МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ КОМ'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____Савченко А.С.
"____"_____2020 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"МАГІСТРА"

ЗА СПЕЦІАЛІЗАЦІЄЮ "ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ (ЗА ГАЛУЗЯМИ)"

Тема: "Мобільна Ad Hoc мережа з випадковим множинним доступом (система управління якістю сервісу)"

Виконав: *Сурядов Богдан Ігорович*.

Керівник: професор *Віноградов Микола Анатолійович*.

Нормоконтролер: Райчев І.Е.

Київ - 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра Комп'ютерних інформаційних технологій

Галузь знань, спеціальність, спеціалізація: 12 "Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології (за галузями)"

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____Савченко А.С.

«____»_____2020р.

ЗАВДАННЯ

на виконання дипломної роботи студента

Сурядова Богдана Ігоровича
(прізвище, ім'я, по батькові)

1. **Тема роботи:** «Мобільна Ad Hoc мережа з випадковим множинним доступом (система управління якістю сервісу)» затверджена наказом ректора від 02.10.2020 за № "1891/ст".
2. **Термін виконання роботи:** з 05.10.2020 до 31.12.2020
3. **Вихідні данні до роботи:** теоретичні відомості та норми проектування бездротових мереж без інфраструктури, інформація про сучасні бездротові мережі, документація щодо середовищ розробки складної мережевої інфраструктури, вимоги до майбутньої бездротової мережі з випадковим множинним доступом.
4. **Зміст пояснювальної записки:** вступ, загальний огляд бездротових мереж без інфраструктури, аналіз протоколів маршрутизації, огляд наскрізного контролю якості сервісу, аналіз методології контролю якості, розрахунок критеріїв якості сервісу, модель якості сервісу бездротової мережі без інфраструктури, висновки.

5. Перелік обов'язкового ілюстративного матеріалу: діаграми та схеми технологій мережевих інфраструктурних рішень, таблиці, рисунки, графіки.

6. Календарний план-графік

№ п/п	Завдання	Термін виконання	Підпис керівника
1.	Отримання завдання на дипломну роботу. Розробка календарного плану.	05.10.2020–10.10.2020	
2.	Аналіз літературних джерел за темою дипломного проекту.	11.10.2020–25.10.2020	
3.	Аналіз протоколів маршрутизації та якості сервісу у MANET.	25.10.2020–27.10.2020	
4.	Постановка задачі контролю якості сервісу у MANET.	28.10.2020–02.10.2020	
5.	Ознайомлення зв функціональними можливостями MATLAB та NS-3.	03.10.2020–06.11.2020	
6.	Проведення математичних розрахунків якості сервісу .	07.11.2020–15.11.2020	
7.	Моделювання контролю якості сервісу за допомогою заданого алгоритму маршрутизації.	15.11.2020–30.11.2020	
8.	Висновки та оформлення пояснювальної записки дипломного проекту.	01.12.2020–14.12.2020	
9.	Підготовка до захисту дипломного проекту.	15.12.2020–20.12.2020	

7. Дата видачі завдання: «05» жовтня 2020р.

Керівник дипломного проекту Віноградов М.А.

Завдання прийняв до виконання Сурядов Б.І.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи “Мобільна Ad Hoc мережа з випадковим множинним доступом (система управління якістю сервісу)” складається із вступу, трьох розділів, загальних висновків, списку використаних джерел і містить 84 сторінки, 14 рисунків, 8 бібліографічних посилань та один додаток, що містить 12 сторінок.

Метою дипломної роботи є застосування теоретичних і практичних засад для моделювання бездротової мережі з випадковим множинним доступом, вирішення задач топології та управління якістю сервісу.

Предметом дослідження модель бездротової системи з випадковим множинним доступом побудованої на базі сучасного безкоштовного дослідницького програмного забезпечення NS-3 Network Simulator та пакету прикладних програм для числового аналізу MATLAB.

Об’єктом дослідження безпосередньо є якість сервісу у мобільних мережах без інфраструктури з випадковим множинним доступом.

В дипломній роботі подано і охарактеризовано модель перевірки бездротової мережі без інфраструктури на предмет якості сервісу за триплетом критеріїв.

Розроблена в дипломній роботі модель контролю якістю сервісу у бездротових мережах з випадковим множинним доступом надає можливість перевірити надійність та якість мережі відповідно до характеристик обраного протоколу маршрутизації.

