каналів з однаково пропускною спроможністю вимагає високих витрат. Зазвичай організації підключають основний високошвидкісний канал і один або кілька резервних низькошвидкісних каналів. В цьому випадку резервний канал буде простоювати до тих пір, поки не відмовить основний, що економічно недоцільно.

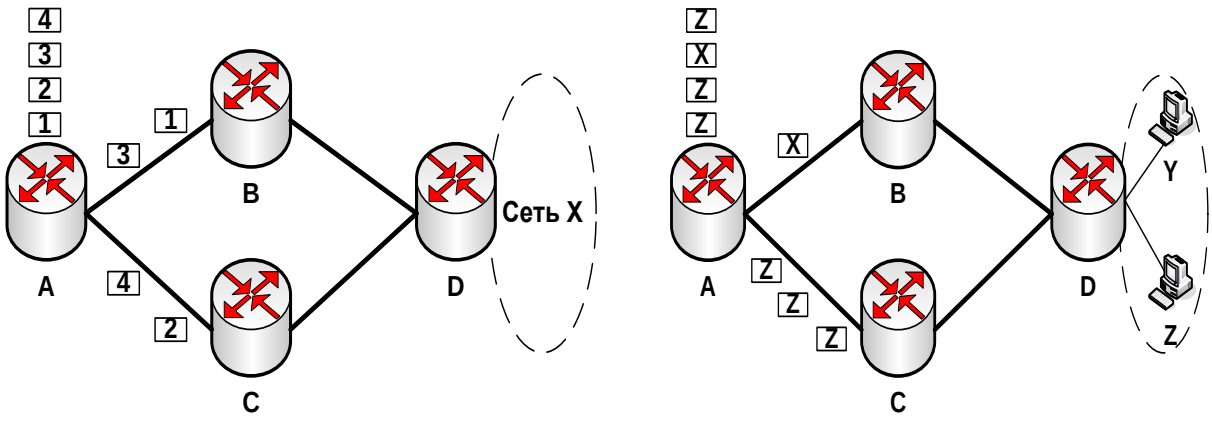


Рисунок 1.6 – Розподіл навантаження а) по пакетам б) по потоку

Схеми багатошляхової маршрутизації з розподілом ресурсів по шляхах з неоднаковою вартістю дозволяють вирішити цю проблему. Найпростіший і очевидний спосіб - пропорційний розподіл ресурсів відповідно до метрикою. Найбільш відомі протоколи, які реалізують таку схему - IGRP (Interior Gateway Routing Protocol) і EIGRP (Enhanced Interior Gateway Routing Protocol). Обидва протоколу є закритими фірмовими алгоритмами компанії Cisco. Для визначення якості шляху використовується композитна метрика на підставі п'яти складових: пропускна здатність (*Bw*), затримка *dl*, надійність *R*, завантаження *L* і максимальний розмір даних, який можна переслати по даному шляху (*MTU*):

$$metric = [k1 \cdot Bw + \frac{k2 \cdot Bw}{256 - L} + k3 \cdot dl] \cdot [\frac{k5}{R + k4}] \qquad (1.6)$$

Використання композитної метрики дозволяє врахувати особливості шляхів, викликані використовуваної транспортної технологією. Розподіл навантаження проводиться обернено пропорційно значенням метрики, тобто по шляху з меншим значенням метрики передається більший обсяг трафіку. У цих протоколах використовується попакетно підхід, що вимагає значних обчислювальних ресурсів. Крім того, фірмовий статус протоколів IGRP / EIGRP не дозволяє використовувати їх в обладнанні сторонніх виробників. При цьому, механізми розподілу навантаження по шляхах з різною вартістю не визначені у відкритих протоколах, таких як OSPF, RIP, IS-IS. Тому актуальною є розробка методики багатошляхової маршрутизації для розподілу навантаження по шляхах з неоднаковою вартістю, яку можна реалізувати як в рамках існуючих промислових протоколів маршрутизації, так і у вигляді нового незалежного протоколу маршрутизації.

2 ОСОБЛИВОСТІ МАРШРУТИЗАЦІЇ У БЕЗПРОВОДОВИХ МЕРЕЖАХ

2.1 Особливості реалізації маршрутизації у безпроводових мережах

Безпроводови широкосмугові мережі різко розширили область свого застосування на рубежі тисячоліть завдяки актуальності двох задач, відомих як задача останньої милі і задача побудови децентралізованих мереж.

Задача останньої милі полягає в організації доступу до сервісів традиційної провідної інфраструктурної мережі для кінцевих користувачів. Для її вирішення в проводову мережу включається спеціальний пристрій - точка доступу, або базова станція, до якої по безпроводовому каналу підключаються клієнтські станції кінцевих користувачів. В рамках такої архітектури "клієнт-сервер" доступ до середовища може здійснюватися централізованим або розподіленим методами. У першому випадку точка доступу монопольно керує доступом до середовища, запобігаючи колізії (одночасну передачу пакетів різними станціями), причому, так як у відсутності точки доступу клієнтські станції все одно не можуть підключитися до проводової мережі, наділення її монопольними правами не знижує надійності мережі в цілому . У другому випадку доступ до середовища здійснюється на конкурентних засадах, і всі клієнтські станції, а також сама точка доступу змагаються за право передати свої пакети.

Децентралізовані мережі, або мережі класу ad hoc, - це самоорганізуються мережі, створювані з рівнозначних станцій тоді, коли це необхідно, без провідної інфраструктури. Задача побудови таких мереж також може бути вирішена за допомогою виділення в мережі деякого пристрою-координатора і наділення його повноваженнями "сервера" по відношенню до решти пристроїв, що грає роль "клієнтських" станцій, але це недоцільно. На відміну від задача останньої милі, при вирішенні якої архітектура "клієнт-сервер" є природною, штучне призначення станціям ролей "клієнтів" і "сервера" при вирішенні задач побудови децентралізованих мереж знижує надійність мережі. Дійсно, вихід з ладу пристрою-координатора перериває роботу мережі, незважаючи на те, що цей пристрій не виконує ніяких функцій, які не могли б виконувати інші станції. Ось чому при вирішенні задачі побудови децентралізованих мереж переважно використання виключно розподіленого управління доступом до каналу.

Відмова від архітектури "клієнт-сервер" при побудові мереж класу ad hoc робить рішення задачі останньої милі і рішення задачі побудови децентралізованих мереж істотно різними, що найбільш яскраво відображено в розробленому міжнародним комітетом IEEE 8021 стандарті IEEE 802.11 безпроводових локальних мереж, відомих під торговою маркою Wi-Fi , - в стандарті описані два типи мереж: інфраструктурні мережі і мережі ad hoc.

Технологія інфраструктурних мереж (Wi-Fi Hotspot) широко відома за мільйонами точок безпроводовому доступу, розгорнутих у всьому світі. Спираючись на проводову інфраструктурну мережу, точки доступу надають клієнтським станціям, як правило, вихід в Інтернет. Завдяки своєму широкому поширенню і простоті технологія Wi-Fi Hot Spot добре вивчена.

Мережі ad hoc, які не потребують інфраструктури, в рамках базового стандарту IEEE 802.11 є однорангових мережами, в яких кожна станція знаходиться в зоні безпосереднього радиоприема всіх інших станцій [12-14].

Як відомо, вузли базового набору 802.11 або мережі Bluetooth з'єднані безпосередньо один з одним (рис.2.1) у маршрутизації немає необхідності, і IP (рівень 3) практично не працює. Джерело визначає, що приймач знаходиться в тій самій підмережі IP. При цьому обов'язкова наявність прямого зв'язку між джерелом і приймачем на 2 мережевому рівні Address Resolution Protocol (ARP) дозволяє джерелу визначити адресу (MAC) 2 рівня приймача. Джерело капсулирует датаграмму IP у фреймі 2 рівня, відповідним чином адресує кадр і передає його «Межсетевое пристрій рівня 2 (наприклад, бридж Ethernet, 802.11 AP) може виконувати деякі функції перенаправлення і маршрутизації. Звичайно вузли можуть не мати з'єднання на рівні 2. Вузли, які знаходяться в різних підмережах IP, тобто, IP мережі приймача відрізняється від IP локальної мережі. Виникає необхідність маршрутизації на рівні 3. Вузли, які знаходяться за межами радіодіапазону безпроводової мережі. В даному випадку необхідна маршрутизація на рівні 3 [14].

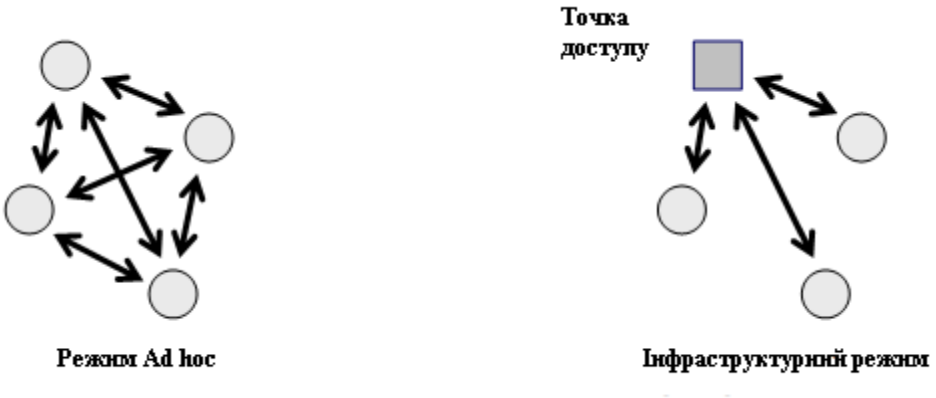


Рисунок 2.1 – Режим Ad Hoc та Інфраструктурний режим

Відправник визначає маршрут і вказує його у заголовку пакета (підтримується в IP), хоча не є типовою схемою маршрутизація від променя до променю (в датаграмме) Рішення про подальше маршруті приймається в кожній точці проходження Стандартна схема маршрутизації IP створення віртуального маршруту, визначення та конфігурування шляху до посилки першого пакету.

Таблиця маршрутизації містить інформацію, що дозволяє визначити, як направляти пакети. У маршрутизації джерела таблиця маршрутизації використовується для вказівки місця призначення в пакеті маршрутизація від променя до променя. Таблиця маршрутизації використовується для пошуку наступного променя в потрібному напрямку. При створенні віртуального маршруту таблиця маршрутизації використовується для пошуку шляху через мережу. Розподілений алгоритм вимагає побудови таблиці маршрутизації. Алгоритми формування вектора відстані (рис.2.2) обчислюють "відстань" для кожного з'єднання в мережі, що є мінімізованою величиною. Кожне з'єднання може мати "відстань" 1 для мінімізації кількості променів. Алгоритм намагається мінімізувати відстань. Таблиця маршрутизації в кожному вузлі вказує наступний промінь для кожного приймача, вказує відстань до приймача, сусіди можуть обмінюватися інформацією зі своїх таблиць для пошуку маршруту (або найкращого маршруту) до приймача.

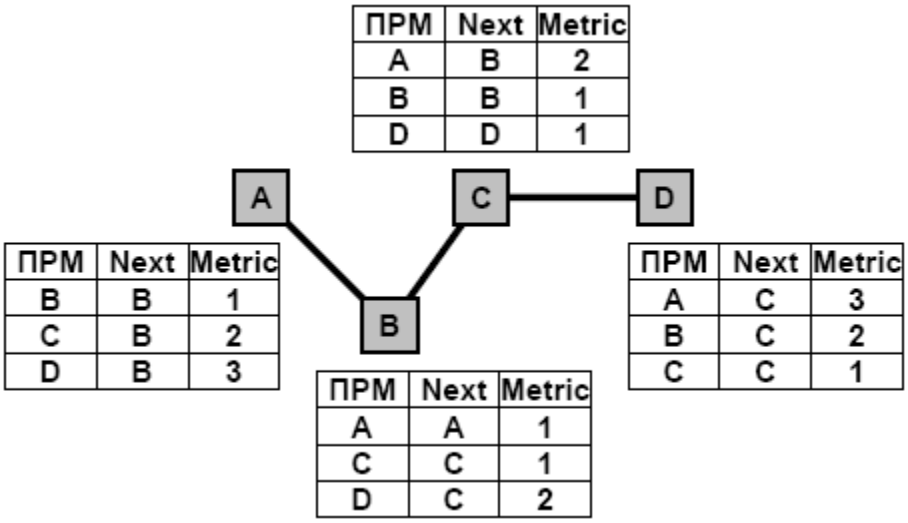


Рисунок 2.2 – Алгоритм формування вектора відстані

На рис.2.3 наведено процес, в якому вузол A дізнається від вузла з про найкоротший шлях до вузла D і оновить свою таблицю маршрутизації.

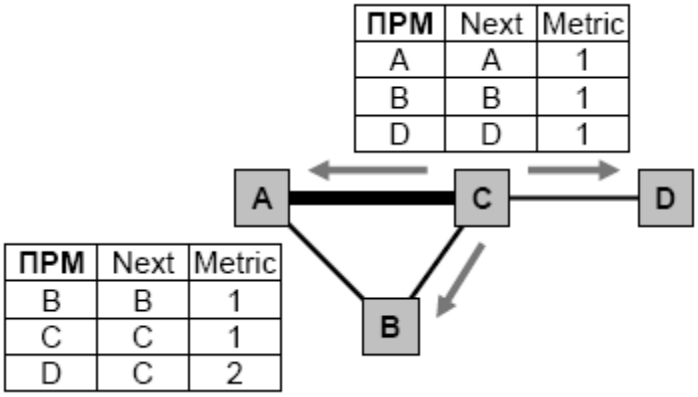


Рисунок 2.3 – Алгоритм формування вектора відстані

Припустимо, що топологія залишається стабільною досить довго, всі вузли матимуть однакову інформацію про топологію (рис.2.4).

При виконанні алгоритму стану зв'язку кожен вузол ділиться інформацією про свої з'єднання, так що всі вузли можуть побудувати карту повної мережевої топології. Інформація про з'єднанні оновлюється тоді, коли воно змінює свій стан, стан з'єднання перевіряється посилкою коротких пакетів "hello" сусідам. Маючи повну інформацію про топологію, вузол може визначити найкращий маршрут від джерела. На рис.2.5 показано як вузли A і C повідомляють про існування з'єднання AC своїм сусідам, і, в кінцевому підсумку, всієї мережі.

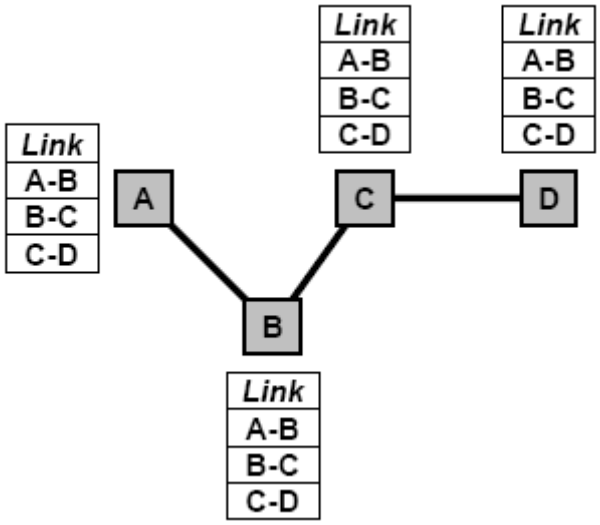


Рисунок 2.4 – Формування вектора топології мережі

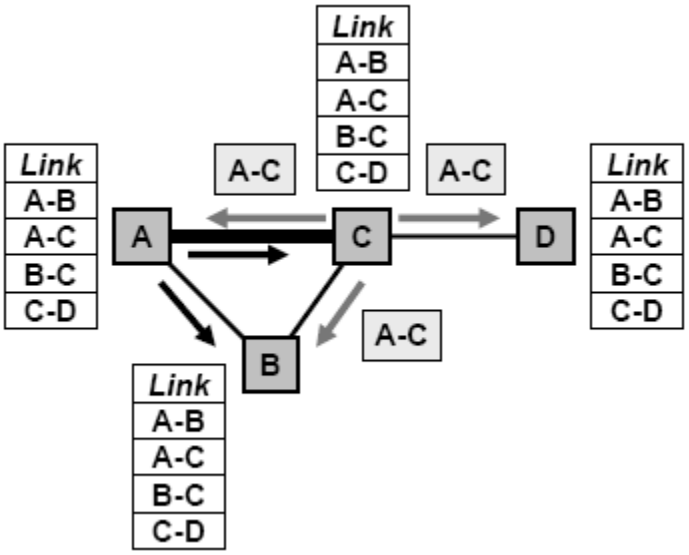


Рисунок 2.5 – Формування вектора топології мережі

У цьому контексті маршрутизація даних це велика дослідницька задача, так як дуже багато питань повинні бути охоплені: масштабованість, безпека, час життя мережі, безпроводова передача, постійно зростаючі потреби додатків. Впровадження багатошляхового алгоритму Дейкстри в протокол маршрутизації частково вирішує цю задачу для децентралізованих безпроводових мереж, таких як MANET (Mobile Ad hoc NETwork) [2, 5].

2.2 Особливості маршрутизації в MANET

Залишатися підключеним до мережі завжди це дійсно головна задача мобільних технологій. Мобільні Ad hoc мережі можуть надати рішення. З MANET всі вузли і маршрути передаються в пакетах без будь-якої інфраструктури (тобто немає шлюзів, які цим займаються). Це тип мережі спонтанний, самоорганізований і самопідтримуваний. Це однорангові безпроводові мережі передачі даних зі змінною топологією і відсутністю чіткої інфраструктури, де кожен вузол може виконувати функції маршрутизатора і брати участь в ретрансляції пакетів даних. Подібні мережі можуть застосовуватися у:

1. домашніх, офісних і заводських мережах;
2. мережах університетських містечок;
3. муніципальних і комерційно публічних мережах;
4. мережах транспортних вузлів (автомобілів, а в останні кілька років і літаків);
5. мережах, що розгортаються в зонах надзвичайних ситуацій;
6. мережах військового призначення.

Ці задачі вимагали розширення зони покриття мережі і забезпечення безперебійної роботи рухомих станцій [13].

Розширення зони покриття мережі означає, що, хоча мережу в цілому залишається зв'язковою, деякі станції знаходяться поза зоною радиоприема один одного, тому для доставки пакетів між ними потрібно ретрансляція пакетів через проміжні станції. Таким чином, розширення зони покриття мережі призводить до переходу від однокрокової мережі до многошаговой.

Рух же станцій означає, що топологія мережі змінюється з часом і станції можуть протягом своєї роботи знаходитися то в зоні безпосереднього радиоприема один одного, то за межами цієї зони.Технологіямі , покликаними розширити зону покриття мережі і забезпечити безперебійну роботу рухомих станцій, стали технологія самоорганізованих мобільних ad hoc мереж MANET.

Маршрутизація даних це велика дослідницька задача, так як дуже багато питань повинні бути охоплені: масштабованість, безпека, час життя мережі, безпроводова передача, постійно зростаючі потреби програм [5].

На рис.2.6 показаний принцип реалізації MANET.