Ключові слова: БЕЗДРОТОВА МЕРЕЖА, MANET, ЯКІСТЬ СЕРВІСУ, ПРОТОКОЛ МАРШРУТИЗАЦІЇ, QOS, ІНСТРУМЕНТИ, ОПТИМАЛЬНІСТЬ, НАДІЙНІСТЬ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ 7

ВСТУП 8

РОЗДІЛ 1 10

ХАРАКТЕРИСТИКИ БЕЗДРОТОВИХ МЕРЕЖ БЕЗ ІНФРАСТРУКТУРИ 10

1.1 Загальний огляд MANET 10

1.2 Характеристики MANET 11

1.2.1 Застосування MANET 14

1.2.2 Мобільна маршрутизація IP-рівня 15

1.2.3 Взаємодія зі стандартною IP-маршрутизацією 17

1.3 Типи MANET 23

1.4 Аналіз протоколів маршрутизації у MANET 24

1.4.1 Проактивні протоколи маршрутизації 26

1.4.2 Реактивні протоколи маршрутизації 28

1.4.3 Гібридні протоколи маршрутизації 29

ВИСНОВКИ ДО РОЗДІЛУ 1 30

РОЗДІЛ 2 31

ЯКІСТЬ СЕРВІСУ QOS У БЕЗДРОТОВИХ МЕРЕЖАХ БЕЗ ІНФРАСТРУКТУРИ 31

2.1 Стисла історія QoS 31

2.1.1 Основи та концепції QoS 32

2.1.2 Моделі QoS: IntServ та DiffServ 32

2.2 Аналіз якості сервісу у MANET 35

2.2.1 Обробка пакетів в ad hoc мережах 36

2.2.2 Характеристики MANET з позиції QoS 39
2.2.3 Виклики проектування MANET 41
2.2.4 Маршрутизація у MANET з точки зору QoS 42
2.2.4.1 Реактивні протоколи маршрутизації 44
ВИСНОВКИ ДО РОЗДІЛУ 2 47
РОЗДІЛ 3 48
РОЗРОБКА МЕТОДУ ПОШУКУ ОПТИМАЛЬНОГО МАРШРУТУ ІЗ ЗАБЕЗПЕЧЕННЯМ НАСКІЗНОЇ ЯКОСТІ СЕРВІСУ 48
3.1 Розрахунок компромісу між надійністю, затримкою та пропусною здатністю у бездротових мережах з випадковим множинним доступом 47
3.1.1 Огляд моделі мережі 51
3.1.2 Розрахунок меж компромісу між характеристиками якості 53
3.1.3 Приклад компромісу між характеристиками якості 58
3.2 Розробка моделі MANET з оптимальним маршрутом доставки 61
3.2.1 Інтеграція методів QoS та протоколу маршрутизації AODV 62
3.2.2 Алгоритм MAODV-BER 63
3.2.3 Параметри моделі MANET 65
3.2.3 Моделювання та результати 66
ВИСНОВКИ ДО РОЗДІЛУ 3 70
ВИСНОВКИ 71
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ 72
ДОДАТОК А 73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

MANET – Mobile Ad hoc NETwork – бездротова децентралізована IP мережа

Маршрутизація – процес визначення маршруту прямування інформації у мережі

End-to-end – спосіб передачі даних, в якому тільки користувачі, що беруть участь в спілкуванні, мають доступ до інформації

Peer-to-peer – варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів

IP – Internet Protocol – протокол мережевого рівня для передавання датаграм меж мережами

TCP – протокол управління передачею даних у комп'ютерних мережах

TTL – максимальний період часу або кількість ітерацій або переходів, за який набір даних (пакет) може існувати до свого зникнення

LTE – мобільний протокол передавання даних

QOS – Quality of Service – набір методів для управління ресурсами пакетних мереж

AODV – протокол динамічної маршрутизації для мобільних ad-hoc мереж та інших бездротових мереж

BER – частота бітових помилок

ВСТУП

З розвитком мережевих технологій потреба у бездротових мережах постійно зростає. Питання надання якісного сервісу залишається відкритим уже багато років і особливо гостро воно постає у проектуванні мереж з мобільними топологіями. Не дивлячись на свою гнучкість, такі мережі мають ряд недоліків та складностей у їх проектуванні.

Мобільні ad hoc мережі (MANET) складаються з особливого типу бездротових мобільних вузлів, які утворюють тимчасову мережу без використання будь-якої інфраструктури або централізованого адміністрування. MANET можна використовувати в широкому діапазоні майбутніх додатків, оскільки вони мають можливість встановлювати мережі в будь-який час і в будь-якому місці без допомоги будь-якої встановленої інфраструктури.

Питання пошуку оптимального маршруту у мережах з настільки гнучкою топологією стоїть дуже гостро. Для поліпшення вирішення цієї проблеми можуть бути застосовані методології контролю якості сервісу, що мають на увазі набір методів управління ресурсами пакетних мереж. Особливо цікавим у контексті даної проблеми є триплет якості сервісу пропускна спроможність – затримка – рівень бітових помилок.