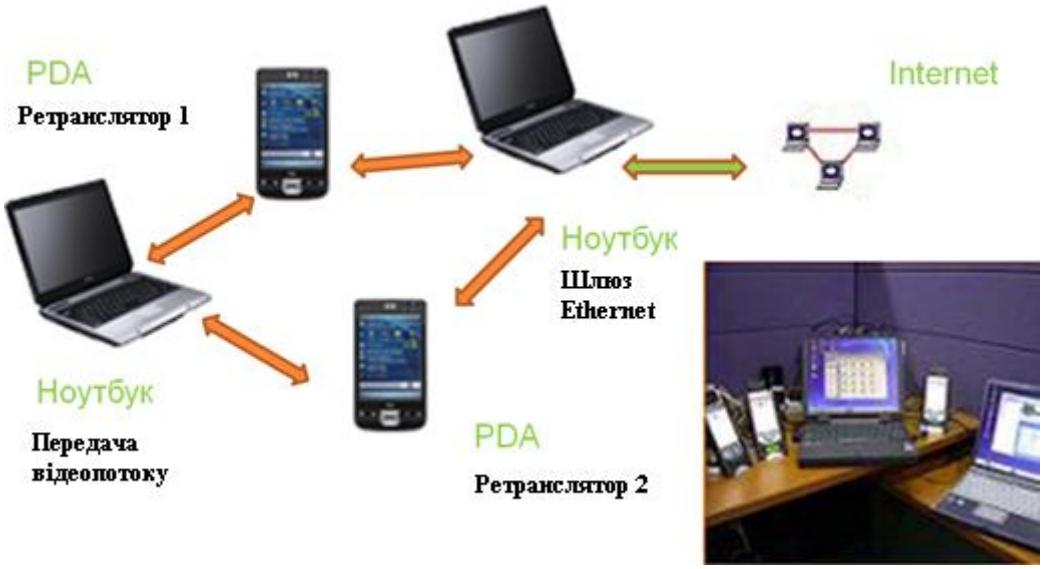


Рисунок 2.6 – Принцип реалізація MANET

Деякі протоколи багатошляхової маршрутизації були запропоновані для ad hoc мереж [7]. Основна задача протоколів багатошляхової маршрутизації це надання надійного зв'язку і гарантованість розподілу навантаження, а також поліпшити якість обслуговування ad hoc і мобільних мереж. Інші задачі протоколів багатошляхової маршрутизації це зменшення затримки, зменшення втрат і збільшення часу життя мережі. Специфіка мереж Ad hoc полягає в тому, що їх топологія постійно змінюється через переміщення вузлів мережі в просторі або зміни умов поширення радіосигналу. Крім цього, Ad hoc мереж, як і для будь-яких безпроводових систем, характерні обмежені смуга пропускання і зона радіовидимості (рис.2.7). В результаті протоколи і технічні рішення, використовувані в класичних проводових мережах передачі даних, наприклад, централізована маршрутизація з ієрархією заздалегідь призначених маршрутизаторів, в мережах Ad hoc виявляються неефективними і не забезпечують потрібну продуктивність [15,16].

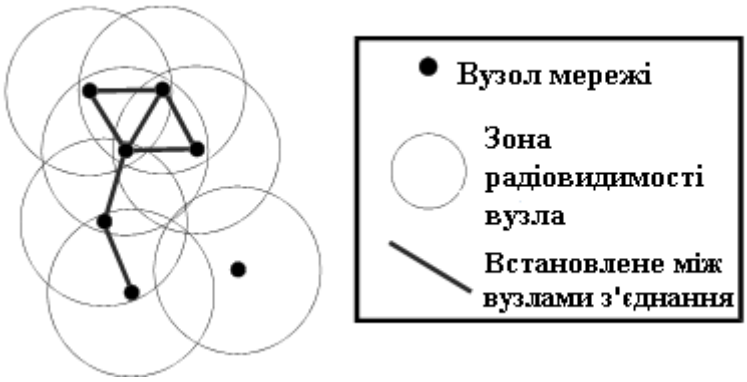


Рисунок 2.7 – Приклад структури мережі Ad Hoc

Множинні шляхи можуть бути використані як резервний шлях або можуть бути задіяні одночасно для паралельної передачі даних (так званий алгоритм round robin циклічного розподілу даних). Отримані множини шляхів може бути згруповано за трьома категоріями:

1. Роз'єднані (непересічні): ця група може бути класифікована як роз'єднана по вузлах і роз'єднана по з'єднаннях. У множин шляхів роз'єднаних по вузлам не існує загальних вузлів (задіяних більше одного разу) у зв'язку джерело – одержувач. Шляхи, роз'єднані по зв'язках можуть містити повторювані вузли, але зв'язки між вузлами повинні бути різними.
2. Переплетені: переплетені множинні шляхи можуть використовувати один або більше зв'язків маршруту (тобто безліч маршрутів може мати однакові зв'язки).
3. Змішані (гібридні): це різні комбінації раніше розглянутих типів.

З усіх типів, роз'єднаний по вузлах є самим роз'єднаним, так як всі вузли і зв'язки з множини маршрутів не повторюються, тобто певний ресурс мережі виділено для певного маршруту. Проте, чисто роз'єднаний тип це не завжди оптимальне рішення, особливо для нещільних мереж і багатокритеріального обчислення. Багатошляховий алгоритм Дейкстри є більш гнучким при збереженні всіх рішень в алгоритмі найкоротших шляхів, тобто здатний виконати всі поставлені задачі.

MP-OLSR пропонується для використання в мережах Ad Hoc [8]. По-перше, основна модифікація алгоритму Дейкстри дозволяє визначати множину шляхів, як для нещільних так і для ущільнених топологій. Дві функції ваг використовується для створення роз'єднаних (непересічних) по вузлах і роз'єднаних по зв'язках

шляхів. По-друге, проактивний характер протоколу OLSR змінюється для обчислення за запитом.

MP-OLSR є протоколом, залежним від джерела (з маршрутизацією від джерела). По-третє, підтримка частої зміни топології, додаткові функції, такі як відновлення маршруту і пошук петель (циклів). Задача цих функцій описані в рамках параметрів якості обслуговування і порівнюються з протоколом OLSR.

2.3 Одношляхова та багатошляхова маршрутизація в MANET

Для будь-якої мережі маршрутизація важлива, оскільки маршрутизація вибирає найбільш підходящий шлях у мережі для зв'язку між джерелами та вузлами призначення. Мережа має головну проблему вибрати відповідний протокол маршрутизації для мережі. Алгоритми маршрутизації бувають двох типів: одношляховий та багатошляховий [22], [23]. Протоколи одношляхової маршрутизації не працюють у кількох середовищах. Навпаки, багатошляхова маршрутизація працює ефективніше в декількох середовищах. У механізмі маршрутизації з одним шляхом встановлено єдиний маршрут між джерелами до пункту призначення, тоді як у техніці багатошляхової маршрутизації встановлено кілька маршрутів серед подібного джерела до пункту призначення. Він має багато переваг перед одношляхової маршрутизації. Це забезпечує краще існування мережі, ефективність живлення та нижчу наскрізну затримку.

Як показано на рис.2.8. прогнозується, що таксономія протоколів маршрутизації багатошляхових механізмів маршрутизації поділяється на MANET за категоріями відповідно до їх поведінки. Це a) усвідомлена затримка (b) надійна (c) низкі накладні витрати (d) енергоефективна (e) гібридна.

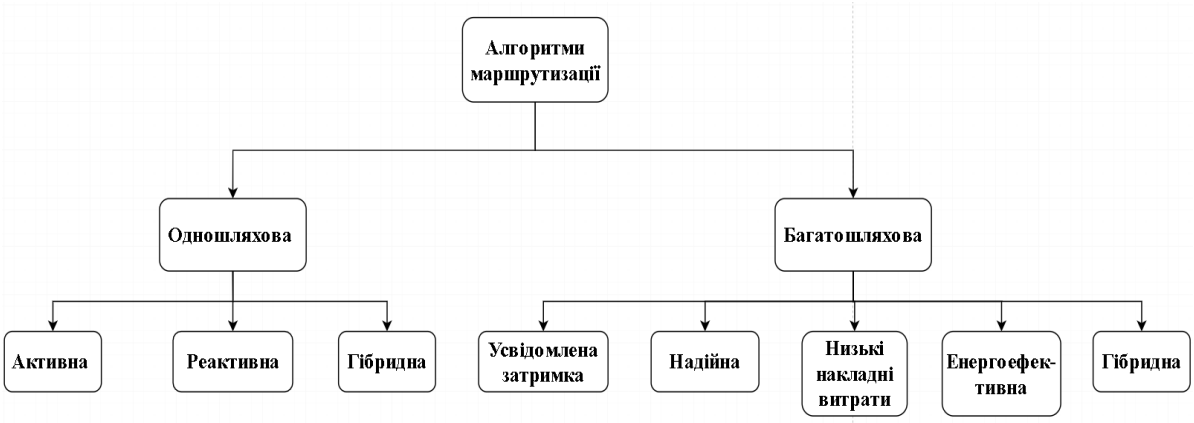


Рисунок 2.8 – Таксономія протоколів маршрутизації

Таксономія одношляхової маршрутизації буває типу, реактивна, активна та гібридна. Поряд з цим існують енергозберігаючі та розроблені безпечні механізми маршрутизації. Вихідний вузол у проактивній стратегії зберігає всю можливу інформацію про маршрути. Кожен вузол складається з таблиці маршрутизації для збереження інформації про маршрут, яка буде часто оновлюватися. Ця оновлена інформація про маршрут передається кожному вузлу в мережі. Перевага цього полягає в тому, що траєкторії швидко вивчаються і створюється сеанс. Недоліком цього механізму є споживання високої пропускної здатності та погіршення продуктивності мережі в умовах порушених маршрутів та змін топології.

Для подолання обмежень для MANET була запропонована стратегія реактивної маршрутизації.

Вихідний вузол у реактивному механізмі ініціює процес виявлення маршруту лише тоді, коли джерело хоче зв’язатися з місцем призначення. Як тільки маршрут виявляється серед джерела до пункту призначення, цей маршрут зберігається в процесі збереження маршруту. У порівнянні з активними показниками реактивного механізму набагато краще.

Проблема цього - висока затримка в процесі виявлення маршруту та погіршення продуктивності для великих мереж. Прикладами є AODV, DSR. Цей механізм визначає найкоротший шлях між джерелами до пункту призначення. Дослідження дають докази використання найкоротшого шляху, можливо, не є підходящим вибором для MANET. Щоб подолати обмеження найкоротшого єдиного шляху, дослідники рекомендували багатошляхову маршрутизацію. Поєднуючи особливості реактивного та проактивного

гібридного типу, розробляється механізм маршрутизації. Краса цієї стратегії полягає в тому, що в міру зміни топології мережі вона може змінюватися. Слабкою стороною цієї техніки є висока складність. Різні протоколи гібридної маршрутизації, наприклад, ZRP.

Процес відновлення маршруту запускається в багатошляховому реактивному механізмі маршрутизації швидко і динамічно, якщо маршрут є помилковим у мережі. Ця функція приваблює багатьох дослідників, щоб винайти алгоритми багатошляхової маршрутизації для мережі. Встановлено більше одного шляху від джерела до вузла призначення. Серед цих кількох маршрутів принаймні один шлях є основним, а решта або декілька альтернативних шляхів доступні між джерелами до пункту призначення. Вихідний вузол у цій техніці має можливість виявити безліч маршрутів між джерелами до пункту призначення в одному процесі виявлення маршруту.

Поведінка, що усвідомлює затримку, обирає кілька шляхів для поліпшення загальної продуктивності мережі затримки. Надійна методологія продовжує надійну передачу даних від джерела до місця призначення. Методологія мінімальних накладних витрат визначає кілька шляхів, використовуючи найменші накладні витрати на контрольні повідомлення. Енергоефективна методологія вибирає шлях енергетичного ефекту для покращення жвавості мережі. Для визначення енергоефективного шляху між джерелом до вузла призначення використовуються різні методи. Гібридна стратегія включає найкращі особливості пошуку найкоротшого шляху та багатошляхового алгоритму.

Кожен алгоритм багатошляхової маршрутизації має надзвичайні переваги та обмеження. Існує кілька загальних розбіжностей, таких як: створення кількох шляхів, вибір цих шляхів, поширення навантаження між цими траєкторіями. Протоколи маршрутизації перероблені для висвітлення розбіжностей, заявлених раніше. Визначення відповідного алгоритму або набору алгоритмів, які забезпечують цілі потреби ефективного алгоритму маршрутизації. На даний час кількість протоколів маршрутизації рекомендована в MANET з іншою метою та для конкретних різних потреб. Протоколи маршрутизації віддають перевагу одному шляху і пересилають цілі пакети по цьому шляху. Однак протоколи одношляхової маршрутизації не працюють у багатьох середовищах. Маршрутизація з одним шляхом може

збільшити наскрізну затримку, забирає більше часу на виявлення шляху у разі зміни топології. Багатошляхова маршрутизація витрачає менше часу на виявлення декількох шляхів та вибирає кілька маршрутів з одного джерела до пункту призначення. Існує так багато переваг багатошляхової маршрутизації в порівнянні з одношляхової, показаним у табл. 2.1 [4-8]. Це дає кращий термін служби, енергоефективність та нижчу кінцеву затримку. У них також є деякі проблеми з точки зору упорядкування пакетів даних, обслуговування шляхів, вибору декількох шляхів тощо.

Таблиця 2.1 – Порівняння одношляхової та багатошляхової маршрутизації

Параметр	Одношляхова	Багатошляхова
Кількість шляхів	Один	Кілька
Відправка даних	За єдиним шляхом	Одиночний, а також кілька шляхів
Затримка	Висока	Знижена затримка в порівнянні з одиночним шляхом
Час відновлення маршруту	Потребується більше часу, а ніж багатошляховій	Потребується меньше часу, а ніж одношляховій
Пропускна спроможність	Недостатня пропускна здатність	Висока
Пропускна здатність	Низька	Висока
Термін служби мережі	Низька	Висока
Кінцева затримка	Висока	Низька
Простір таблиці маршрутів	Потрібно менше в порівнянні з багатошляхової	Потрібно більше в порівнянні з одношляхової
Перевантаження обчислень	Менше в порівнянні з багатошляхової	Більше в порівнянні з одношляхової

Незважаючи на те, що алгоритми багатошляхової маршрутизації покращують зниження навантаження, надійність, затримку та енергоефективність, вони також мають кілька недоліків. Переваги та недоліки наведені в табл. 2.2 [4-8].

Таблиця 2.2 – Переваги та недоліки протоколів багатошляхової маршрутизації

Переваги	Недоліки
Відмовостійкість	Довший шлях
Балансування навантаження	Спеціальне контрольне повідомлення
Агрегація смуги пропускання	Більша кількість запитів маршруту
Зменшена затримка	Неефективне виявлення маршруту

У проводовій мережі задача маршрутизації виконують виділені маршрутизатори. Тоді як безпроводова мережа не має жодного виділеного маршрутизатора, оскільки задача маршрутизації повинен виконувати звичайний вузол. Маршрутизація - одна з вимог мережі для передачі даних від одного вузла до іншого. Алгоритм маршрутизації відіграє важливу роль у MANET. У MANET всі вузли виконують роль маршрутизаторів, серверів та точок доступу. Маршрутизація - це основна операція MANET. Жоден дизайн протоколу маршрутизації, розроблений на сьогоднішній день, не є повним підтвердженням. Якщо будь-який протокол маршрутизації є надійним, тоді буде проблема з продуктивністю. У деяких протоколах маршрутизації часто використовується лише надійний і найкращий шлях, тоді вузли, що знаходяться в шляху, можуть страждати від енергоефективності. Багато протоколів маршрутизації страждають від різних атак. Безпека є головною проблемою протоколу маршрутизації. Для вирішення проблем, пов'язаних з маршрутизацією, модифікація протоколу робиться багатьма дослідниками, але вона долає існуючі проблеми, але призводить до нових проблем.

3 ПРОТОКОЛИ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ В MANET

3.1 Класифікація протоколів маршрутизації

Багато протоколів маршрутизації були розроблені для Ad hoc мережі [2].

Для успішного застосування в Ad hoc мережах протоколи маршрутизації повинні володіти наступними якостями:

1. Бути розподіленими. Всі вузли в мережі повинні бути здатні здійснювати маршрутизацію і не мати жорстко закріплених за собою функцій.
2. Забезпечувати надійну доставку пакетів в умовах постійно мінливої топології мережі, коли використання класичних механізмів гарантованої доставки, як, наприклад, на транспортному рівні в протоколі Transmission Control Protocol (TCP), утруднено.
3. Забезпечувати малий час побудови маршруту в умовах постійно змінюється топології мережі.
4. Володіти механізмами оперативного виявлення розриву маршруту і його відновлення.
5. Не допускати утворення петель в маршрутах.
6. Розсилати при функціонуванні якомога менший обсяг службової інформації.
7. Володіти високою масштабованістю, тобто забезпечувати високу продуктивність мережі при різних розмірах.
8. Підтримувати QoS.

Протоколи можуть класифікуватися за різними критеріями, найбільш важливий, з яких – за типом з'ясування маршруту, він дозволяє розділити протоколи маршрутизації на три категорії: проактивні, реактивні та комбіновані (рис.3.1). У реактивних протоколах, таких як Dynamic Source Routing (DSR [2]) і Ad hoc Ondemand Distance Vector routing (AODV [5]), запит на маршрутизацію надсилається на вимогу, тобто якщо вузол хоче з'єднатися з іншим вузлом, він генерує широкомовну розсилку із запитом шляху і чекає відповіді від точки призначення. Проте ж проактивні протоколи оновлюють свою інформацію про

маршрутизації, щоб мати постійний огляд мережевий топологи, наприклад OLSR.

Рисунок 3.1 – Протоколи маршрутизації MANET

Інший критерій для ad hoc протоколів маршрутизації класифікується за кількістю вузлів розраховуються між джерелом і отримувачем: багатошляхові та одношляхові протоколи маршрутизації. На відміну від провідних мереж ad hoc мережі більш залежать як від збою з'єднання, так і від збою вузла через те, що вузол мобільний або може розрядитися акумулятор.

В результаті маршрут, який використовується для маршрутизації може бути зіпсований з різних причин. Для підвищення опірності маршруту збоям з'єднання або вузла існує рішення-маршрутизаційне сполучення між численними роз'єднаними шляхами одночасно. Таким чином, вузол одержувача все ще буде здатний отримати повідомлення навіть у тому випадку, якщо не пошкодженим залишився тільки один шлях. Цей підхід спрямований на вирішення проблем масштабованості, мобільності, стабільності зв'язку в мережі. Багатошляховий підхід має перевагу у великих і щільних мережах.

До недоліків багатошляхової маршрутизації ставитися те, що таблиці маршрутизації займають більший обсяг, ніж при використанні одноколійної маршрутизації, а самі алгоритми стають складнішими.

3.2 Протокол AODV

AODV (Ad hoc On-Demand Distance Vector) – спеціалізований протокол вектора відстані за запитом. Вузол не виконує пошук маршруту або його підтримку до тих пір, поки йому не знадобиться маршрут до іншого вузла або поки він не запропонує свої послуги в якості проміжного вузла. Вузли, що знаходяться в стороні активного маршруту, не підтримують інформацію про маршрутизації і не беруть участь у формуванні таблиці маршрутизації. AODV використовує маршрутизацію від вузла до вузла. Маршрутизація заснована на динамічній таблиці, підтримуваної в проміжних вузлах. Протокол аналогічний DSR, але DSR використовує маршрутизацію джерела.

Для визначення місцевих з'єднань використовуються локальні повідомлення «hello». Таким чином можна зменшити час відгуку на запити маршруту і ініціювати оновлення в міру необхідності.

Маршрутами і записами в таблиці маршрутизації присвоюються послідовні номери, які використовуються для заміщення застарілої інформації. Кожен вузол підтримує два лічильника: послідовний лічильник вузла і широкомовний ID.

Запит маршруту AODV ініціюється в тому випадку, коли вузол хоче з'єднатися з іншим вузлом, але не знає маршруту. Вузол-джерело посилає широкомовний пакет із запитом маршруту (RREQ) своїм сусідам. Поля пакету наведені на рисунку 3.2.

Порядковий номер джерела в запиті маршруту показує "ступінь свіжості" зворотного маршруту до джерела. Порядковий номер приймача показує ступінь свіжості» зворотного маршруту до приймача.

Кожен вузол, який приймає Route Request (RREQ) або повертає пакет з відповіддю маршруту (RREP), або пересилає RREQ своїм сусідам.

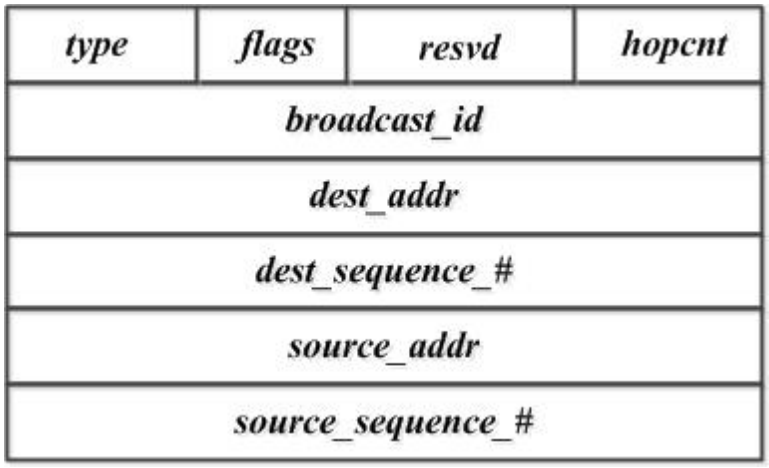


Рисунок 3.2 – Поля пакету RREQ

Поля source_addr і broadcast_id унікально ідентифікують RREQ. Broadcasr_id инкрементируется для кожного посланого пакета RREQ, так

що приймачі можуть розпізнати і видалити дублюючі пакети RREQ.

Якщо вузол не може відповісти на RREQ, то він інкрементує лічильник вузлів і зберігає інформацію, необхідну для підтримки зворотного маршруту (в протоколі передбачається наявність симетричних з'єднань). [5]

До необхідної інформації відноситься:

1. ідентифікатор сусіднього вузла, який надіслав цей пакет RREQ;
2. IP-адреса місця призначення;
3. IP адреса джерела;
4. широкомовний ID;
5. послідовний номер вузла джерела;
6. час закінчення запису для зворотного маршруту.

Якщо вузол приймає пакет RREQ і у нього є поточний маршрут до місця призначення, то він пошле односпрямований пакет з відповіддю маршруту (RREP) того сусіда, від якого він прийняв пакет RREQ. На рисунку 3.3 наведено структуру пакету RREP.

Проміжні вузли будуть ретранслювати перший RREP у напрямку до джерела, використовуючи ці записи зворотного маршруту. Інші пакети RREP відкидаються до тих пір, поки номер dest_sequence_# більше попереднього, або dest_sequence_# такий же, але hopcnt менше (тобто це найкращий шлях). Зрештою RREP досягає вузла, який може використовувати сусіда, який надіслав RREP, в якості наступного променя для пересилання інформації до місця при-

значення. Ці зворотні маршрути будуть видалятися в тих вузлах, які не бачать пакету RREP.

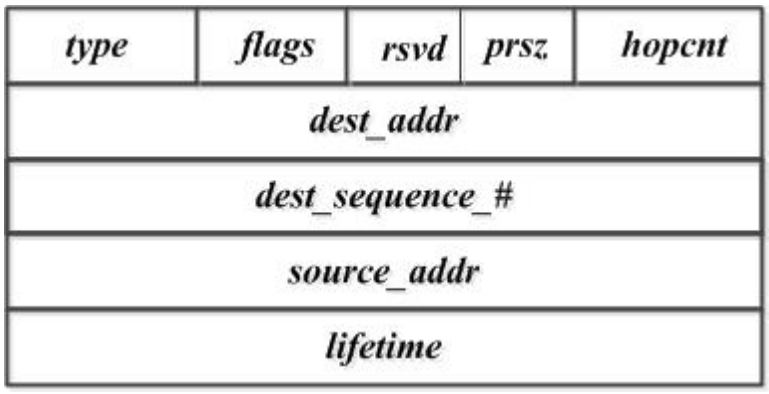


Рисунок 3.3 – Структура пакета RREP

Причиною зміни маршруту може бути втрата періодичних повідомлень «hello», аварія на зв'язному рівні, помилка передачі пакета до наступного вузла (може бути виявлена за допомогою прослуховування ретрансляції, якщо це не кінцева точка призначення). Вищестоящий (по напрямку до джерела) вузол, виявивши помилку, передає пакет помилкового маршруту (RERR) з новим порядковим номером місця призначення і кількістю променів, рівним нескінченності (недосяжний маршрут). Джерело (або інший вузол маршруту) може знову побудувати шлях, надіславши пакет RREQ.

3.3 Протокол DSR

DSR (Dynamic source routing) – реактивний протокол динамічної маршрутизації від джерела, як випливає з назви, є одним з протоколів маршрутизації на вимогу, заснований на концепції побудови шляху від джерела передачі, тобто явну маршрутизацію. Мережі на основі DSR повністю самоорганізуються і самостійно конфігуруються. У DSR не застосовується метод періодичної розсилки повідомлень як в AODV, таким чином знижується навантаження на смугу пропускання, зберігається заряд акумулятора мобільних пристроїв, а також вдається уникнути занадто частого оновлення маршрутних даних і обміну занадто великою кількістю інформації.

Згідно з протоколом DSR пошук маршруту та підтримка інформації про нього від вузла до вузла здійснюється двома головними механізмами: пошук

маршруту і підтримка маршруту. DSR постійно оновлює кеш маршрутів з метою доступності нових зручних маршрутів. «Пошук маршруту» – механізм, за допомогою якого вузол S, що збирається послати якісь пакети вузла D, отримує вихідний маршрут до нього. Пошук маршруту використовується тільки в тому випадку, якщо вузол S в перший раз намагається отримати доступ до D і не знає шляхи до нього. Пошук здійснюється відправкою broadcast-запиту RREQ. Під час пошуку шляху відбувається накопичення адрес пристроїв, що знаходяться між одержувачем і відправником. У цьому процесі беруть участь всі вузли, що обробляють broadcast-запит. Інформація про адреси вузлів, через які пройшли пакети маршрутизації, записується в заголовках пакетів.

Таким чином, вузли можуть отримувати інформацію про стан інших пристроїв та існуючих маршрутах, за умови, що через них проходять пакети. Маршрут вважається сформованим тільки в тому випадку, якщо пакет досяг адресата, тоді відправляється повідомлення-відповідь. Відповідь може бути відправлений або за відомим маршрутом, записаним в пам'яті вузла-одержувача, або по ланцюжку, записаної в заголовку прийнятого пакету-запиту. В цьому випадку накладається умова на лінії зв'язку мережі - вони повинні бути симетричні. «Підтримка маршруту» – механізм, за допомогою якого вузол S здатний виявити за допомогою існуючого маршруту до D, именилась чи топологія мережі таким чином, що даний маршрут більше не можна використовувати внаслідок втрати з'єднання на шляху. Якщо розрив з'єднання між відправником і одержувачем знайдено, вузол-відправник намагається підшукати інший шлях або застосовує механізм пошуку маршруту DSR.

У протоколі присутній засіб захисту від утворення петель. Вся інформація про пакет знаходиться в його заголовку, в тому числі і інформація по маршрутизації. Тому проміжні вузли можуть записувати цю інформацію в кеш і свої маршрутні таблиці для використання в майбутньому.

Отже, коли пристрій хоче передати якісь дані іншого пристрою, до якого немає відомого шляху, він ініціалізує пакет RREQ, який поширюється по мережі. Кожен вузол після отримання пакета RREQ пересилає його своїм сусідам, якщо не є одержувачем і час життя пакету не вийшло. У разі, якщо копія цього пакету знову прийшла в вузол, повторно пересилатися вона не буде. Перевірка на дублікати проводиться за порядковим номером, записаним в заголовку пакету. Номер Цей був присвоєний вузлом-джерелом, він запам'ятовується кожним

вузлом, через який пройшов одного разу. Таким чином, петлі в маршрутах повністю виключаються. Вузол-адресат при отриманні цього пакету RREQ відповідає на запит повідомленням RREP, направляючи зворотного маршруту, або по вже існуючому шляху, що зберігається в кеші сайту. [9]

До недоліків протоколу відноситься нездатність відновлювати розірвані з'єднання в місцевому масштабі механізмом підтримки маршруту. Застаріла інформація з Кеша маршруту може призвести до неузгодженості при реконструкції маршруту. Продуктивність протоколу зменшується зі збільшенням рухливості вузлів. При використанні методу маршрутизації від джерела спостерігаються витрати маршрутизації при збільшенні довжини шляху.

3.4 Протокол OLSR

Протокол OLSR (Optimized Link-State Routing Protocol) вирішує задача виявлення сусідніх вузлів і підтримки з'єднань з ними, поширення інформації про існуючі з'єднаннях з сусідніми вузлами по всій мережі, пошуку найкоротших маршрутів на підставі наявної на сайті маршрутної інформації і покрокової ретрансляції пакетів.

Для виявлення сусідніх вузлів і підтримки з'єднання з ними (пара вузлів є сусідами, якщо знаходиться в межах впевненого прийому один одного) всі вузли мережі періодично (з інтервалом HELLO_INTERVAL) широкомовно розсилають повідомлення HELLO, що містять адреси сусідніх вузлів та інформацію про встановлені з ними сполуках. Якщо протягом часу NEIGHB_HOLD_INTERVAL вузол не отримує жодного повідомлення HELLO від свого сусіда, то з'єднання з цим вузлом вважається розірваним.

Повідомлення HELLO не ретранслюються по всій мережі, тому з їх допомогою кожен вузол може дізнатися мережеву інформацію лише про своє двухшаговом оточенні.

Назвемо вузол n однокроковим сусідом вузла x, якщо вузол x знаходиться в області впевненого прийому вузла n. Вузол d, не є однокроковим сусідом вузла x, назвемо двухшаговым сусідом вузла x, якщо вузол d є однокроковим сусідом хоча б одного однокрокового сусіда вузла x.

Для поширення інформації про з'єднання з однокроковими сусідами по всій мережі вузли періодично (з інтервалом TC_INTERVAL) відправляють ши-

рокомовні повідомлення TOPOLOGY_CONTROL (TC). Інформація про з'єднання між парою вузлів, отримана з TC деякого вузла-джерела, оновлюється при отриманні кожного нового TC повідомлення від цього вузла, і віддаляється, якщо або вузол-джерело TC більше не розсилає інформацію про даному з'єднанні, або завершився інтервал TOP_HOLD_INTERVAL з моменту отримання останнього TC від розглянутого вузла-джерела.

Всі широкомовні повідомлення ретранслюються з використанням випадкової затримки – джиттера; за замовчуванням він вибирається рівноймовірно з інтервалу [0, HELLO_INTERVAL/4).

На підставі інформації, одержуваної з HELLO і TC, кожен вузол будує орієнтований граф, який є поданням безпроводової мережі даного вузла. До кожного вузла мережі в отриманому графі визначається найкоротший маршрут, що представляє собою ланцюжок ретрансляторів. Адреса кінцевого одержувача і першого ретранслятора утворюють запис в таблиці маршрутизації.

При необхідності доставити пакет до кінцевого одержувача вузол знаходить потрібну запис в таблиці маршрутизації і пересилає пакет вказаною в ній ретранслятора. Ретранслятор, отримавши пакет, виконує аналогічну процедуру, при цьому маршрут, використовуваний вузлом-ретранслятором, може відрізнятися від маршруту джерела, оскільки ретранслятор має власне бачення топології мережі.

Таким чином, пакет передається до тих пір, поки не досягне кінцевого одержувача або не буде відкинутий у разі зациклення маршруту.

Ключовою особливістю протоколу OLSR, що знижує завантаженість мережі при широкомовної розсилці, є використання так званих MPR-ретрансляторів (MultiPoint Relays). Кожен вузол вибирає з множини своїх однокрокових сусідів, з якими встановлено двонаправлене з'єднання, MPR-ретранслятори таким чином, щоб кожен двокроковий сусід даного сайту був однокроковим сусідом принаймні одного з його MPR-ретрансляторів.

MPR-ретранслятори відіграють важливу роль при поширенні маршрутної інформації та пересиланні широкомовних повідомлень. По-перше, кожен вузол, за замовчуванням, включає в повідомлення TC інформацію про двонаправлених з'єднаннях тільки з тими сусідами, які вибрали даний сайт в якості MPR-ретранслятора. Завдяки цьому зменшується число з'єднань, інформація про які розсилається по мережі. По-друге, вузол Y пересилає широкомовне повідомлення,

отримане від його сусіда – вузла X, тільки в тому випадку, якщо Y є MPR-ретранслятором вузла X. Таким чином знижується число пересилань при поширенні одного широкомовного повідомлення [8].

3.5 Протокол OSPF

Протокол OSPF (Open Shortest Path First) розроблявся як механізм, за допомогою якого маршрутизатори можуть обмінюватися інформацією про вміст таблиць маршрутизації у великій міжмережевий середовищі. Протокол OSPF є протоколом маршрутизації з оголошенням стану каналу зв'язку. В основі функціонування протоколу OSPF лежить алгоритм "першочергового виявлення найкоротшого шляху" (Shortest Path First, SPF), який використовується для обчислення маршрутів в таблиці маршрутизації. Використовуючи алгоритм SPF, маршрутизатор обчислює найкоротший (тобто володіє найменшою вартістю) шлях до всіх подсетям в міжмережевий середовищі. В маршрутах, розрахованих за допомогою алгоритму SPF, завжди відсутні цикли.

На відміну від протоколу RIP, протокол OSPF підтримує "карту" корпоративної мережі. Ця карта модифікується кожен раз, коли відбувається будь-яка зміна в структурі мережі. Ця карта, звана базою даних стану зв'язків (link state database), синхронізована для всіх OSPF-маршрутизатори і використовується, щоб обчислити маршрути в таблиці маршрутизації. Зміни в структурі мережі призводять до негайного поширення відомостей про цих змінах на всі маршрутизатори, які, в свою чергу, оновлюють власний екземпляр бази даних стану зв'язків. Оновлення бази даних станів зв'язків призводить до повторного перерахунку таблиці маршрутизації.

Починаючи свою роботу, кожен маршрутизатор сповіщає інші маршрутизатори про своє існування, відправляючи спеціальне повідомлення в усі доступні підмережі. Інші маршрутизатори отримують це повідомлення і оновлюють свій екземпляр бази даних про стан зв'язків. Фактично зазначена база даних і формується на підставі цих повідомлень.

Оскільки розмір бази даних станів зв'язків зростає, вимоги до обсягу пам'яті і час на обчислення маршруту збільшуються. Щоб вирішити цю проблему, OSPF розглядає міжмережеву середовище як сукупність областей (під областю в даному випадку розуміється сукупність безперервних мереж),

з'єднаних один з одним через деяку базову область (backbone area). Всі маршрутизатори, що належать до однієї області, володіють ідентичними репліками бази даних стану зв'язків.

З метою ідентифікації областей кожної з них виділяється спеціальний ідентифікатор (area ID), що представляє собою 32-розрядне число. Цей код записується так само як і IP-адреса — в десятково-точковому форматі (тобто у вигляді чотирьох однобайтових чисел, розділених крапками). Ідентифікатор області ніяк не пов'язаний з IP-адресацією. Адміністратор може присвоювати ідентифікатори областям на свій розсуд, не озираючись на використовувані в мережі IP-адреси. При цьому одна область OSPF може включати в свій склад необмежену кількість підмереж (розмір області обмежується виключно розміром бази даних стану зв'язків).

Кожен маршрутизатор зберігає базу даних станів зв'язків лише для тих областей, які приєднані до маршрутизатора безпосередньо. Маршрутизатори, що з'єднують базову область з іншими областями, називаються прикордонними маршрутизаторами областей (Area Border Router, ABR). Прикордонні маршрутизатори накопичують зміни, отримані від інших маршрутизаторів області, і передають їх разом маршрутизаторам, розташованих в інших областях.

Найбільша перевага протоколу OSPF полягає в тому, що він є високопродуктивним протоколом і призводить до незначних витрат навіть в дуже великих міжмережевих конфігураціях. В якості недоліку протоколу OSPF можна відзначити певну складність його розгортання і конфігурування.

3.6 Протокол FSR

Протокол FSR (Fisheye State Routing) – це проактивний протокол, який використовує ієрархічну структуру маршрутизації, що забезпечує скорочення розсилається по мережі службової інформації шляхом введення багаторівневих областей. Аналогічно OLSR використовує механізм збереження таблиць марш-рутизації (локальних карт найкоротших шляхів) на кожному вузлі, якими вузол час від часу обмінюється з іншими вузлами.

FSR складається з трьох задач:

Знаходження сусідів: кожен вузол кожні δ секунди надсилає повідомлення HELLO своїм сусідам, що перестрибують, з метою встановлення та підтримки взаємовідносин із сусідами.

Поширення інформації: кожен вузол розповсюджує повідомлення про стан стану посилання (LSA) кожні Δ секунди (з Δ> δ), що містять інформацію про сусідні посилання, серед усіх інших вузлів мережі.

Обчислення маршруту: на основі інформації, що міститься в повідомленнях LSA, вузол може реконструювати всю топологію мережі та використовувати алгоритм Джикста для обчислення маршрутів до будь-якого вузла в мережі.

Особливістю FSR є те, що повідомлення LSA генеруються кожні Δ секунди, використовуючи послідовність різних значень часу до життя. Візьмемо як приклад послідовності 1, 3, 8, 64, сусіди з 1 стрибком отримують LSA кожні Δs, тому вони мають найбільш оновлену інформацію. Сусіди з 2 стрибками отримують LSA з TTL 3, 8, 24. Вузли на відстані від 4 до 8 стрибків отримують лише LSA з TTL 8 і 64. Всі інші отримують лише LSA з TTL 64. Як наслідок, кожен вузол має поступово менш оновлену інформацію про топологію мережі із збільшенням відстані.

Протокол використовує той факт, що коли пакет рухається від джерела до пункту призначення, вузли, що зустрічаються на найкоротшому шляху, мають дедалі точнішу інформацію про топологічне положення пункту призначення (оскільки їх відстань до пункту призначення зменшується), тому втрата Точність обчислення найкоротшого шляху від вузла-джерела компенсується вздовж шляху до пункту призначення.

Таким чином, FSR зменшує загальну кількість інформації, що поширюється в мережі, оскільки LSA не надсилаються з фіксованим максимальним TTL.

Однією з типових проблем з протоколами стану зв'язку є те, що при розриві вузла або посилання можуть створюватися тимчасові цикли. Це пов'язано з тим, що повідомлення HELLO надсилаються з більш високою частотою, ніж повідомлення LSA, тому, якщо вузол виходить з ладу, його сусіди відчувають непрацюючий зв'язок перед іншими вузлами. Вони негайно перераховують свої таблиці маршрутизації, що може суперечити таблиці маршрутизації інших вузлів, і може бути створений цикл. Це може статися, коли два вузли мають інформацію з різним віком, і, отже, вони обчислюють свої таблиці маршрутизації на двох різних

топологіях мережі. FSR робить це за задумом, він вводить зони в мережі з потенційно різними наборами інформації, тому збільшує ймовірність створення тимчасових циклів.

3.7 Протокол LANMAR

LANMAR - це типовий протокол ієрархічної маршрутизації для масштабованих безпроводових спеціальних мереж групового руху. LANMAR запозичує концепцію орієнтиру, яка вперше була запроваджена в проводових мережах [12]. Він використовує поняття орієнтирів для відстеження логічних підмереж, в яких члени мають спільність інтересів і, ймовірно, рухаються як група (наприклад, бригада на полі бою, група студентів з того самого класу та команда колег на з'їзді).

Схема адресації в LANMAR ефективно відображає такі логічні групи. Він передбачає, що використовується адреса типу IP, що складається з ідентифікатора групи (або ідентифікатора підмережі) та ідентифікатора хоста, тобто <Ідентифікатор групи, Ідентифікатор хосту>. Адреса змінюється, якщо вузол переходить з групи в іншу, так само змінюється і IP-адреса, коли вузол в Інтернеті переходить з однієї підмережі в іншу. Кожна логічна група має обраний орієнтир. Кожен вузол у мережі використовує алгоритм маршрутизації з масштабом (наприклад, FSR [9], OLSR [13] або HSLS [10,21]), щоб дізнатись про маршрути в межах заданої області максимальної кількості стрибків. Щоб направити пакет до пункту призначення, який не входить в область його дії, вузол направить пакет на відповідний орієнтир до ідентифікатора групи такого призначення. Шлях до орієнтира поширюється по всій мережі за допомогою механізму вектора відстані. Як тільки пакет наближається до орієнтира, він, як правило, направляється безпосередньо до пункту призначення за допомогою локальної маршрутизації.