Принципова неможливість своєчасного (в ідеалі – миттєвого) збору та опрацювання повної апріорної інформації про параметри та стан мережі. Навіть коли б ми мали повну інформацію про параметри та стан кожного мережного та термінального вузла – ми принципово не можемо мати інформацію про активність мережних абонентів – коли увійшов у мережу, коли зробив запит на з'єднання з тим чи іншим мережним вузлом; яка миттєва та усереднена інтенсивність запитів впродовж сеансу; коли завершив з'єднання, коли вийшов з мережі тощо. Більш того, ми не маємо інформації навіть про миттєву кількість абонентів у мережі.Таким чином, для аналізу та оптимізації характеристик бездротових мереж без інфраструктури необхідно застосовувати методи теорії імовірностей та математичної статистики

У ході виконання дипломної роботі буде оброблено значну кількість наукового матеріалу, охарактеризовано основні сильні та слабкі сторони мобільних мереж без інфраструктури, категоризовано протоколи маршрутизації таких мереж. Буде розглянуто питання маршрутизації у контексті контролю якістю сервісу.

Однією з головних цілей є розробка моделі бездротової мережі без інфраструктури MANET та дослідження контролю якості за триплетом якості сервісу пропускна спроможність – затримка – рівень бітових помилок. Моделювання бездротової мережі MANET на базі наукового програмного забезпечення NS-3 та аналіз алгоритми пошуку оптимального шляху також є важливими компонентами роботи.

РОЗДІЛ 1. ХАРАКТЕРИСТИКИ БЕЗДРОТОВИХ МЕРЕЖ БЕЗ ІНФРАСТРУКТУРИ

1.1 Загальний огляд MANET

З останніми досягненнями продуктивності в роботі бездротового зв'язку та комунікаційних технології, передові мобільні бездротові обчислення очікують все більшого і більшого розповсюдження і застосування, більшість із яких передбачає використання Інтернет-протоколу (IP). Бачення мобільних спеціальних мереж полягає у підтримці надійної та ефективної роботи мобільних бездротових мереж шляхом включення маршрутизаційної функціональності у мобільних вузлах. Такі мережі мають динамічні, часом швидко мінливі, випадкові багатоточкові топології які, ймовірно, складатимуться з бездротових зв'язків обмеженої пропускної здатності.

MANET розшифровується як Mobile adhoc Network, яку також називають бездротовою ad hoc мережею або ad hoc бездротовою мережею, яка зазвичай має маршрутизоване мережеве середовище поверх спеціальної мережі Link Layer. Вони складаються з безлічі мобільних вузлів, підключених бездротовим способом до самоконфігурованої самовідновлювальної мережі не маючи фіксованої інфраструктури. Вузли MANET можуть вільно переміщуватися у випадковому порядку, оскільки топологія мережі часто змінюється. Кожен вузол поводиться як маршрутизатор, коли вони перенаправляють трафік на інший вказаний вузол у мережі.

В рамках Інтернет-спільноти підтримка маршрутизації для мобільних хостів в даний час формулюється як технологія "мобільного IP". Це технологія підтримки кочового хоста "в роумінгу", де роумінг хости можуть бути підключені різними способами до Інтернету, крім його добре відомого доменного простору з фіксованою адресою. Господар може бути безпосередньо фізично підключений до фіксованої мережі

Метою мобільних мереж ad hoc є розширення мобільності в області автономних, мобільних, бездротових доменів, де набір з вузлів - які можуть бути комбінованими маршрутизаторами та хостами - самі утворюють інфраструктуру маршрутизації мережі в режимі ad hoc.

1.2 Характеристики MANET

MANET складається з мобільних платформ (наприклад, маршрутизатора з декількома хостами та пристроїв бездротового зв'язку) - надалі просто "вузли", які вільні переміщуються довільно. Вузли можуть розташовуватися в літаках, кораблях, вантажних автомобілях, автомобілях або навіть на людях або дуже маленьких пристроях, і можуть мати кілька хостів на маршрутизатор. MANET - це автономна система мобільних вузлів. Система може працювати ізольовано, або може мати шлюзи до та з ними взаємодіяти у фіксованій мережі. В останньому режимі роботи це зазвичай передбачається як "заглушена" мережа, що підключається до фіксованої робота в Інтернеті. Заглушені мережі несуть трафік, що надходить з та / або призначені для внутрішніх вузлів, але не дозволяють екзогенного трафіку "транзит" через тупикову мережу. Вузли MANET оснащені бездротовими передавачами та приймачами використовуючи антени, які можуть бути всеспрямованими (широкомовними), високо спрямований (точка-точка), можливо керований, або комбінація цього.