Для кожної групи алгоритм маршрутизації, що лежить в основі, надаватиме точну інформацію про маршрутизацію для вузлів, що знаходяться в області дії. Пакети оновлення маршрутизації обмежені лише в межах області дії. Інформація про маршрутизацію до віддалених вузлів (вузлів поза сферою дії вузла) узагальнюється відповідними орієнтирами. Цей вид узагальненої маршрутизації не буде сильно впливати на точність маршрутизації, оскільки вузли групи рухаються разом.

3.8 Протокол ZRP

Гібридний протокол ZRP (Zone Routing Protocol), в якому використовується проактивний механізм пошуку вузлів, що знаходяться в зоні маршрутизації, яка визначається сукупністю вузлів з мінімальною відстанню в хопах, що не перевищує вибраний радіус зони.

Пошук маршруту поза зоною заснований на розсилку службової інформації по її периметру, замість розсилки по всій мережі, і використання реактивного механізму пошуку маршрутів на вимогу до пунктів призначення, розташованих за межами зони маршрутизації. Проактивний компонент ZRP, званий внутризоновым протоколом маршрутизації (Intrazone routing protocol, IARP), реалізований на основі дистанційно-векторного алгоритму пошуку маршрутів, а межзоновый протокол (Interzone routing protocol, IERP) використовує механізм запит-відповідь для пошуку маршрутів на вимогу для взаємодії з вузлами в різних зонах.

3.9 Безпека протоколів багатошляхової маршрутизації

Спочатку протоколи маршрутизації, що розробляються для динамічно організованих телекомунікаційних мереж, не мали будь-якими захисними механізмами, які враховують специфіку даних мереж. Вказана обставина сприяло виникненню безлічі пасивних і активних атак на ці протоколи. Найбільшого поширення набули традиційні атаки типу «людина посередині» і «отказвобслуживаніі», а так само клас атак, що дозволяють перенаправляти мережеві пакети по помилковому маршруту [9, 10]. Далі перераховані основні види мережевих атак на протоколи маршрутизації для телекомунікаційних мереж з динамічною топологією. Класичним прикладом атаки типу «отказвобслуживаніі» є переповнення таблиць маршрутизації (Routing Table Overflow) сусідніх вузлів шляхом оголошення безлічі маршрутів до неіснуючих вузлів. У разі переповнення таблиці маршрутизації додавання в неї легітимних маршрутів стане неможливим. Атаку типу «блекхол» (Black Hole Attack) також можна віднести до атак типу «отказвобслуживаніі». У прикладі (рис. 3.4), що ілюструє атаку, мережеві пакети,

що проходять від відправника V1 через вузол порушника M, відкидаються і не передаються далі до одержувача V4.

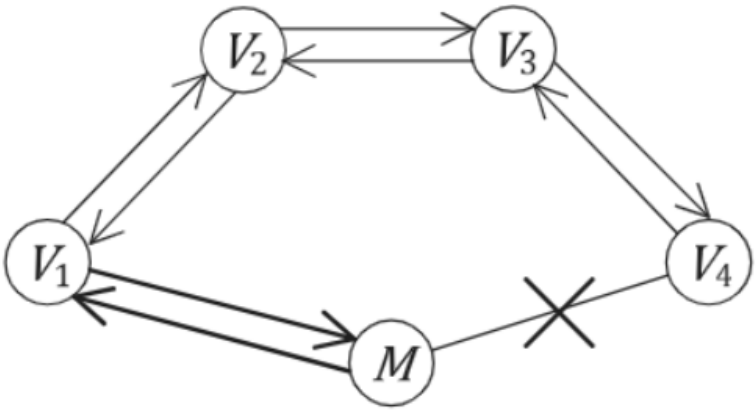


Рисунок 3.4 – Схема атак типа «блекхол» и «грейхол»

Існує безліч різновидів зазначеної атаки, включаючи вибіркове блокування керуючих пакетів протоколу маршрутизації, вибіркове блокування окремих пакетів даних (атака типу «грейхол») і повне блокування всіх пакетів. Вході атаки типу «сінкхол» (Sink Hole Attack) порушник M поширює помилковий оптимальний маршрут до вузла одержувача V4 і тим самим направляє через себе мережеві пакети, відправлені сусідніми вузлами V1 і V2 (рис. 3.5).

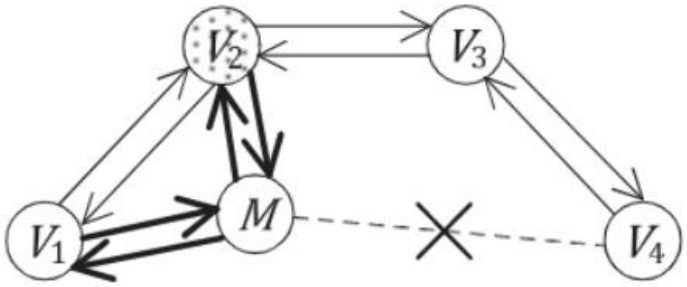


Рисунок 3.5 – Схема атаки типа «синкхол»

В результаті кооперації порушників здійснюється атака типу «вормхол» (Worm Hole Attack), суть якої полягає поза санкціонованому доступі до пакетів сусідніх пристроїв, що передаються до одержувача по реально існуючому високоякісному каналу, створеного порушниками. У прикладі (рис. 3.6), що ілюструє атаку, високі характеристики створюваного каналу дозволяють порушникам M1 і M2 запропонувати оптимальний маршрут від вузла V1 до вузла

V5 і в зворотному напрямку. В результаті мережеві пакети, що доставляються раніше через вузли V2, V3 і V4, будуть перенаправлені через вузли порушників.

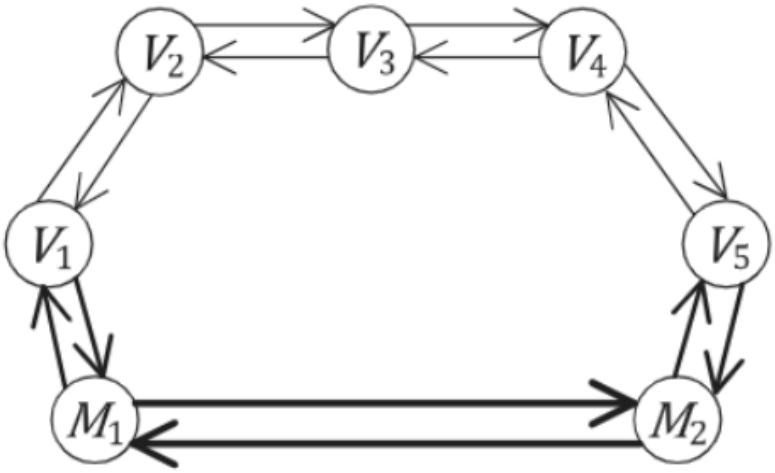


Рисунок 3.6 – Схема атаки типа «вормхол»

Крім вищеназваних атак, окремо можнавідзначити актуальність проблеми егоїстичності вузлів (Selfish Attack), що приховують маршрути з метою економії ресурсів, і атаки змови на механізм репутації, який використовується в ряді протоколів маршрутизації для забезпечення їх захисту (різновид Sybil Attack). Реалізація зазначеної атаки дозволяє завищити або занизити значення репутаціївузла, що також може привести до зміни маршруту доставки пакета.

В ході досліджень з питань забезпечення безпеки протоколів маршрутизації було запропоновано безліч рішень, що призвело до розробки ряду нових захищених протоколів. Слід зазначити, що більшість розроблених протоколів спираються на механізми криптографічних перетворень і були представлені як захищені версії (розширення) існуючих протоколів.

З огляду на домінуючий статус реактивних протоколів маршрутизації, основна увага дослідників і розробників приділяється забезпеченню безпеки даних протоколів. Так, протокол SAODV (Secure AODV) був запропонований для захисту керуючих пакетів протоколу AODV на основі асиметричної криптосистеми [12]. Аутентифікація пакетів RREQ і RREP проводиться за допомогою електронних підписів. Кожен керуючий пакет підписується секретним ключем відправника цього пакета. Проміжні вузли та кінцеві одержувачі пакетів проводять перевірку підпису і здійснюють обробку та передачу пакетів тільки в разі її валідності.

Оскільки пакети RREQ і RREP містять змінюване в процесі передачі поле Hop_Count (число переходів), аутентифікація цього поля проводиться окремо на основі ланцюжка хеш. Узелісточнік вибирає випадкове значення (seed) на початку процесу виявлення маршруту і встановлює максимальну кількість переходів (MHC).

Далі джерело обчислює значення Hash як хеш вихідного числа h (seed) і значення Top_Hash, як hMHC (seed). Проміжні вузли при отриманні керуючого пакета проводять перевірку коректності значення Top_Hash, враховуючи поточне значення поля Hop_Count, після чого збільшують значення поля Hop_Count і обчислюють нове значення Hash як h (Hash) перед подальшою розсилкою керуючого пакета RREQ. Одна з головних проблем протоколу SAODV пов'язана зі складністю безпечного розподілу ключів (протокол піддається атакам типу «людина посередині»).

Для вирішення даної проблеми реактивний протокол маршрутизації ARAN (Authenticated routing for ad hoc networks) [13] передбачає наявність в самоорганізується мережі засвідчує, і застосування криптографічних сертифікатів, що дозволяє забезпечити аутентифікацію сторін, цілісність даних і неспростовності.

В ході першої попередньої стадії протоколу кожен підключається до мережі вузол повинен ініціювати створення сертифіката відкритого ключа, підписаного підтверджуючий центр. Далі в ході реактивного виявлення маршрутів для всіх переданих повідомлень на основі згенерованих сертифікатів виконується обов'язкова аутентифікація джерела і одержувача, що дозволяє побудувати безпечний маршрут.

Крім того, для підвищення безпеки в рамках протоколу також передбачені перевірка підпису відправника повідомлення і формування нового підпису кожним проміжним передавальним вузлом. Разом з тим через складність і ресурсоємності процедури аутентифікації протокол ARAN не отримав широкого розповсюдження. Серед інших недоліків протоколу можна виділити проблему вибору, що засвідчує, і вразливість до атак типу «вормхол».

Підхід до захисту OLSRv1 на основі асиметричної криптографії запропонований розробниками протоколу SLSP (Secure Link State Routing Protocol) [15]. Протокол не передбачає створення виділеного центру розподілу ключів, натомість кожен вузол самостійно генерує ключову пару і передає свій

відкритий ключ всім сусіднім вузлам. Поширювані повідомлення вітання та відновлення маршрутизації підписуються секретним ключем відправника. Захист змінюваного поля «Hop Count» проводиться на основі розглянутого раніше механізму ланцюжка хеш; крім того, кожне оновлення містить поле «Sequence Number» (порядковий номер) для захисту від атаки відтворенням.

Таким чином, протокол забезпечує захищене виявлення сусідніх вузлів і поширення маршрутної інформації по мережі. Крім того, протокол SLSP стійкий до атак, виконуваних з метою переповнення таблиці маршрутизації. Кожному з сусідніх вузлів присвоюється значення пріоритету. Вузли, що генерують максимальну кількість оновлень маршрутизації, мають мінімальний пріоритет, що дозволяє знизити ефективність атаки на відмову в обслуговуванні. Незважаючи на те, що даний протокол не схильний до зовнішніх атак типу «блекхол» і «сінкхол», він не дозволяє протистояти різним атакам змови декількох порушників.

Протокол SRP (Secure Routing Protocol) [16], застосовуваний для захисту DSR і реактивної складової IERP гібридного протоколу ZRP, передбачає наявність загального ключа, використовуваного вузлом джерела і вузлом призначення при організації захищеного зв'язку SA (Security Association). Вузол джерела виробляє виявлення маршруту до вузла призначення за допомогою широкомовної розсилки керуючого пакета запиту маршруту RREQ, що включає пару ідентифікаторів (порядковий номер запиту і довільний ідентифікатор запиту) і код автентичності - значення ключової хеш-функції, яка розраховується на основі параметрів запиту (адреса вузла-джерела, адреса вузла призначення, ідентифікатори). Проміжні вузли, які беруть участь у пересиланні пакета RREQ, додають в пакет свої адреси, а вузол призначення здійснює аутентифікацію запиту за допомогою перевірки коду автентичності і формує відповідь пакет RREP, що включає використані ідентифікатори і новий код автентичності. Доставка пакета RREP проводиться повністю відповідно до маршруту доставки пакета RREQ, а вузол джерела здійснює його аутентифікацію при отриманні.

Застосування концепції маршрутизації від джерела дозволяє виключити необхідність здійснення криптографічних перетворень проміжними вузлами, що забезпечують пересилання пакетів між сторонами захищеного зв'язку, що особливо актуально в рамках даної архітектури з метою підвищення продуктивності і економії ресурсів. Незважаючи на всі переваги SRP, в рамках протоколу не розглядається проблема безпечного розподілу ключів в динамічно

організує мережі. Крім того, протокол SRP, як і багато інших, також піддається атакам типу «вормхол».

Протокол SEAD (Secure Efficient Ad hoc Distance-Vector), запропонований в роботі [17], базується на принципах роботи проактивного дистанційно-векторного протоколу DSDV. Особливістю протоколу можна вважати нестандартний механізм аутентифікації записів оновлень маршрутизації, заснований на ланцюжку хеш і дереві Меркле [18]. У відповідності зі специфікаціями протоколу DSDV кожен запис маршрутизації крім метрики маршруту включає порядковий номер. Довільний вузол при отриманні поновлення маршруту замінює запис в таблиці маршрутизації, тільки якщо порядковий номер поновлення вище поточного або значення метрики поновлення менше поточного значення за умови збігу порядкових номерів. Кожне оновлення також включає ідентифікатор джерела маршруту і значення hn-i * m + j з ланцюжка хеш, де m - діаметр мережі, i - порядковий номер запису маршруту, а j - значення метрики маршруту.

Таким чином, перехоплені значення ланцюжка хеш не дозволяють порушнику згенерувати оновлення з більш високим порядковим номером або с меншою метрикою (за умови збігу порядкових номерів). Разом з тим даний підхід не забезпечує захисту від модифікації інших важливих полів протоколу, а процедура генерації дерева Меркле, прив'язаного до ідентифікаторів вузлів мережі, обмежує застосування протоколу в мережах з динамічною топологією.

Протокол SDSDV (Secure DSDV) [19] переглядає підхід, закладений в протоколі SEAD. На відміну від SEAD протокол SDSDV не передбачає побудову дерева Меркле, в той час як кожен вузол генерує 2 * n ланцюжків хеш, де n - кількість вузлів мережі. Аутентифікація оновлень маршрутизації проводиться на основі додаткових полів AL (Alteration Field) і AC (Accumulation Field), які використовуються для захисту від зниження значення метрики і підвищення номера послідовності відповідно. Слід зазначити, що протоколи SEAD і SDSDV володіють типовими недоліками і схильні до всіх уязвимостям, характерним для протоколів даного класу.

Розробниками реактивного протоколу SAR (Security-Aware Ad-hoc Routing) [20] був запропонований перспективний підхід, що дозволяє забезпечити високу ступінь безпеки маршрутизації. Ключовою особливістю протоколу є присвоювання кожному вузлу деякого рівня безпеки. Проходження пакетів через вузли з рівнем безпеки нижче необхідного не є безпечним. При цьому головною

метрикою маршруту стає рівень його безпеки, а його значення визначається як найменше серед рівнів безпеки всіх вузлів, що входять в маршрут до вузла призначення. Виявлення маршрутів в рамках протоколу проводиться за запитом вузла відправника, оскільки спочатку SAR був запропонований як розширення безпеки протоколу маршрутизації AODV. У службовий пакет запиту маршруту RREQ поміщається необхідну відправником пакетів значення метрики безпеки маршруту. В результаті вузли, які отримали RREQ, але не володіють необхідним рівнем безпеки, не мають можливості оголошувати маршрут і не беруть участі в подальшій трансляції керуючого пакета. Вузол, що володіє маршрутом до вузла призначення з необхідним значенням метрики безпеки, відправляє вузлу джерела розширений відповідно до протоколу SAR службовий пакет RREP. Додатково протокол передбачає криптографічний захист всіх переданих пакетів (аутентифікація і шифрування). У ситуації, коли знайдено кілька маршрутів, які відповідають вимогам безпеки, передача пакетів здійснюється за маршрутом з мінімальним значенням метрики відстані. З іншого боку, навіть для повно-телекомунікаційної мережі вірогідні випадки, коли безпечний в розумінні протоколу маршрут не може бути запропонований.

Гнучкість протоколу SAR може бути розширена в рамках рольового підходу [21], що дозволяє враховувати тип інформаційного потоку при визначенні безпечного маршруту. Одна з основних проблем протоколу полягає у відсутності регламентованого механізму встановлення рівнів безпеки взаємодіючих вузлів, що ускладнює його практичне застосування.

Ефективний підхід для протидії атакам «блекхол», «сінкхол» і «вормхол» був запропонований в рамках протоколу SPREAD [22]. Ідея протоколу полягає в застосуванні порогової (k, n) схеми поділу секрету [23] до переданих повідомлень і подальшої доставки всіх частин секрету до одержувача за різними маршрутами на базі багатоколійні маршрутизації. Оскільки для відновлення секрету потрібно k частин, реалізація атак типу «блекхол» або «сінкхол» може бути успішною тільки при кооперації (n - k) порушників. Разом з тим надмірність, утворена при застосуванні зазначеної схеми, може бути суттєвим обмеженням у багатьох динамічно організованих мережах.

В цілому можна відзначити, що криптографічні перетворення дозволяють забезпечити повну аутентифікацію взаємодіючих сторін і шифрування даних, переданих в тому числі в рамках протоколів маршрутизації. Але в умовах

обмеженості ресурсів в безпроводових систем, що самоорганізуються мережах дані механізми (особливо криптосистеми з відкритим ключем) є надто витратними, що змушує шукати допоміжні рішення. Крім того, розглянуті підходи не дозволяють вирішити проблему егоїстичності вузлів, а правильність інформації, що надається аутентифицироваться вузлами, не може бути гарантована в рамках схем захисту, заснованих виключно на криптографічних перетвореннях. Таким чином, всі протоколи маршрутизації, безпеку яких забезпечується за даними схемами (з певними застереженнями, за винятком протоколів SAR і SPREAD), вразливі до атак внутрішніх порушників і заражених вузлів, оскільки передбачається, що будь-який аутентіфіцированний вузол є довіреною вузлом без будь-якої додаткової перевірки.

4 ДОСЛІДЖЕННЯ ПРОТОКОЛІВ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ

4.1 Аналіз продуктивності протоколів багашляхової маршрутизації

Як було зазначено, підвищити продуктивність Ad-hoc мереж можна за рахунок використання алгоритмів багатошляхової маршрутизації, які, на відміну від алгоритмів маршрутизації найкоротшого маршруту, дозволяють балансувати завантаженість мережі, збільшуючи її продуктивність у 1,5 – 2 рази [21]. Додатково забезпечується відмовостійкість мережі.

В табл. 4.1 – 4.3 представлені основні показники продуктивності Ad-hoc мереж, які являють собою найгірший сценарій кожного протоколу маршрутизації. У зазначених таблицях використані наступні позначення:

– СЗНВ – складність зв'язку в найгіршому випадку, тобто кількість повідомлень, необхідних для виконання операції оновлення;

– ТСГВ – тимчасова складність гіршого випадку, тобто кількість кроків, необхідних для виконання операції оновлення;

– СМ – структура маршрутизації: П – плоска; І – ієрархічна; – HELLO – hello-повідомлення;

– N – кількість вузлів в мережі; – D – діаметр мережі; – КМ – кілька маршрутів;

– ПМ – періодичні маячки;

– А – кількість вузлів учасників процесу маршрутизації;

– Z – діаметр спрямованого шляху, в якому проходить RREP або RERR-пакет;

– Y – загальна кількість вузлів, що утворюють спрямований шлях, в якому проходить RREP або RERR-пакет;

– * – маяки з точки зору повідомлень hello;

– # – маяки, що визначають відправлення періодичних пробних пакетів уздовж активних маршрутів – - G-максимальний ступінь маршрутизатора;

– | E | – кількість ребер у мережі;

– r – кількість вузлів в шляху відповіді маршруту;

– n – кількість вузлів в зоні, кластері або дереві;

– d – діаметр зони, кластера або дерева;

– MPR – багатошляхове реле.

Таблиця 4.1 – Показники продуктивності проактивних протоколів багатошляхової маршрутизації

Протоколи маршрутизації	СЗНВ	ТСГВ	СМ	HELLO	Критичні вузли	Частота оновлень	Кількість таблиць	Перевага	Недоліки
OLSR	O(N)	O(D)	П	Так	Ні	Переодична	3 (таблиці маршрутизації, сусідів і топологій)	MPR зменшує контроль головного вузла	Потрібне знання сусідів на 2 хопу
OSPF	O(N)	O(D)	І	Так	Ні	Переодична, відправляя LSA	1 (таблиця маршрутизації побудована з бази даних стану каналу)	Оптимізація протоколу маршрутизації чистого каналу зв'язку	Використовується тільки для інтернет-спільноти
FSR	O(N)	O(D)	І	Так	Ні	Переодична, відправляя LSA	3 (таблиці маршрутизації, сусідів і топологій)	Зменшений обсяг службової інформації розсилаємої по мережі	При розриві вузла або каналу можуть створюватися тимчасові цикли

Більшість проактивних протоколів маршрутизації має погану масштабованість. Це пов'язано з тим, що процедура оновлення споживає значну пропускну здатність мережі. З розглянутих протоколів маршрутизації протокол OLSR має найкращу масштабованість. Стійкість протоколу OLSR досягається за рахунок скорочення числа ретрансляцій через механізм MPR, використовуваний для вибору декількох сусідніх вузлів для ретрансляції повідомлення. Протоколи з ієрархічною структурою масштабують більшу частину потоків повідомлень, оскільки вони ввели структуру в мережу, яка контролює кількість службових повідомлень, що передаються через мережу. Загальним недоліком, пов'язаним з усіма ієрархічними протоколами, є необхідність управління мобільністю. Управління мобільністю вводить непотрібні накладні витрати в мережі (наприклад, додаткові службові надбавки для формування і обслуговування кластерів). Через динамічні зміни в управлінні мобільністю в протоколі OSPF передаються непотрібні пакети управління.

Таблиця 4.2 – Показники продуктивності реактивних протоколів багатошляхової маршрутизації

Протоколи маршрутизації	СЗНВ (виявлення маршруту)	СЗНВ (обслуговування маршруту)	ТСГВ (виявлення маршруту)	ТСГВ (обслуговування маршруту)	СМ	ПМ	КМ	Перевага	Недоліки
AODV	O(2N)	O(2N)	O(2D)	O(2D)	П	Так	Так	Відсутність додаткового трафіку при передачі даних за встановленим маршрутом	Вимагає періодичних повідомлень HELLO
DSR	O(2N)	O(2N)	O(2D)	O(2D)	П	Ні	Так	Не застосовується метод періодичної розсилки повідомлень як в AODV	Не відновлює розірвані з'єднання в місцевому масштабі

Реактивні багатошляхові протоколи маршрутизації зменшують витрати енергії, зберігаючи інформацію тільки для активних маршрутів. Це означає, що маршрути визначаються і підтримуються щоразу, коли вузлам необхідно відправляти дані в конкретний пункт призначення. Виявлення маршруту відбувається шляхом розсилки пакетів запиту маршруту через всю мережу. Коли запит досяг вузла призначення, він посилає у відповідь пакет з маршрутом назад у вихідний вузол з використанням розвороту посилань, якщо запит маршруту пройшов через двонаправлені лінії або шляхом підгонки маршруту. Існує дві категорії реактивних багатошляхових протоколів на основі стратегії маршрутизації [9]: маршрутизація джерела та маршрутизація з одним переходом.

Серед різних реактивних протоколів багатошляхової маршрутизації (табл. 4.2) протоколи маршрутизації з одним переходом є більш використовуваними в Ad-hoc мережах, ніж протоколи маршрутизації від джерела.

Гібридні протоколи маршрутизації є протоколами нового покоління. Ці протоколи маршрутизації мають як реактивні, так і проективні властивості, зберігаючи внутрішньозонову інформацію (проактивні властивості) і міжзональну інформацію (реактивні властивості). Ці протоколи призначені для підвищення масштабованості, дозволяючи вузлів, розташованих близько один до одного, працювати разом, щоб сформувати якусь основу для скорочення витрат енергії на виявлення маршруту. Це досягається за рахунок проактивного підтримки

маршруту поруч з вузлами і визначення маршрутів до далеких вузлів, використовуючи стратегії реактивної маршрутизації.

Таблиця 4.3 – Показники продуктивності гібридного протоколів багатошляхової маршрутизації

Протоколи маршрутизації	СЗНВ (виявлення маршруту)	СЗНВ (обслуговування маршруту)	ТСГВ (виявлення маршруту)	ТСГВ (обслуговування маршруту)	СМ	ПМ	КМ	Перевага	Недоліки
ZRP	O(N+r) або O(n)	O(N+r) або O(n)	O(2D) або O(d)	O(2D) або O(d)	П	Так	Так	Зниження зв'язку в порівнянні з проактивними алгоритмами маршрутизації; більш швидке виявлення маршруту в зоні, ніж в будь-якому протоколі реактивної маршрутизації	Для великих значень зони маршрутизації він може вести себе як протокол реактивної маршрутизації; накладання зони
LANMAR	O(N+r) або O(n)	O(N+r) або O(n)	O(2D) або O(d)	O(2D) або O(d)	П	Так	Так	Покращена масштабованість для великих Ad hoc мереж	Застосовується виключно в спеціалізованих мережах, які показують групу мобільності

Гібридні протоколи маршрутизації є протоколами нового покоління. Ці протоколи маршрутизації мають як реактивні, так і проективні властивості, зберігаючи внутрішньозонову інформацію (проактивні властивості) і міжзональну інформацію (реактивні властивості). Ці протоколи призначені для підвищення масштабованості, дозволяючи вузлів, розташованих близько один до одного, працювати разом, щоб сформувати якусь основу для скорочення витрат енергії на виявлення маршруту. Це досягається за рахунок проактивного підтримки маршруту поруч з вузлами і визначення маршрутів до далеких вузлів, використовуючи стратегії реактивної маршрутизації.

Більшість гібридних протоколів, пропонованих на сьогоднішній день, засновані на формуванні зон (вузли поділяються в зони) або кластерів, що означає, що вузли групуються в дерева або кластери.

В табл. 4.4 показано загальне порівняння всіх груп багатошляхової маршрутизації. Розглядаючи показники продуктивності і характеристики всіх категорій протоколів маршрутизації, можна зробити наступні висновки.

У проактивній маршрутизації адресація може бути простою в реалізації, однак вона може не дуже добре масштабуватися для великих мереж [11]. Однак найбільшою проблемою проактивних протоколів є управління місцем розташування. Реактивні протоколи маршрутизації мають проблеми з масштабністю. Щоб підвищити масштабованість, необхідно контролювати виявлення маршруту і обслуговування маршруту. Це може бути досягнуто шляхом локалізації поширення керуючого повідомлення в певному сегменті, де знаходиться пункт призначення.

Протокол маршрутизації ZRP є гібридним протоколом маршрутизації, який призначений для підвищення масштабованості Ad-hoc мережі. Перевага цього протоколу полягає в тому, що він підтримує сильну мережеву зв'язок (проактивно) в зонах маршрутизації при визначенні віддаленого маршруту (за межами зони маршрутизації) швидше, ніж інші. Ще одна перевага ZRP полягає в тому, що він може взаємодіяти з іншими протоколами маршрутизації для підвищення його продуктивності.

Всі розглянуті протоколи маршрутизації, проактивні, реактивні або гібридні, спрямовані на забезпечення QoS, але поки не можуть гарантувати повного задоволення всіх вимог за якістю. Властиві їм недоліки в тій чи іншій мірі обмежують область застосування протоколів або можливості роботи з мережею, де вони використовуються. Протоколи мають кілька показників продуктивності тому для порівняльного аналізу та вироблення рекомендацій щодо застосування можна використовувати методи багатокритеріальної оптимізації [3].

У вивченій літературі наводиться детальне порівняння вищевказаних протоколів шляхом імітаційного моделювання їх роботи в різних умовах (рис. 4.1)., сукупність яких називаються сценаріями роботи мережі [18-20].

Таблиця 4.4 – Загальне порівняння всіх груп протоколів багатошляхової маршрутизації

Параметр	Проактивні протоколи	Реактивні протоколи	Гібридні протоколи
Структура маршрутизації	Як плоскі, так і ієрархічні	Зазвичай плоскі	Зазвичай ієрархічні
Доступність маршрутів	Завжди доступні для досяжних вузлів	Визначаються, коли це необхідно. Іноді альтернативні маршрути зберігаються протягом обмеженого часу	Завжди доступні, коли джерело і одержувач знаходяться в межах тієї ж зони/кластера/дерева
Обсяг керуючого трафіку	Зазвичай високий обсяг, але іноді робляться скорочення	Зазвичай нижче, ніж у проактивній маршрутизації	Значно нижче ніж в проактивних і реактивних протоколах маршрутизації
Вимоги до зберігання	Досить високі	Залежать від кількості збережених або необхідних маршрутів. Зазвичай нижчі, ніж для проактивних	Нижчі, ніж для проактивних і реактивних протоколів маршрутизації, за умови правильного визначення розміру зон / кластерів / дерев у великих мережах
Затримка для виявлення маршруту	Визначається, коли маршрути малі	Вище, ніж для проактивних протоколів маршрутизації	Затримка така ж як у проактивних протоколів маршрутизації, якщо джерело і одержувач знаходяться в одній і тій же зоні / кластері / дереві. В іншому випадку затримка вище, ніж у проактивних протоколів, але нижче, ніж у реактивних
Підтримка мобільності	Підтримка низької або помірної мобільності. Для ієрархічної структурованої маршрутизації зазвичай потрібна мобільність груп	Може підтримувати більш високу мобільність, ніж проактивні протоколи маршрутизації	Зазвичай підтримується більш низький рівень мобільності, ніж протоколи реактивної маршрутизації, оскільки структура маршрутизації в основному є ієрархічною
Масштабованість	Зазвичай до 100 вузлів. В OSPF і OLSR можуть збільшуватися	Протокол маршрутизації джерела погано масштабується (зазвичай до декількох сотень вузлів)	1000 або більше

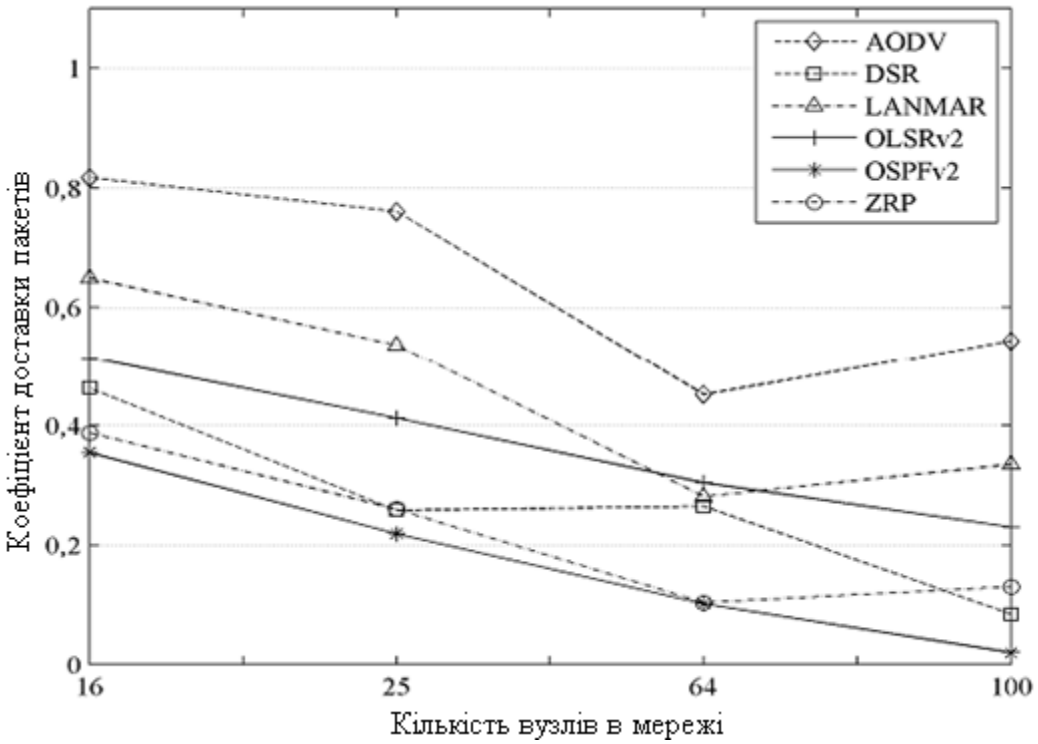


Рисунок 4.1 – Результати імітаційного моделювання

Як приклад наведені результати одного подібного експерименту, виробленого в симуляторі «QualNet Developer 4.5». Вимірювалася залежність коефіцієнта доставки пакетів (відношення числа прийнятих пакетів з даними до числа переданих) від розміру мережі для протоколів AODV, DSR, LANMAR, OLSR, OSPFv2, ZRP.

Представлені результати дозволяє кількісно оцінити роботу протоколів, наприклад, переконатися в тому, що класичний OSPF показує більш низькі результати в умовах мобільних Ad hoc мереж, ніж спочатку розроблені для них протоколи маршрутизації [19]. Тому, в атестаційній роботі розглядається модифікований MP-OLSR з використанням багатошляхового алгоритму Дейкстри.

4.2 Багатошляховий алгоритм Дейкстри

Довільна мережа може бути представлена графом G = (V, E, c), де V набір вузлів, E ⊂ V xV набір ребер, c: V → R*+ строго позитивна функція ваг. Передбачається, що граф спочатку ненаправлений тобто (v1, v2) ∈ E => (v2,

v1) ∈ E і c(v1, v2) = c(v2, v1), і цей граф без «петель», тобто не існує дуг, що з'єднують вузол з самим собою. Також передбачається, що не існує пар вершин, які можуть бути з'єднані більш ніж однією дугою. Якщо дана пара різних вершин (s, d) ми можемо визначити шлях між s і d як послідовність вершин (v_1, v_2, ... , v_m) таким чином, що (v_q, v_{q+1}) ∈ E , v_1 = s и v_m = d.

Для вихідного вузла мережі, MP-OLSR буде підтримувати оновлюваний прапор для кожного можливого вузла в мережі, щоб визначити достовірність шляху до відповідного вузла. Спочатку для кожного вузла і $updatedFlag_i$ (оновлений флаг$_i$) встановлено в false, що означає, що маршрут до відповідного призначення не існує або повинен бути оновлений. Коли з'являється запит маршруту до конкретного вузла i, вузол джерело буде перевіряти $updatedFlag_i$.

Якщо $updatedFlag_i$ рівний false вузол буде виконувати алгоритм (рис. 4.2) для отримання множини шляхів до вузла i, збереження їх в таблицю багатошляхової маршрутизації та оновлення відповідного флага $updatedFlag_i$ на true.

Якщо $updatedFlag_i$ рівний true, вузол буде шукати ефективний шлях до вузла i в таблиці багатошляхової маршрутизації. Кожен раз, коли вузол отримує нове повідомлення TC або HELLO, результатом цього буде зміна інформації в базі топології, всі $updatedFlag_i$ будуть встановлені в false.

Запропонований алгоритм застосовується до графа G = (V, E, c), двом вершинам (s, d) ∈ E^2 і строго позитивному цілому числу N. Він надає множини N (P_1, P_2,…, P_N) із (s, d) шляхів, витягнутих з графа G. Функція Dijkstra(G, n) це стандартний алгоритм Дейкстри, який надає вихідне дерево найкоротших шляхів від вершини n у графі G; GetPath(SourceTree,n) це функція, яка витягує найкоротший шлях до n з дерева джерела SourceTree; Reverse(e) дає протилежне ребро e; Head(e) надає ребро вершини, на яке вказує e.

Функція f_p и f_e використовується на кожному кроці для того, щоб отримати роз'єднаний шлях між s и d. f_p використовується для збільшення ваг дуг, які належать попередньому шляху P_i. Це змушує наступні шляхи використовувати інші дуги. fe використовується для підвищення ваг дуг, які ведуть до вершин попереднього шляху Pi. Таким чином маємо три можливих значення установок:

Якщо id = f_e < f_p, шляхи будуть роз'єднані по дугах;

Якщо id < f_e = f_p, шляхи будуть роз'єднані по вершинам;

Якщо id < f_e < f_p, шляхи також будуть роз'єднані по вершинах, але не обов'язково роз'єднані по дугах.

Де id це функція ідентифікації.

```
MultiPathDijkstra(s, d, 𝒢, N)
c_1 ← c
𝒢_1 ← 𝒢
for i ← 1 to N do
   SourceTree_i ← Dijkstra(𝒢_i, s)
   P_i ← GetPath(SourceTree_i, d)
   for all arcs e in ℰ
      if e is in P_i OR Reverse(e) is in P_i then
         c_{i+1}(e) ← f_p(c_i(e))
      else if the vertex Head(e) is in P_i then
         c_{i+1}(e) ← f_e(c_i(e))
      else
         c_{i+1}(e) ← c_i(e)
      end if
   end for
   𝒢_{i+1} ← (𝒱, ℰ, c_{i+1})
end for
return (P_1, P_2, ..., P_N)
```

Рисунок 4.2 – Багатошляховий алгоритм Дейкстри

Використовуючи функції ваг ми можемо очікувати виявлення відмінності в N шляхах щодо мережевої топології. Але навпаки того, щоб представляти строго роз'єднані по вузлах шляху, множинні шляхи генеруються алгоритмом необов'язково будуть повністю роз'єднаними. Причина цьому в тому, що кількість роз'єднаних шляхів обмежена в (s, d) мінімальним зрізом (визначеним як розмір найменшої множини ребер, який не може бути порушений для того, щоб з'єднати s d). Цей мінімальний зріз часто визначається оточенням джерела і одержувача. Наприклад, якщо s має лише три різних поруч стоять вузла, не можливо згенерувати більш, ніж три роз'єднаних шляху від s до d. Як наслідок, це обмеження роз'єднаності може бути локальним, а залишок мережі бути досить широкий для надання набагато більшої кількості роз'єднаних шляхів. Інший

недолік алгоритму з повністю роз'єднаними шляхами це те, що він може згенерувати дуже довгі шляхи, так як локальний зріз (дуг) може бути використане лише раз. Наприклад, на (рис.4.3) вузол S намагається отримати множину шляхів до вузла D. Для багатошляхового алгоритму Дейкстри ми використовуємо кількість переходів як вартість шляху (метрика) і набір $f_p(c)=3c$, и $f_e(c)=2c$. Спочатку ваги всіх зв'язків встановлені в 1. На першому кроці буде знайдений найкоротший шлях S→A→B→G→D. Далі будуть використані функції ваг для збільшення ваг відповідних дуг:

1. S→A, A→B, B→ G и G→D будуть змінені з 1 в 3, використовувати f_p.
2. S→C и F→G будуть змінені з 1 в 2, використовувати f_e.

Тоді на наступному кроці буде знайдений наступний найкоротший шлях

S→C→E→F→G→D. Якщо використовувати стандартний алгоритм, і видаляти проміжні вузли A, B, G після першого кроку, то це унеможливлює отримання другого шляху [17].

Як продемонстровано вище, інша перевага використання функції ваг це те, що можна отримати різні множинні шляхи (роз'єднаним по вузлам або роз'єднаним зв'язків) використовуючи різні функції ваг відповідно нашим побажанням і задачам мережі.