В даний момент часу, залежно від положення вузлів та їх схеми покриття передавача та приймача, передачі рівнів потужності та рівнів перешкод спільного каналу, бездротова мережа підключення у вигляді випадкового багатогранного графіку або ad hoc мережа існує між вузлами. Ця спеціальна топологія може змінюватися з часом, коли вузли рухаються або регулюють свою передачу і параметри прийому. MANET мають кілька основних характеристик:

1. Динамічні топології: Вузли можуть вільно переміщуватися довільно; таким чином, топологія мережі - яка, як правило, мультишоп - може змінитися випадково і швидко в непередбачуваний час, і може складатися з як двонаправленого, так і односпрямованого зв’язку.
2. Зв'язок з обмеженою пропускною здатністю, змінна пропускна здатність: бездротові зв’язки матимуть значно меншу потужність, ніж їхні жорсткі дроти. Крім того, реалізована пропускна здатність бездротового зв'язоку - після обліку наслідків умови багаторазового доступу, вицвітання, шуму та перешкод, тощо - часто набагато менше максимальної швидкості передачі радіо. Одним з ефектів відносно низької та помірної пропускної здатності є те, що затори зазвичай є нормою, а не винятком, тобто сукупний попит на програми, швидше за все, наблизиться або перевищить ємність мережі. Оскільки мобільна мережа часто просто розширення інфраструктури фіксованої мережі, користувачі мобільної мережі ad hoc вимагатимуть подібних послуг. Ці вимоги будуть і надалі збільшуються в міру зростання обчислень у мультимедіа та спільних мереж додатків.
3. Енергообмежена: деякі або всі вузли в MANET можуть покладатися на батареї або інші вичерпні засоби енергія. Для цих вузлів найважливішим критерієм проектування системи для оптимізації може бути енергозбереження.
4. Обмежена фізична безпека: мобільні бездротові мережі є як правило, більш схильні до фізичних загроз безпеці, ніж кабельні сітки. Підвищена можливість прослуховування, підробки, та атаки на відмову в обслуговуванні слід ретельно розглянути. Існуючі методи захисту посилань часто застосовуються всередині бездротові мережі для зменшення загроз безпеці.

Як перевага децентралізований характер управління мережею в MANET забезпечує додаткову надійність проти окремих точок відмови, ніж більш централізовані підходи. Крім того, деякі передбачені мережі (наприклад, мобільні військові мережі або шосейних мереж) можуть бути відносно великим (наприклад, десятки або сотні вузлів

на область маршрутизації). Потреба в масштабованості не є унікальною до MANET. Однак у світлі попередніх характеристик механізми, необхідні для досягнення масштабованості. Ці характеристики створюють набір основних припущень і проблеми ефективності проектування протоколів, які виходять за рамки керуючих дизайном маршрутизації в межах більш швидкісних, напівстатичних топологій фіксованого Інтернету.