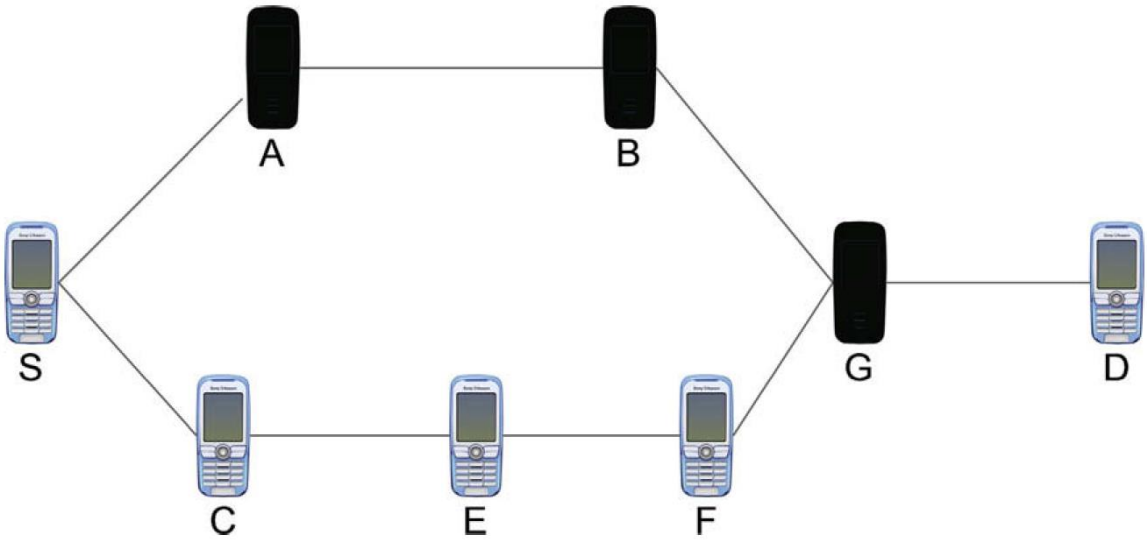


Рисунок 4.3 Множина шляхів від вузла S до вузла D

Другий приклад мережевої топології наведено на (рис.4.4).

Якщо ми виберемо $f_p(c)=3c$ и $f_e(c)= c$ (штраф тільки до використаних зв'язків) тоді ми отримаємо два роз'єднані по зв'язках шляху: S→A→C→B→D и

S→E→C→H→D. Якщо ми виберемо $f_p(c)=3c$ и $f_e(c)= 2c$ (штраф тільки до використаних вузлів), тоді алгоритм буде шукати роз'єднані по вузлах шляху. Таким чином будуть знайдені шляхи S→A→C→B→D и S→E→ F →G→H→D.

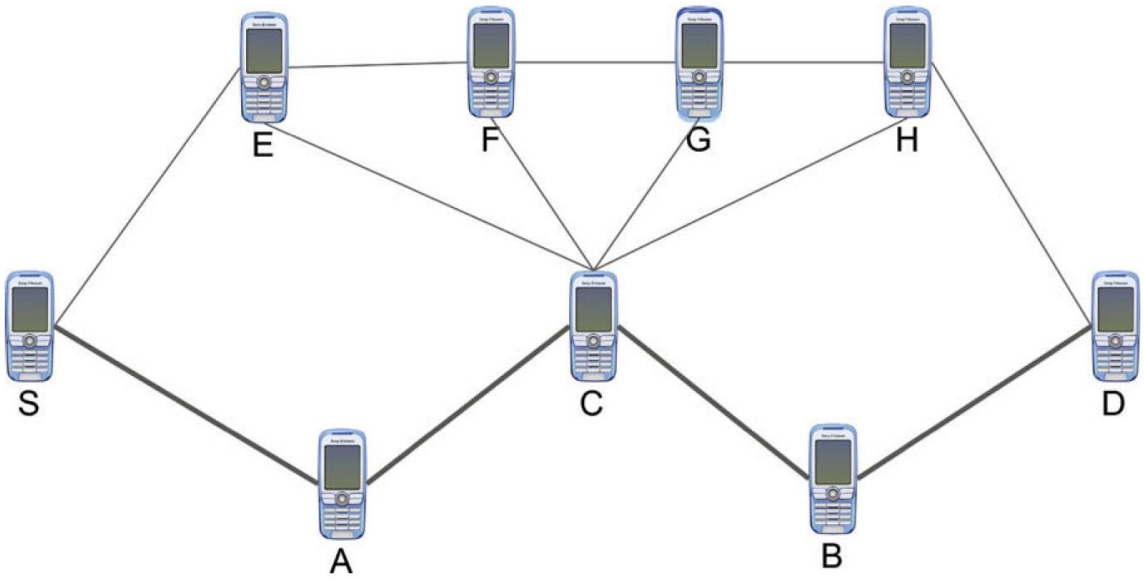


Рисунок 4.4 – Приклад мережевої топології

4.3 Порівняльний аналіз протоколів MP-OLSR і OLSR

У аналізованої літературі проведено порівняння продуктивності протоколів MP-OLSR і OLSR в різних ситуаціях з різними метриками [22]. MP-OLSR в даному порівнянні використовується з наступними функціональностями - визначення петель і відновлення маршруту. Табл.1 із заданими параметрами моделювання уявлення в додатку А. Табл.2 з параметрами протоколів представлена в додатку Б. На рис.4.5 представлений відсоток доставки даних по двох протоколах. OLSR має трохи кращий відсоток доставлених пакетів у порівнянні з MP-OLSR (близько 3%) лише на швидкості 1 м/с (3,6 км/год). Причиною тому збільшення кількості шляхів одночасної передачі, зростає ймовірність виникнення колізій на MAC рівні. Ці міжколійний впливу можуть бути усунені шляхом використання багатоканальної апаратури, яка гарантує різні смуги частот для кожного з шляхів [19]. В даному випадку використовується тільки один частотний канал, тому протокол MP-OLSR має більше втрачених пакетів через колізії на MAC рівні.

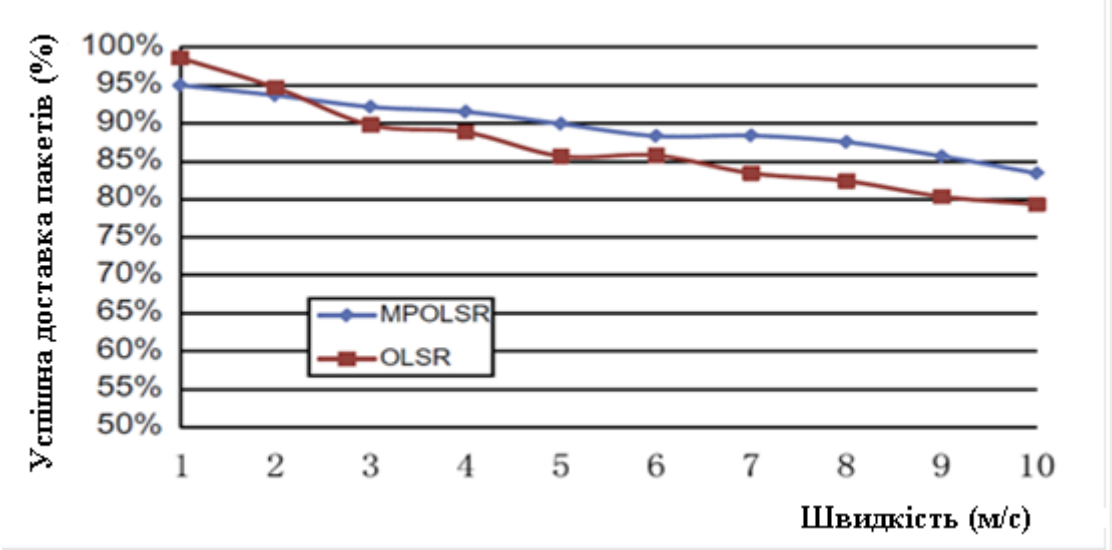


Рисунок 4.5 – Доставка пакетів протоколами MP-OLSR і OLSR в ситуації з 81 вузлом і 4 джерелами

Однак, у міру збільшення швидкості руху вузлів зв'язку між ними стають більш нестабільними і в мережі з'являється більше «петель». Відсоток вдалої доставки протоколу OLSR швидко зменшується і він поступається MP-OLSR. У порівнянні з невеликим виграшем у відсотку вдалої доставки (близько 5% на високій швидкості, рис.4.5), протокол MP-OLSR працює набагато краще за показниками середньої затримки, ніж протокол OLSR (як показано на рис.4.6).

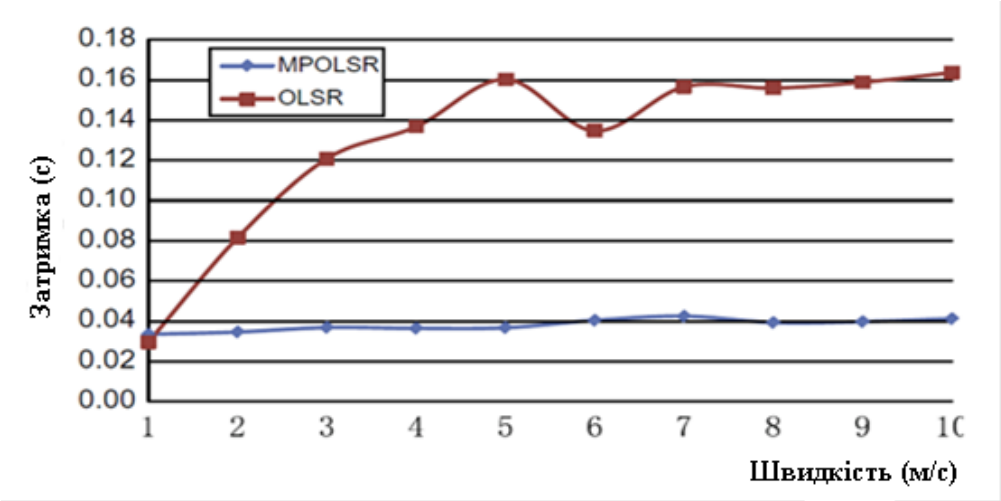


Рисунок 4.6 – Середня затримка від відправника до одержувача в ситуації з 81 вузлом і 4 джерелами

Затримка OLSR в 4 рази більше, ніж MP-OLSR починаючи зі швидкості 4 м/с (14,4 км/год). Затримка з кінця в кінець» включає затримку поширення від відправника до одержувача та затримку в черзі в кожному транзитному вузлі. MP-OLSR може мати більш тривалу затримку поширення тому, що деякі пакети

направляються по більш довгим маршрутах. Як показано (рис.4.7), MP-OLSR, має значно менший час затримки в черзі в порівнянні з OLSR.

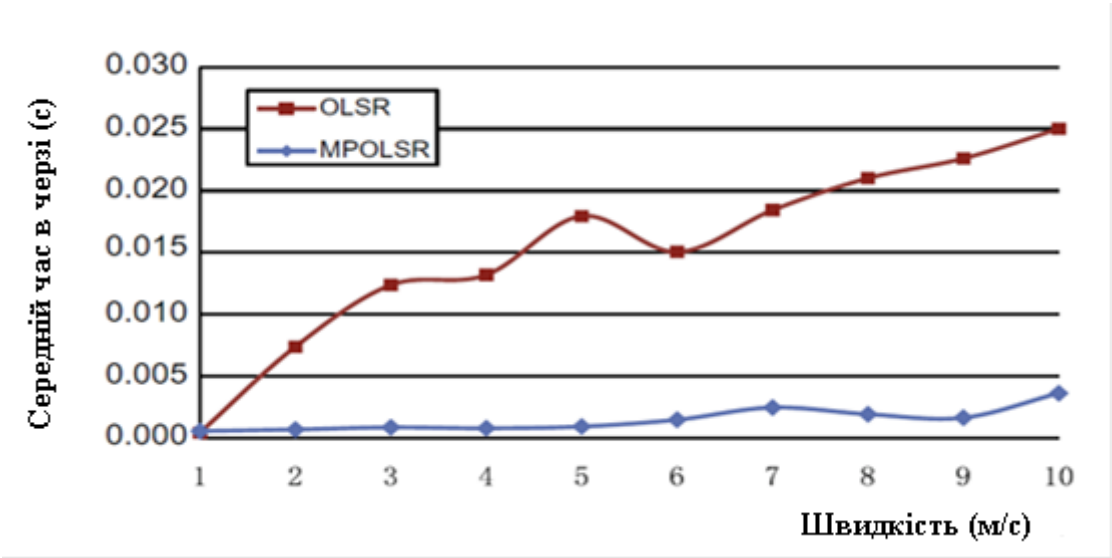


Рисунок 4.7 – Середній час в черзі MP-OLSR і OLSR в ситуації з 81 вузлом і 4 джерелами

У моделювання MP-OLSR також дає більш стабільну затримку при різних умовах [17,19]. Рис.4.8 і 4.9 показують розподіл затримки всіх прийнятих пакетів в ситуації із середньою рухливістю (0-5 м / с). Розподіл затримки OLSR досягає великих значень в порівнянні з OLSR. В цьому випадку з 2731 пакета, прийнятих з використанням OLSR, 1967 пакетів (82,96%) прийнято з затримкою менше 0,1 с. Для MP-OLSR з 2776 пакетів (97,69%) досягло одержувача за 0,1 с. Фактично, стандартна девіація затримки протоколу OLSR щонайменше в 10 разів більше, ніж для протоколу MP-OLSR і навіть іноді в 100 разів для ситуацій з більш рухливими вузлами.

Що стосується повідомлень управління маршрутизацією, так як MP-OLSR не змінює механізм контролю топології протоколу OLSR, обидва протоколи, як правило, мають однакову кількість згенерованих повідомлень управління маршрутизації. У моделюванні кількість згенерованих повідомлень HELLO і TC практично однаково [19]. З отриманих результатів моделювання можна зробити висновок, що в порівнянні з OLSR, MP-OLSR має майже таку ж продуктивність при низькій рухливості вузлів і завантаженні мережі. Однак, коли швидкість вузлів або завантаження мережі зростає, MP-OLSR має кращий відсоток доставки і більш меншу затримку, ніж OLSR через здатність розподіляти пакети по різних маршрутах.

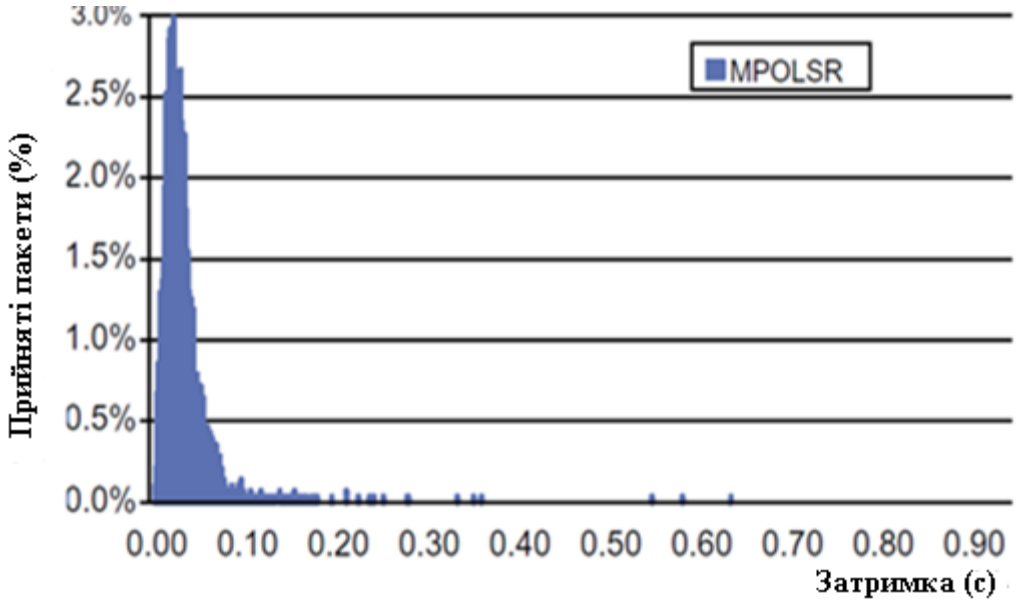


Рисунок 4.8 – Розподіл затримки прийнятих пакетів MP-OLSR в ситуації з 81 вузлом і 4 джерелами

На (рис.4.10) показаний відсоток вдалої доставки пакетів в ситуації з 81 вузлом і 10 джерелами. У порівнянні з предидущим сценарієм, цей є більш складним, так як трафік в мережі зростає, отже зростає затримка на обробку в чергах (рiс.4.11), також можлива поява більшого числа колізій.

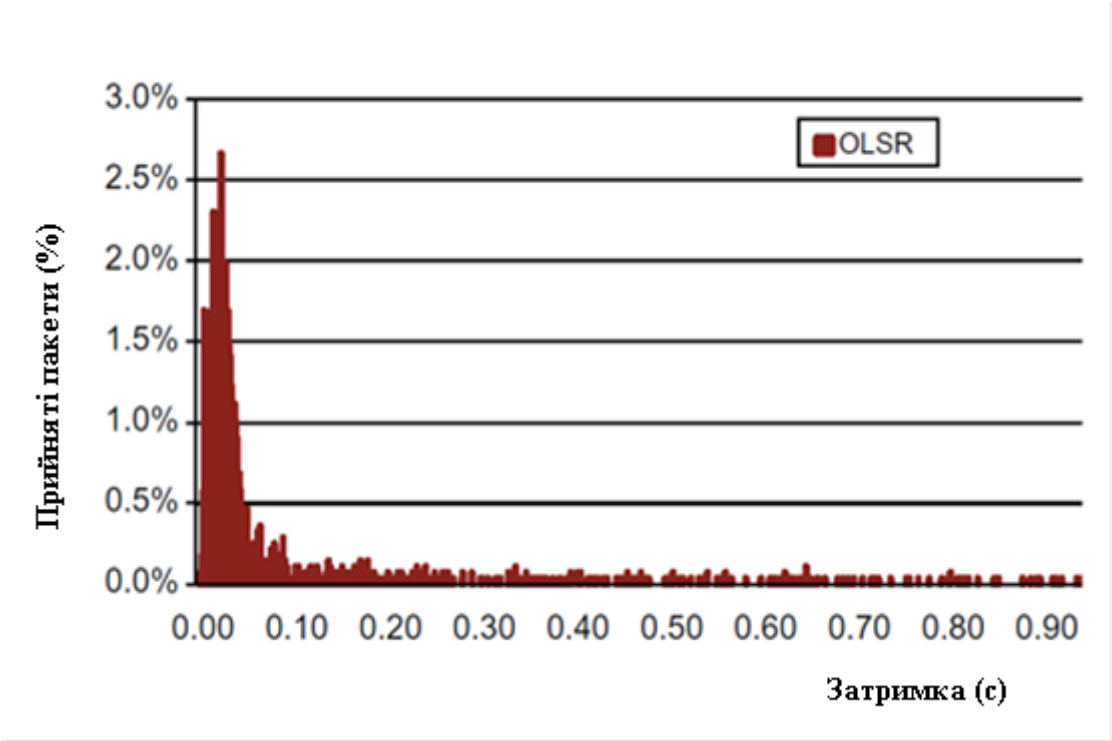


Рисунок 4.9 – Розподіл затримки прийнятих пакетів OLSR в ситуації з 81 вузлом і 4 джерелами

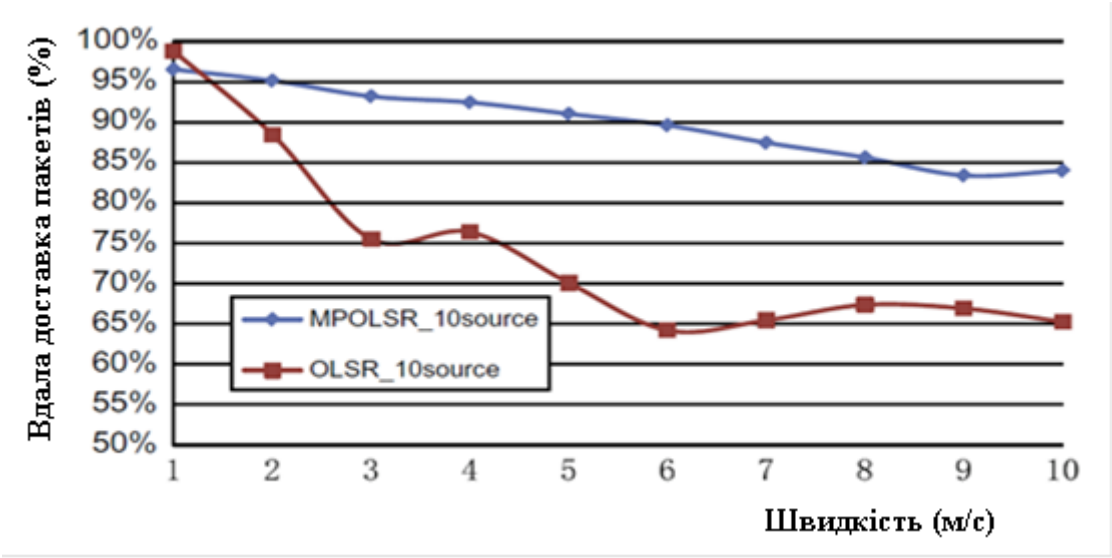


Рисунок 4.10 – Відсоток доставки OLSR і MP-OLSR в ситуації з 81 вузлом і 10 джерелами

Так як MP-OLSR це гібридний протокол і використовує маршрутизацію від джерела, то необхідно проаналізувати різницю між проактивного маршрутизацією і реактивної.

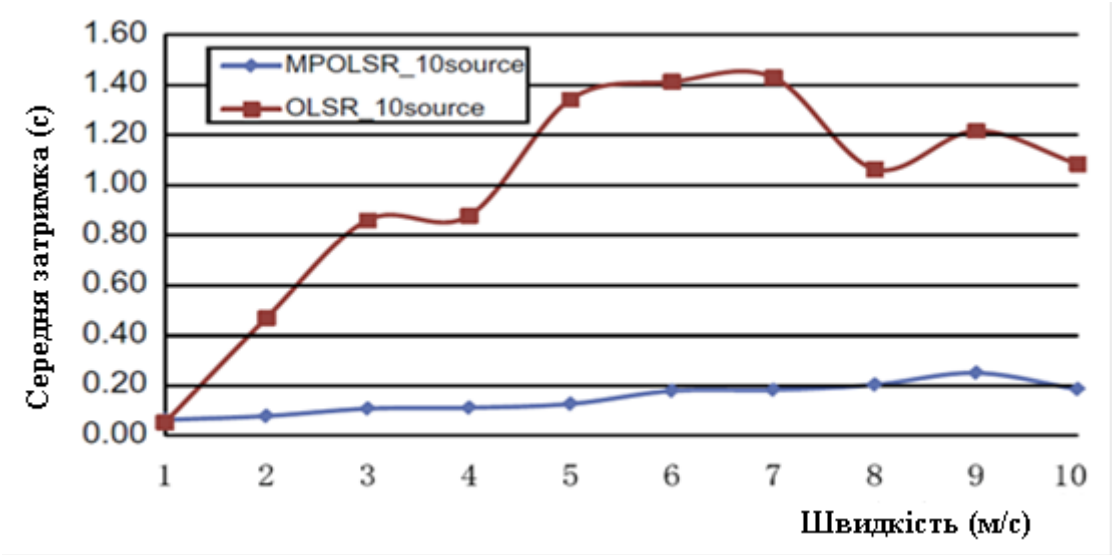


Рисунок 4.11 – Середня затримка OLSR і MP-OLSR в ситуації з 81 вузлом і 10 джерелами

Продуктивність DSR також була виміряна. (Рис.4.12, 4.13) показують відсоток доставки і затримку DSR відповідно (у порівнянні з OLSR і MP-OLSR). DSR має практично ту ж продуктивність, що і інші протоколи при низькій швидкості вузла (1 м/с і 2 м/с).

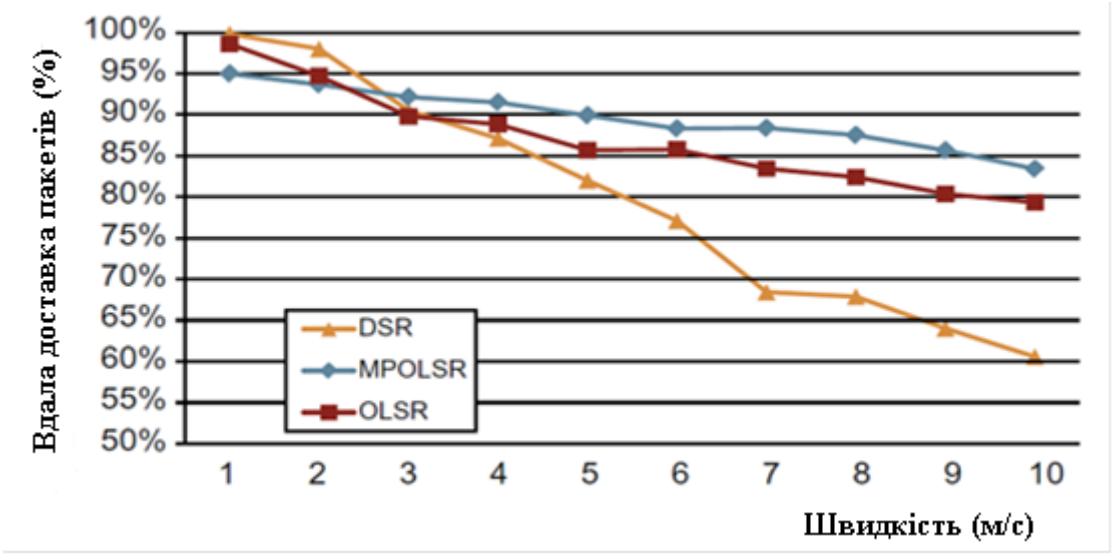


Рисунок 4.12 – Відсоток доставки пакетів при використанні різних протоколів

Однак, коли рухливість зростає, втрата пакетів і затримка DSR значно збільшуються. Фактично, DSR використовує маршрутизацію від джерела, як MP-OLSR, і також має відповідний механізм відновлення маршруту. Але реактивна природа DSR не може адаптуватися до частих змін топології. Його механізм відновлення маршруту заснований на передачі додаткових повідомлень RERR (rout error, помилка маршруту), які будуть швидко збільшуватися (кількість) при зростанні швидкості вузла. З іншого боку, відновлення маршруту MP-OLSR, яке засноване на відповіді канального рівня і локальної інформаційної бази даних топології мережі, не вимагає додаткових передач пакетів в мережі. Були запропоновані кілька багатоколійні протоколів маршрутизації, заснованих на DSR, наприклад SMR, які залежать від такого ж реактивного механізму [13]. Реактивний властивість робить ці протоколи важкими для порівняння з проактивними аналогами в ситуаціях з частими змінами топології. Згідно результатів моделювання? навіть якщо він може зменшити затримку до 1/5 від DSR (в порівнянні із значенням в DSR) це все ще значно більше, ніж у проактивних протоколів [13]. Як і OLSR, після прийняття повідомлень HELLO u TC, MP-OLSR оновлює інформаційну базу мережевої топології.

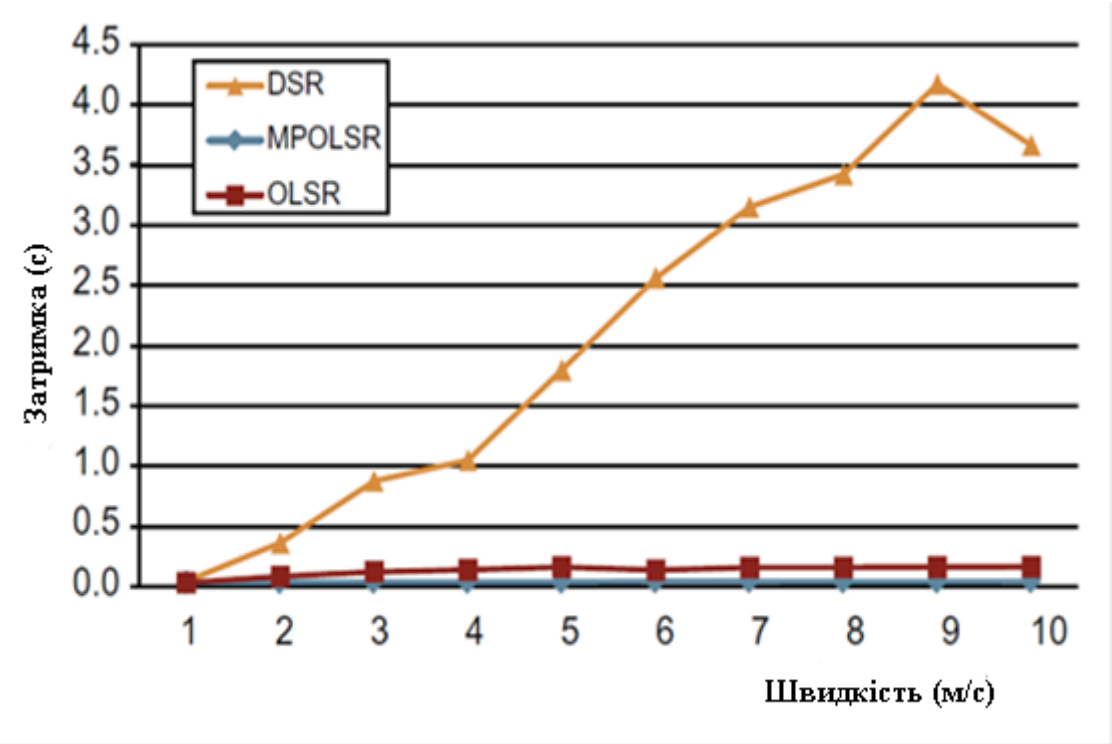


Рисунок 4.13 – Середня затримка в сценарії з 81 вузлом і 4 джерелами

Але для MP-OLSR більш ніяких операцій не проводиться, так як маршрутізаціонная таблиця в цей момент не перераховується. Для відправки призначених для користувача даних стек TCP / IP надсилає запит до MP-OLSR для обчислення безлічі шляхів до одержувача (для першого запиту або коли змінюється топологія) або для повернення обчислених маршрутів (для подальших запитів).

Варто зазначити, що для зручності розробки і налагодження модуль MP-OLSR в даний час існує в вигляді програми рівня додатків (рис.4.14). В майбутньому, заради ефективності та практичного використання, а не в даній моделі, буде краще, якщо помістити модуль MP-OLSR в ядро Linux, як модуль.

Далі представлеются два різні сценарії для порівняння продуктивності багатоколійні і однопутевого протоколів.

Сценарій 1, OLSR і MP-OLSR для чотирьох шляхів.

У перший представлений сценарій включені шість вузлів. Розташування вузлів показано на (рис.4.15). Об'єкт тестування - багатоколійні алгоритм, тож спроба пошуку стільки шляхів, скільки можливо в цьому простому сценарії.

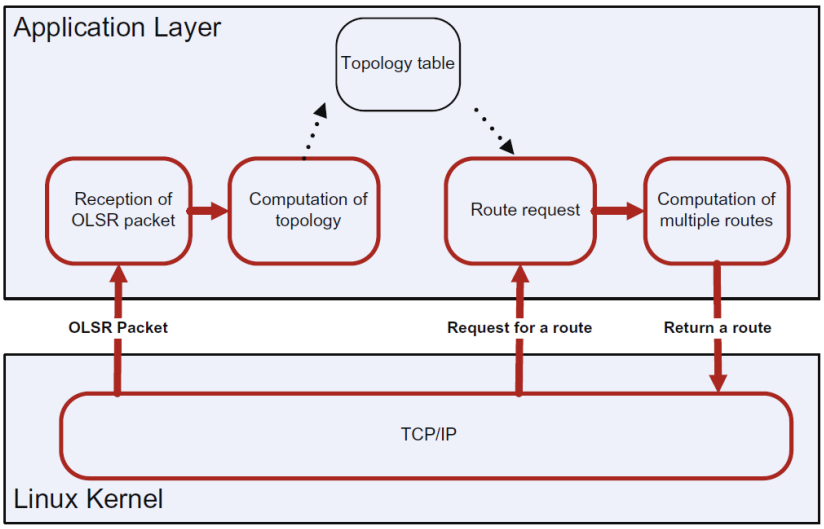


Рисунок 4.15 – Реалізація MP-OLSR на Linux

Кількість шляхів в MP-OLSR встановлено в 4. Вузол з IP адресою 10.0.0.100 обраний як джерело, а інший вузол з IP адресою 10.0.0.98 - як одержувач. Відстань між вузлом джерела і вузлом одержувача складає близько 60 метрів. У сценарії існують різні перешкоди: дерева, будови, рухомі машини між вузлами, які блокують певні зв'язки на випадковий проміжок часу. Правила IP таблиць (Iptable rules, firewall) використовується для блокування прямої передачі між джерелом і одержувачем для побудови багато-Скачкова сценарію. У наступних тестах швидкість передачі даних встановлена в 62KB / s для передачі файлу 17.8MB. Результати представлені в Додатку Б. Для MP-OLSR передача була завершена за 6 хвилин 12 секунд. Вузли з IP адресами 10.0.0.90, 10.0.0.95, 10.0.0.99 і 10.0.0.105 обрані як проміжні вузли для передачі пакетів. Протягом передачі було втрачено 9,9% пакетів. Для OLSR, використовувалися для передачі пакетів даних лише вузли 10.0.0.90 і 10.0.0.95. Зв'язок урвався через 5 хвилин 17 секунд передачі. Для відправлених пакетів втрати склали 37,53%. Для порівняння продуктивності цих двох протоколів також аналізується log file (файл журналу) програми Wireshark. Pic.4.17, 4.18 показують кількість відправлених пакетів на різні вузлів від джерела (10.0.0.100) до наступних вузлів за кожен тик (1 з на тик (робота моделі за один період умовного часу)), для MP-OLSR і OLSR відповідно.

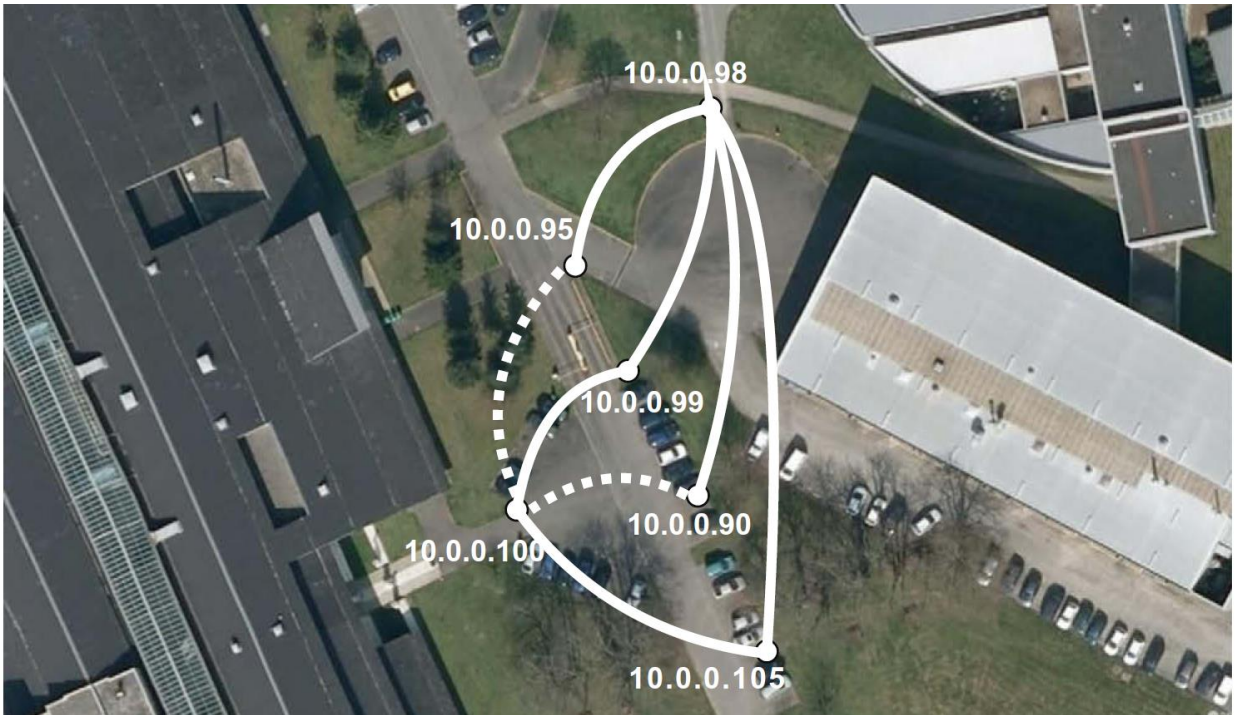


Рисунок 4.16 – Топологія мережі для сценарію 1. (Вузол з IP адресою 10.0.0.100 обраний як джерело, а вузол з IP адресою 10.0.0.98 - як одержувач)

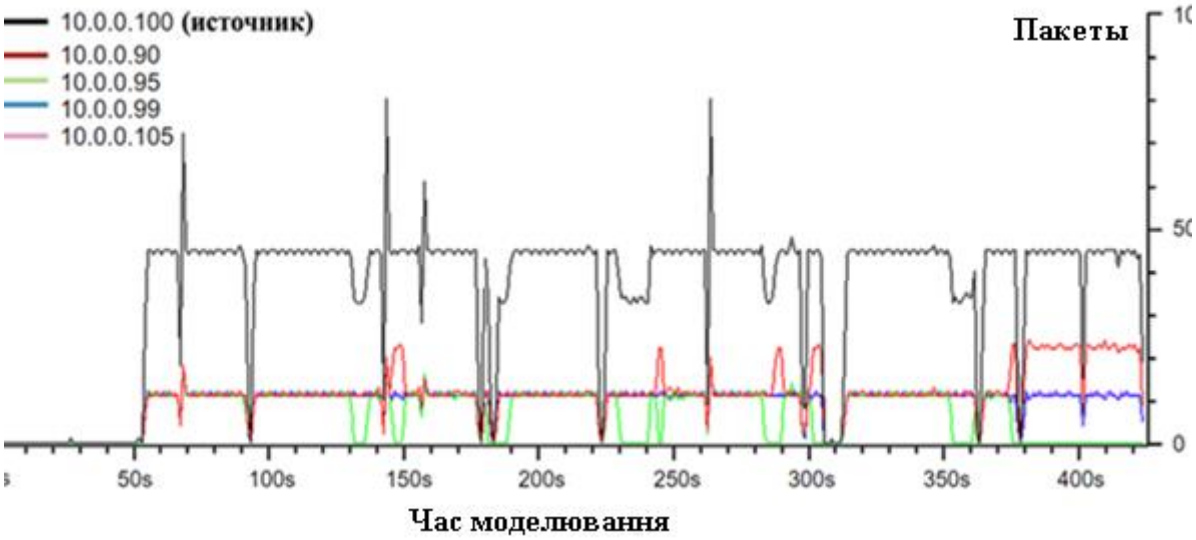


Рисунок 4.17 – Трасування Wireshark для сценарію 1

Як представлено на рис.4.17, для фіксованої швидкості джерела (10.0.0.100), навантаження розподіляється між чотирма шляхами. Передача практично послідовна навіть якщо деякі зв'язку недоступні. Якщо певний зв'язок розривається, трафік буде направлений на інші вузли (наприклад, з 290 с. По 300 с. І з 380 с. По 420 с.). У порівнянні з MP-OLSR, передача за допомогою OLSR

(рис.4.18) здійснюється тільки через один шлях (таким чином, швидкість залишається колишньою з одним і тим же шляхом і не відображається тут).