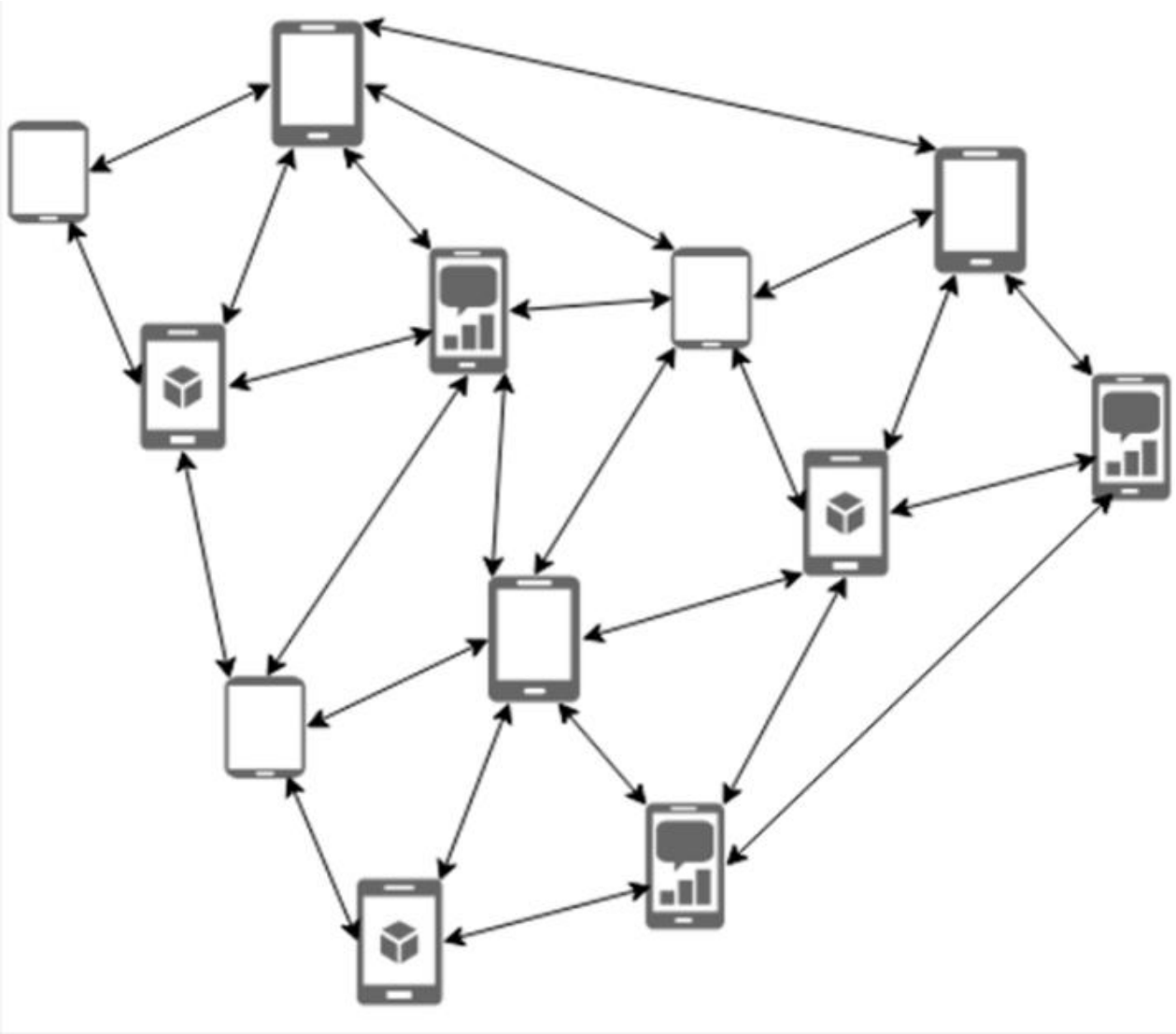

Рис 1.1. Приклад топології MANET

1.2.1 Застосування MANET

Технологія мобільних ad hoc мереж є дещо синонімічною з мобільною пакетною радіомережею (термін, придуманий протягом раннього періоду військові дослідження в 70-80-ті роки), Mobile Mesh Networking (а термін, який з'явився у статті в The Economist стосовно структури майбутніх військових мереж) та Mobile, Multihop, Wireless Network (можливо, найточніший термін, хоча і трохи громіздкий). Існує поточна та майбутня потреба в динамічних ad hoc мережевих технологій. Нова сфера мобільних і кочових обчислень, с поточним акцентом на роботі мобільної IP повинен поступово розширюватися і вимагає високоадаптивної технології мобільних мереж, щоб ефективно управляти мультишопними, ad hoc мережевими кластерами, які можуть працювати автономно або, що, швидше за все, бути приєднаним до деяких пунктів (и) до фіксованого Інтернету. Деякі програми технології MANET можуть включати промислові та комерційні програми, що передбачають спільний обмін мобільними даними. Крім того, мобільні мережі на основі сітки можуть працювати як надійні, недорогі альтернативи або вдосконалення стільникової мобільної мережевої інфраструктури. Існують також існуючі та майбутні військові вимоги до мережі для надійних служб передачі даних, сумісних з мобільними мережами IP бездротового зв'язку - багато з цих мереж складаються з високодинамічних сегментів автономної топології. Крім того, розробка технологій носимих обчислень та зв'язку може надавати програми для технології MANET. При правильному поєднанні за допомогою супутникової доставки інформації технологія MANET може забезпечити надзвичайно гнучкий метод встановлення комунікацій для пожежних / безпекових / рятувальних операцій або інших необхідних сценаріїв швидкого розгортання комунікації з виживною, ефективною динамікою створення мереж. Ймовірно, існують інші додатки для технології MANET які в даний час не реалізовані та не передбачені авторами. Це простіше кажучи, вдосконалена мережева технологія на основі IP для динамічних,

автономних бездротових мереж. MANET можуть застосовуватися у таких середовищах:

- Поле бою. Спеціальна мережа погодиться на те, щоб військові отримали переваги звичайних мережевих технологій, щоб утримувати інформаційну мережу між солдатами, транспортними засобами та головним кварталом військової інформації.
- Коворкінг. Для різних бізнес-середовищ потреба у загальних обчисленнях може бути важливішою за межами офісного середовища, ніж усередині, і там, де людям потрібно проводити зовнішні наради, щоб допомогати обмінятися інформацією щодо даного проекту .
- Локальний рівень. Ad hoc мережі можуть окремо пов'язувати миттєву та короткострокову мультимедійну мережу, використовуючи портативні комп'ютери, щоб поширювати та обмінюватися інформацією з учасниками. Наприклад, конференція або клас.
- Персональні та блютус мережі. Персональна мережа - це невеликий діапазон, локалізована мережуві вузли тут, як правило, пов'язані з певною людиною. MANET короткого діапазону, такий як Bluetooth.
- Комерційний сектор. Ad hoc може бути використана в операціях з невідкладною ситуацією для допомоги у разі катастрофи, наприклад, при пожежі, повені чи землетрусі. Аварійно-рятувальні операції повинні зайняти положення, де необхідна неіснуюча або поранена комунікаційна інфраструктура та швидке розгортання комунікаційної мережі