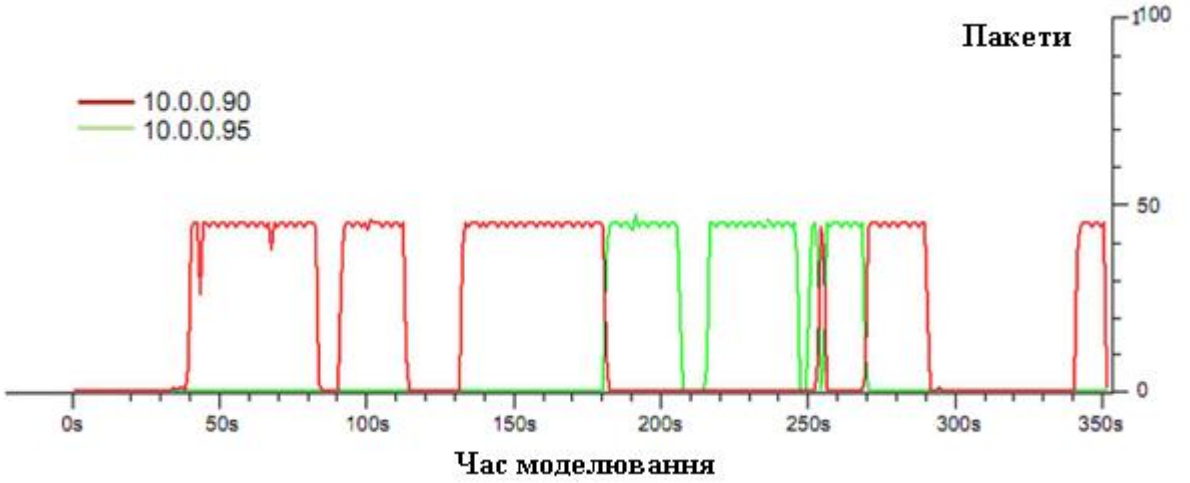


Рисунок 4.18 – Трасування Wireshark протоколу OLSR для сценарію 1

Передача переривається на короткий період тому, що доступний тільки один шлях. В цьому випадку вузол спробує знайти інший маршрут до точки призначення. Але передача даних буде зупинена протягом цього періоду

(Наприклад, з 80-90 с., 115-130 с. Рис.4.18). І цей тип перемикання маршрутів займає надто багато часу, з'єднання буде втрачено і в підсумку приведе до збою передачі файлу [13,15].

Сценарій 2: OLSR і MP-OLSR маршрутизація за трьома шляхами.

У другому сценарії порівнюється OLSR і MP-OLSR з трьома шляхами, які містять три або чотири стрибка (переходу). Задача полягає в тестуванні протоколу з більш довгими шляхами в складному сценарії. Розташування вузлів показано на рис.4.19. Відстань між джерелом і одержувачем становить приблизно 200 метрів. Між ними знаходиться велика будова. Для того, щоб досягти вузла призначення пакети повинні пройти навколо будови або пройти через хол цієї будівлі. Деякі зв'язку нестабільні, в основному на території парковки і всередині будівлі (рис.4.20). MP-OLSR використовує лише один або два шляхи. Однак, незважаючи на часті зміни топології передача успішна з протоколом MP-OLSR.

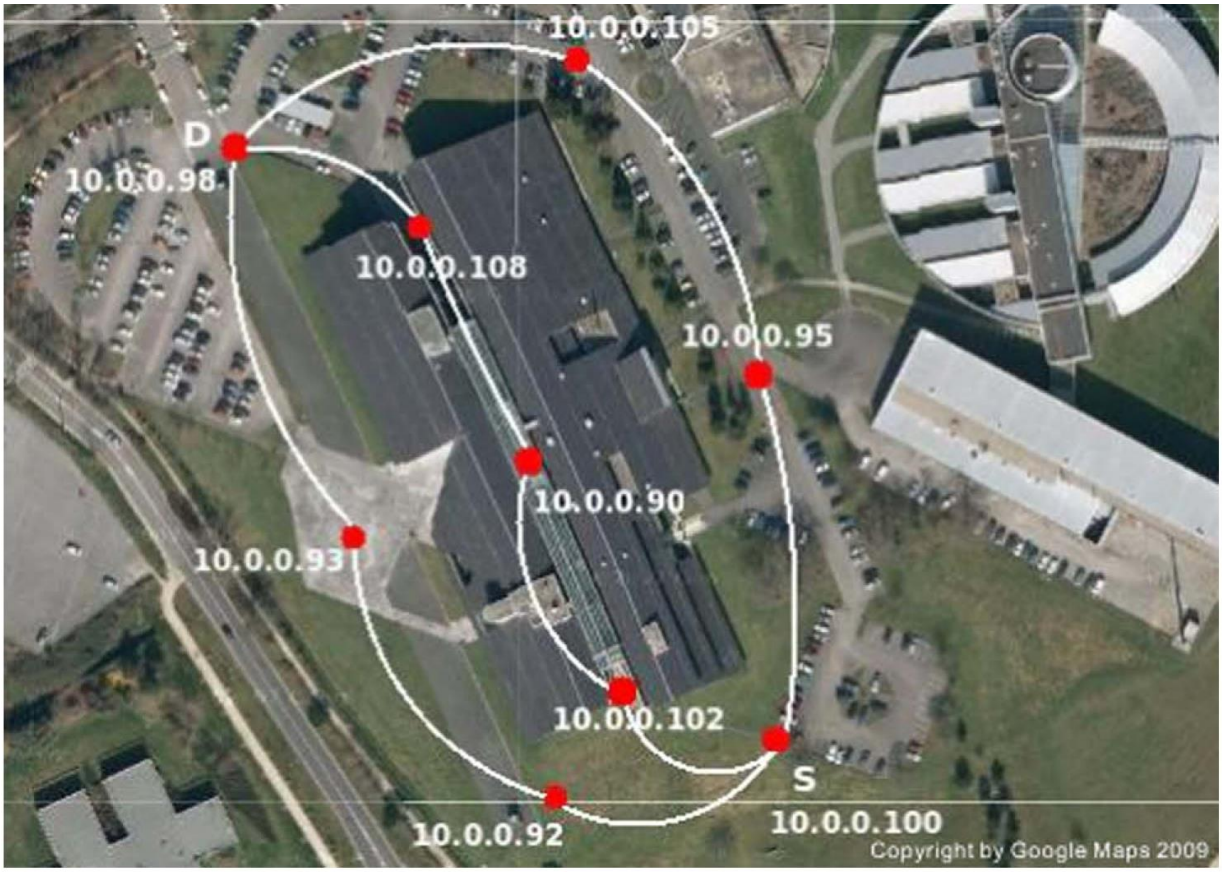


Рисунок 4.19 – Топологія мережі для сценарію 2

При використанні OLSR з'єднання UFTP зупиняється після передачі декількох пакетів. Це відбувається тому, що в порівнянні з багатоколійні в однопутевих протоколах маршрутизації нестабільні шляху призводять до більш негативного ефекту. Таким чином передача файлу обривається через time out`a.

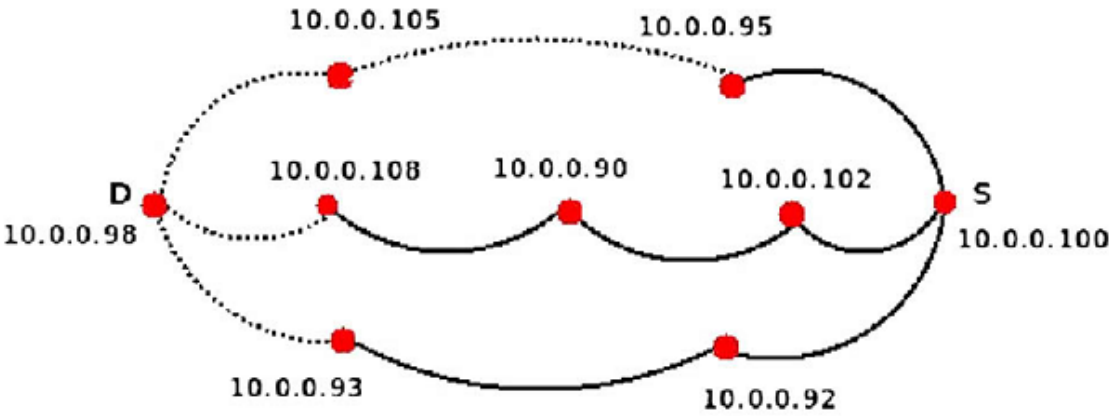


Рисунок 4.20 – Якість зв'язків в сценарії 2

Зроблені експерименти показують ефективність і здатність MP-OLSR працювати в реальних сценаріях [18-19]. UFTP узятий як приклад програми. Мобільний не береться до уваги в даному сценарії, але топологія мережі все таки змінюється через збої зв'язків.

При порівнянні результатів симулятора і реальної тестової моделі, виявляється, що мережева продуктивність в реальному сценарії не так хороша як на симуляторі, але має ту ж спрямованість. Це обґрунтовано тому, що в мережевий симуляції ми симулювали фізичний рівень як вільний простір використовуючи ідеальну математичну модель. В реальних умовах існує набагато більше факторів, які впливають на кінцевий результат: перешкоди, радіо відображення, характер і властивості простору навколишнього середовища, радіо впливу (від інших Wi-Fi пристроїв і так далі), а також вологість і температура. Проте, хоч і важко змоделювати точну реальну ситуацію, ми все таки змогли отримати відповідну гідну оцінку порівняння протоколів за результатами симуляції.

Через обмежених ресурсів дуже важко виконати тести в реальній ситуації з великою кількістю вузлів і такий мобільністю як на симуляторі (наприклад, десятки вузлів, що переміщаються по території в 1 км2). Як компроміс, виробляти тест продуктивності протоколів з реальним додатком UFTP в більш складному сценарії використовувалася напів-реалістичний стенд, засновані на інтерфейсі IPNE (IPNetwork Emulation) [20], як показано на рис.4.21. IPNE здійснює вставку і прийом пакетів (a packet sniffer / injector). Він ловить пакети з фізичного рівня мережі, посилає їх через симулятор Qualnet і вставляє їх назад в фізичну мережу. Віртуальна мережа Qualnet прозора для додатка UFTP. Запускалася передача UFTP на швидкості 100KB / s з тими ж внутрішніми налаштуваннями цього рівня. Там також був 81 вузол із середньою рухливістю (тобто максимальна швидкість 5 м / с). Записи Wireshark показані на (рис.4.17, 4.18) для OLSR і MP-OLSR відповідно. Такі ж тенденції відбувалися в тестах в реальній ситуації, передача файлу обривалася, використовуючи OLSR, за короткий період часу (170 с.).

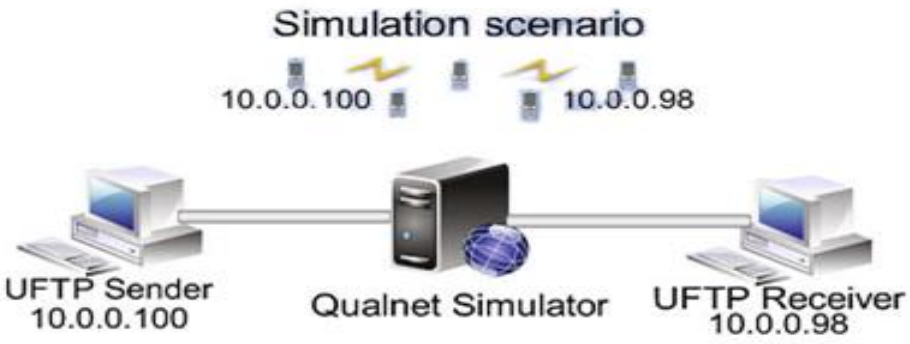


Рисунок 4.21 – Полуреалістіческая модель з UFTP додатком

А для MP-OLSR не дивлячись на те, що він використав не стабільні шляхи протягом цього періоду, файл благополучно досягав точки призначення.

Грунтуючись на результатах, отриманих на симуляторі і реальної моделі можна зробити висновок, що MP-OLSR може надати кращу продуктивність ніж OLSR особливо в жорстких сценаріях (висока мобільність в симуляції і часті збої зв'язків в реальній моделі). Це в основному завдяки тому, засноване на проактивному багатоколійні алгоритмі Дейкстри може знаходити відповідні множинні шляхи і розподіляти трафік за різними шляхами використовуючи маршрутизацію від джерела. А визначення «петель» і відновлення маршруту можуть ефективно усувати недоліки маршрутизації від джерела як можливі петлі в мережі.

ВИСНОВКИ

В кваліфікаційної магістерської роботі проведено дослідження протоколів багатошляхової маршрутизації в безпроводових мережах MANET.

Розглянуто принципи організації, основи функціонування та особливості маршрутизації в MANET мережах. Маршрутизація в AD-hoc мережах набагато складніше, ніж в провідних мережах, через динамічну топологію AD-hoc мереж. Проаналізовано три категорії протоколів багатошляхової маршрутизації: проактивних, реактивних і гібридних протоколів.

Сформульовані критерії для аналізу протоколів багатошляхової маршрутизації. Представлена класифікація протоколів та проведено аналіз протоколів багатошляхової маршрутизації. Для кожної категорії протоколів виконано аналіз продуктивності. Представлені характеристики протоколів всіх груп з точки зору забезпечуваної мережевої продуктивності. Показано, що з проактивних протоколів найкращу продуктивність має протокол OLSR.

Запропоновано використання багатошляхового алгоритму Дейкстри в протоколах багатошляхової маршрутизації для підвищення якості обслуговування в мережах MANET. Наведено результати моделювання, аналіз яких показав, що впровадження багатошляхового алгоритму Дейкстри дозволяє зменшити затримку в 4 рази.

Проведено порівняльний аналіз протоколу OLSR та його модифікації MP-OLSR. Наведено результати моделювання, аналіз яких показав, що відсоток доставки даних по протоколу OLSR трохи вище (близько 3%) відсотка доставлених пакетів по протоколу MP-OLSR лише на швидкості 1 м/с (3,6 км/год). Причина тому, зростання ймовірності виникнення колізій на MAC рівні, викликана збільшенням кількості шляхів одночасної передачі. Зі збільшенням швидкості протокол MP-OLSR демонструє кращі результати.

Зі швидкості 4 м/с (14,4 км/год) затримка OLSR в 4 рази більше, ніж MP-OLSR. Затримка з кінця в кінець» включає затримку поширення від відправника до одержувача та затримку в черзі в кожному транзитному вузлі. MP-OLSR може

мати більш тривалу затримку поширення тому, що деякі пакети направляються по більш довгим маршрутах. Як показав аналіз, MP-OLSR має значно менший час затримки в черзі в порівнянні з OLSR.

Результати кваліфікаційної магістерської роботи можуть бути використані в навчальному процесі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Clausen, P. Optimized Link State Routing Protocol OLSR [Текст] / P. Clausen, P. Jacquet // Request for Comments. – 2003. – № 3626. – С. 28.

2. Abolhasan, M. A review of routing protocols for mobile ad hoc networks [Текст] / M. Abolhasan, T. Wysocki // Ad Hoc Networks. – 2004. – № 2 (1). – С. 22.

3. Поповский, В. В. Многоканальная электросвязь и телекоммуникационные технологии [Текст] / В. В. Поповский, Ю. И. Лосев, С. А. Сабурова, В. С. Марчук.– Х. : СМИТ, 2006. – 596 с.

4. Samir R. Das, Charles E. Perkins, Elizabeth M. Performance comparison of two on-demand routing protocols for ad hoc networks [Текст] // Performance comparison. – 2000. – 85 с.

5. Johnson, D. B. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc
Networks for IPv4 [Текст] / D. B. Johnson, Y. Hu // Request for Comments. – 2007. – № 4728. – С. 18.

6. Perkins, C. In Workshop on Mobile Computing Systems and Applications [Текст] / C. Perkins, E. Royer // Ad-hoc on-demand distance vector routing. – 1999. – № 856. – С. 53.

7. Tarique, K. E. Survey of multipath routing protocols for mobile ad hoc networks [Текст] / K. E. Tarique // Journal of Network and Computer Applications. – 2009. – № 32 – С. 43.

8. Clausen, T. Jitter Considerations in Mobile Ad Hoc Networks [Текст] / T. Clausen, C. Dearlove // Request for Comments. – 2008. – № 5148. – С. 53.

9. Clausen, T. Generalized Mobile Ad Hoc Network (MANET) [Текст] / T. Clausen, C. Dearlove // Request for Comments. – 2009. – № 5444. – С. 28.

10. Clausen, T. Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs) [Текст] / T. Clausen, C. Dearlove // Request for Comments. – 2009. – № 5497. – С. 27.

11. Clausen, T. MANETNeighborhood Discovery Protocol (NHDP), draft-ietf-manet-nhdp-10 [Текст] / T. Clausen, C. Dearlove // Internet Draft. – 2009. – № 659. – С. 64.

12. L. Melnikova, E. Linnyk, D. Ageyev, O. Melnikova, N. Kryvoshapka and V. Barsuk, "Minimizing the Route of Sink Node in Wireless Sensor Network," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 861-864, doi: 10.1109/PICST47496.2019.9061563.

13. Мельнікова Л.І., Лінник О.В.,Кривошапка М.В.,Барсук В.О. Оптимизация маршрута мобильного стока в беспроводной сенсорной сети // Проблеми телекомунікацій. - №1(24). - 2019. - С. 104-112.

14. Кривошапка Н.В., Барсук В.О. Пошук оптимального маршруту мобільного стоку в безпроводовій сенсорній мережі за допомогою генетичного алгоритму// Матеріали шостої Міжнародної науково-технічної конференції "Информатика, управление и искусственный интеллект (ИУИИ-2019)», - Харків, НТУ "ХПИ". – 2019. – С. 37-38.

15. Clausen, T. The Optimized Link State Routing Protocol Version 2 [Текст] / T. Clausen, C. Dearlove // Internet Draft. – 2009. – № 2144. – С. 37.

16. Marina, M. K. On-demand multi path distance vector routing in ad hoc networks in: Proceedings of the Ninth International Conference on Network Protocols [Текст] / M. K. Marina, S. R. Das // Computer Society. – 2001. – № 62. С. 23.

17. Lee, S. Split multipath routing with maximally disjoint paths in ad hoc networks [Текст] / S. Lee, M. Gerla // Helsinki. – 2001. – № 632. – С. 49.

18. Yao, Z. A neighbor table based multipath routing in ad hoc networks [Текст] / Z. Yao // Semi Annual Vehicular Technology Conference : науч. – техн. сб. – NY. : Technology, 2003. – Вып. 57. – С. 1739 – 1743.

19. Cizeron, E. A multiple description coding strategy for multi-path in mobile ad hoc networks [Текст] / E. Cizeron, S. Hamma // the Latest Advances in Networks (ICLAN). – 2007. – № 14. – С. 28.

20. Zhou, X. A novel routing protocol for ad hoc sensor networks using multiple disjoint paths [Текст] / X. Zhou, Y. Lu // International on Broadband Networks. – 2005. – № 2. – С. 64.

21. А. С. Бухаров, В. А. Барсук, Н. В. Кривошапка. Использование многокритериального подхода к оптимизации ТКС. XXIV международный молодёжный форум «Радиоэлектроника и молодежь в XXI веке». – 2020. – №10. – С. 47–48.

22. Stepanov, I. On the impact of a more realistic physical layer on manet simulations results [Текст] / I. Stepanov, K. Rothermel // Ad Hoc Networks. – 2008. – № 4. – С. 61.

23. Maltz, D. Lessons from a full-scale multihop wireless ad hoc network testbed [Текст] / D. Maltz, J. Broch // Personal Communications. – 2001. – № 8. – С. 15.

24. Maltz, D. Olsrd, an adhoc wireless mesh routing daemon [Электронный ресурс] / D. Maltz. – Режим доступа: http: //www.olsr.org/. – 30.05.2011.

25. Md. Anisur Rahman, Md. Shohidul Islam, Alex Talevski, Performance Measurement of Various Routing Protocols in Ad-hoc Network [Текст] / Md. Anisur Rahman, Md. Shohidul Islam, Alex Talevski // Proceedings of the International Multi Conference of Engineers and Computer Scientists. – 2009

26. P.K.Manohari,N. K. Ray, EAOMDV: An Energy Efficient Multipath Routing Protocol for MANET / P.K.Manohari,N. K. Ray // In IEEE Power, Communication and Information Technology Conference (PCITC) . – 2015.

27. R.Sharma,T.Sharma,A.Kalia, A Comparative Review on Routing Protocols in MANET / R.Sharma,T.Sharma,A.Kalia // International Journal of Computer Applications. – 2016. – №1 – С. 33-38