1.2.2 Мобільна маршрутизація IP-рівня

Покращена здатність мобільної маршрутизації на рівні IP може забезпечити вигоду, подібне до наміру оригінального Інтернету, а саме взаємодіючі можливості роботи в мережі Інтернет через неоднорідну мережеву інфраструктура. У цьому

випадку інфраструктура є бездротовою, а не провідною, що складається з декількох бездротових технології, протоколи доступу до каналу тощо. Покращена маршрутизація IP та відповідні мережеві послуги забезпечують зв’язок для збереження цілісності сегменту мобільної мережі в цьому більш динамічному навколишньому середовищі. Іншими словами, реальна вигода від використання маршрутизації на рівні IP у MANET полягає у забезпеченні узгодженості мережевого рівня для мереж multihop, що складається з вузлів із використанням комбінаціх середовища фізичного рівня, тобто комбінацією того, що прийнято вважати технологією підмереж. Вузол MANET в основному складається з маршрутизатора, який може бути фізично підключений до декількох IP-хостів (або пристроїв, що адресуються IP-адресами), який має потенційно кілька бездротових інтерфейсів - кожен інтерфейс використовує а різні бездротові технології. Таким чином, вузол MANET з інтерфейсами використовуючими технології A і B, можна спілкуватися з будь-яким іншим вузлом MANET що володіє інтерфейсом з технологією A або B. Multihop зв'язок технології A утворює багатошаровий фізичний рівень топології, багатопрофільний зв'язок технології B утворює іншу топологію фізичного рівня (яка може відрізнятися від топології A), і об'єднання цих топологій утворює іншу топологію (на графіку теоретичні терміни - мультиграф), що називається "тканиною маршрутизації IP" MANET. Вузли MANET приймають рішення про маршрутизацію з використанням IP-тканини можуть взаємодіяти, використовуючи одну або обидві топології фізичного рівня одночасно. У міру розробки нових технологій фізичного рівня, нові драйвери пристроїв можна писати і на іншому багатошаровому фізичному рівні, топологію можна легко додавати до тканини IP. Так само, від старших технологій можна легко відмовитись. Така функціональність і архітектурна гнучкість, яку може підтримувати маршрутизація на рівні IP, яка приносить із собою апаратну економію на масштабі.

Поняття "ідентифікатор вузла" (окремо та окремо від поняття "ідентифікатор інтерфейсу") має вирішальне значення для підтримки мультиграфної топології тканини маршрутизації. Це те, що об'єднує набір бездротових інтерфейсів і визначає їх як такі,

що належать до однієї мобільної платформи. Цей підхід дозволяє максимальну гнучкість в присвоєнні адреси. Ідентифікатори вузлів використовуються на рівні IP для обчислення маршрутизації.

1.2.3 Взаємодія зі стандартною IP-маршрутизацією

В найближчій перспективі передбачається, що MANET буде функціонувати як мережі заглушки, тобто весь трафік, що здійснюється через вузли MANET будуть або джерелами, або потоками в MANET. Через пропускну здатність та, можливо, обмеження потужності, MANET не передбачає функціонувати як транзитні мережі, що несуть трафік, який надходить і виходить з MANET (хоча це обмеження можуть бути усунені шляхом подальшого розвитку технологій). Це істотно зменшує кількість рекламних маршрутів, необхідних для взаємодії з існуючим фіксованим Інтернетом. Для роботи на заглушці, сумісність маршрутизації досягається за допомогою деякого поєднання таких механізмів, як anycast на базі MANET та мобільного IP. Майбутньої сумісності можна досягти, використовуючи інші механізми, ніж мобільний IP. Взаємодія зі стандартною IP-маршрутизацією значно полегшить використання загального підходу до адресації MANET усіма маршрутизаційними MANET протоколами. Триває розробка такого підходу, який дозволить маршрутизацію через мультитехнологічну тканину, кілька хостів на маршрутизаторі та забезпечить довгострокову сумісність завдяки дотриманню архітектури IP-адресації. З'являється підтримка цих функцій лише вимагати ідентифікації інтерфейсів хоста та маршрутизатора з IP адреси, ідентифікуючи маршрутизатор з окремим ідентифікатором маршрутизатора, та дозволяє маршрутизаторам мати безліч дротових та бездротових інтерфейсів.

1.2.4 Питання продуктивності протоколу маршрутизації MANET

Щоб судити про гідність протоколу маршрутизації, потрібні дві метрики: якісні та кількісні - за допомогою яких вимірюють його придатність та продуктивність. Ці показники повинні бути незалежними від будь-яких даних протоколу маршрутизації. Далі наведено перелік бажаних якісних властивостей MANET протоколи маршрутизації:

1. Розподілена операція: це стала властивість, але це все ж слід зазначити.
2. Свобода циклу: Не вимагається як така у світлі певних кількісних показників (тобто критеріїв ефективності), але загалом бажано уникати таких проблем, як найгірші випадки, напр. невелика частка пакетів обертається в мережі довільні періоди часу. Ad hoc технології, такі як TTL, але більш структурований та сформований підхід загалом бажаний, оскільки це, як правило, призводить до кращого загального результату продуктивність.
3. Операція на основі попиту: Замість того, щоб припускати рівномірний трафік розподілений усередині мережі (і підтримка маршрутизації між усіма вузлами в будь-який час), нехай алгоритм маршрутизації адаптується до схеми руху на основі попиту чи потреби. Якщо це зроблено розумно, він може використовувати енергію мережі та пропускну здатність ресурсів ефективніше, за рахунок збільшення затримки.
4. Проактивна робота: зворотна сторона операції на основі попиту. У певному контексті додаткова затримка на основі попиту може бути неприйнятним. Якщо пропускна здатність та енергетичні ресурси дозволяють, у цих контекстах бажані проактивні операції.
5. Безпека: Без певної форми рівня мережі або рівня зв'язку безпеки, протокол маршрутизації MANET вразливий до багатьох форм нападу. Можливо, досить просто підглянути мережевий трафік, відтворювати передачі, маніпулювати заголовками пакетів і перенаправляти маршрутизацію повідомлень у бездротовій мережі без належного положення про безпеку. Хоча ці занепокоєння існують у дротовій мережі інфраструктури та протоколи

маршрутизації, підтримуючи фізичну безпеку носію передачі важче на практиці з MANET. Достатній захист безпеки для заборони бажане порушення модифікації роботи протоколу. Це може бути дещо ортогональною до будь-якого конкретного протоколу маршрутизації підхід, напр. завдяки застосуванню методів захисту IP.

6. Експлуатація періоду "сну": в результаті економії енергії, або якоїсь іншої потреби бути неактивними, вузли MANET можуть зупинити передачу та / або прийом (навіть отримання вимагає живлення) на довільні періоди часу. Протокол маршрутизації повинен мати можливість забезпечити такі періоди сну без надто несприятливих наслідків. Для цієї властивості може знадобитися тісний зв'язок з протоколом рівня зв'язку через стандартизований інтерфейс.
7. Підтримка односпрямованих зв’язків: Двонаправлені посилання зазвичай є передбаченими при розробці алгоритмів маршрутизації та багатьох алгоритмів не здатних нормально функціонувати за односпрямованими зв’язком. Тим не менше, односпрямовані зв’язки можуть і мають місце в бездротовій мережі мереж. Часто існує достатня кількість дуплексних зв’язків що використання односпрямованих зв’язків має обмежену додану вартість. Однак у ситуаціях, коли пара односпрямованих зв’язків (в протилежні напрямки) утворюють єдиний двонаправлений зв’язок між двома спеціальними регіонами можливість їх використання є цінною.

Далі наведено перелік кількісних показників, до якими можна скористатися для оцінки роботи будь-якого протоколу маршрутизації.

1. Наскрізна пропускна здатність даних та затримка: статистичні показники продуктивності маршрутизації даних (наприклад, засоби, відхилення, розподіл) важливі. Це заходи політики маршрутизації ефективність - наскільки добре вона виконує свою роботу - як вимірюється з зовнішня перспектива інших політик, що використовують маршрутизацію.

2. Час придбання маршруту: певна форма зовнішнього наскрізного вимірювання затримки - особливе занепокоєння щодо "на вимогу" алгоритмами маршрутизації - це час, необхідний для встановлення маршруту на запит.
3. Відсоток доставки поза замовленням: Зовнішній показник продуктивності маршрутизації без підключення, що особливо цікавить протоколи транспортного рівня, такі як TCP, які надають перевагу порядку доставки.
4. Ефективність: якщо ефективність маршрутизації даних є зовнішньою мірою ефективності політики, ефективність є внутрішньою мірою. Для досягнення заданого рівня даних дві різні політики можуть мати різну ефективність маршрутизації суми, залежно від їх внутрішньої ефективності. Ефективність протоколу може безпосередньо впливати, а може і не впливати на продуктивність маршрутизації.

Якщо контроль і трафік даних повинні спільно використовувати той самий канал, а ємність каналу обмежена, надмірна контроль трафіку часто впливає на продуктивність маршрутизації даних. Корисно відстежувати кілька коефіцієнтів, які висвітлюють внутрішню ефективність протоколу у виконанні своєї роботи:

- Середня кількість переданих бітів даних/доставлених бітів даних - це можна розглядати як міру бітової ефективності доставки даних у мережі. Побічно це також дає середню кількість стрибків, пройдених пакетами даних.
- Середня кількість переданих контрольних бітів / біт даних доставлено - вимірює бітову ефективність протоколу в контроль над доставкою даних. Зауважте, що це повинно включати не тільки біти в управлінні маршрутизацією пакетів, а також біти в заголовку пакетів даних. Іншими словами, все, що не є даними, - це витрати на управління, і має враховуватися в контрольній частині алгоритму.
- Середня кількість керованих та переданих пакетів даних/даних доставлених пакетів - замість вимірювання чистої алгоритмічної ефективності з точки зору кількості бітів, ця міра намагається зафіксувати ефективність доступу до каналу

протоколу як вартість каналу доступу високого рівня посилань на основі суперечок.

Крім того, необхідно враховувати мережевий контекст, в якому продуктивність протоколу вимірюється. Основні параметри, які слід включати:

1. Розмір мережі - вимірюється кількістю вузлів
2. Мережеве підключення - середній ступінь вузла (тобто. середня кількість сусідів вузла)
3. Топологічна швидкість змін - швидкість, з якою працює мережева топологія змінюється
4. Ємність лінії зв'язку - ефективна швидкість лінії зв'язку, виміряна в бітах/секунду, після обліку збитків через багаторазовий доступ, кодування та ін.
5. Частка односпрямованих посилань - наскільки ефективно це робить а Протокол виконують як функцію наявності односпрямованості посилання?
6. Шляхи руху - наскільки ефективним є протокол для адаптації до нерівномірних або суцільних режимів руху?
7. Мобільність - коли і за яких тимчасових і просторовиз обставин топологічна кореляція відповідає характеристикам а протокол маршрутизації? У цих випадках, що є найбільш підходящою моделлю для імітації рухливості вузлів в MANET?
8. Частка і частота сплячих вузлів - як поводиться протокол при наявності сплячих і пробуджуючихся вузлів?

Протокол MANET повинен ефективно функціонувати в широкому діапазоні контекстів мереж - від невеликих, спільних, спеціальних груп до більші мобільніх, багатопрофільних мереж. Попереднє обговорення характеристик та показників оцінки дещо диференціюють MANET від традиційних, провідних, багатопрофільних мереж. Бездротовий мережеве середовище – це, певною мірою, недолік, адже пропускна здатність відносно обмежена, і енергія також може бути такою. Підводячи підсумок,

можливості мережі для МАНЕТ інтригують а технічні компроміси є чисельними і складними. Різноманітність сукупності проблем продуктивністі вимагає нових протоколів для управління мережею. Виникає запитання: якою має бути якість політики вимірювання? Щоб допомогти відповісти на це, ми використаємо метрики, наведені вище для побудови критеріїв оцінки якості сервісу. Слід визнати, що протокол маршрутизації має тенденцію бути придатними для певного контексту мережі та менш підходить для інших. Викладаючи опис протоколу, слід зазначити його переваги та обмеження, щоб визначити відповідні контексти мереж для його використання. Ці атрибути протоколу зазвичай можна виразити якісно, наприклад, чи може протокол підтримувати чи маршрутизацію з найкоротшим шляхом. Якісні описи такого характеру дозволяють широку класифікацію протоколів і складають основу для більшої кількості детальних і кількісних оцінок роботи протоколу.

1.3 Типи MANET

Як і будь-яка цифрова технологія MANET знайшли широку кількість застосуваннь. Для більш детального розуміння даного питання корисно буде ознайомитися з варіантами таких мереж. MANET поділяють на наступні категорії:

- Автомобільна ad hoc мережа (VANET) – забезпечує ефективний зв'язок з іншим транспортним засобом або з придорожнім обладнанням. Інтелектуальні ad hoc автомобільні мережі (InVANET) працюють з іншим транспортним засобом або з придорожнім обладнанням.
- Ad hoc мережа для смартфонів (SPANC) – для створення peer to peer з'єднання не покладаючись на мережі стільникових операторів, точки бездротового доступу або традиційну мережеву інфраструктуру. Тут о peer to peer вузли можуть приєднуватися чи виходити з мережі, не руйнуючи її.
- Інтернет-основані мобільні Ad hoc (iMANETs) - підтримує такі інтернет-протоколи, як TCP/UDP і IP. Зв'язати мобільні вузли і встановлює маршрути розподілено і автоматично.
- Hub-Spoke MANET – Кілька підлеглих MANET можуть бути підключені до локальної мережі VPN для створення географічно розподіленої MANET. Звичайний алгоритм Ad hoc маршрутизації не застосовується безпосередньо.
- Військові або тактичні MANET – використовується у військових частинах. Акцент на швидкості передачі даних, попиті в реальному часі, швидкій зміні маршруту та мобільність, безпека, дальність радіозв'язку і т. д.
- Повітряна мережа Ad hoc (FANETs) – складається з безпілотного літального апарату (зазвичай відомого як дрон). Забезпечує зв'язок з віддаленими районами і мобільність.

1.4 Аналіз протоколів маршрутизації у MANET

У ad hoc мережах кожен вузол повинен мати можливість пересилати дані для інших вузлів. Тому пропонуються різні схеми маршрутизації для забезпечення достатньої продуктивності ad hoc мереж. Ad hoc маршрутизація поділяється на проактивну, реактивну та гібридну маршрутизацію.

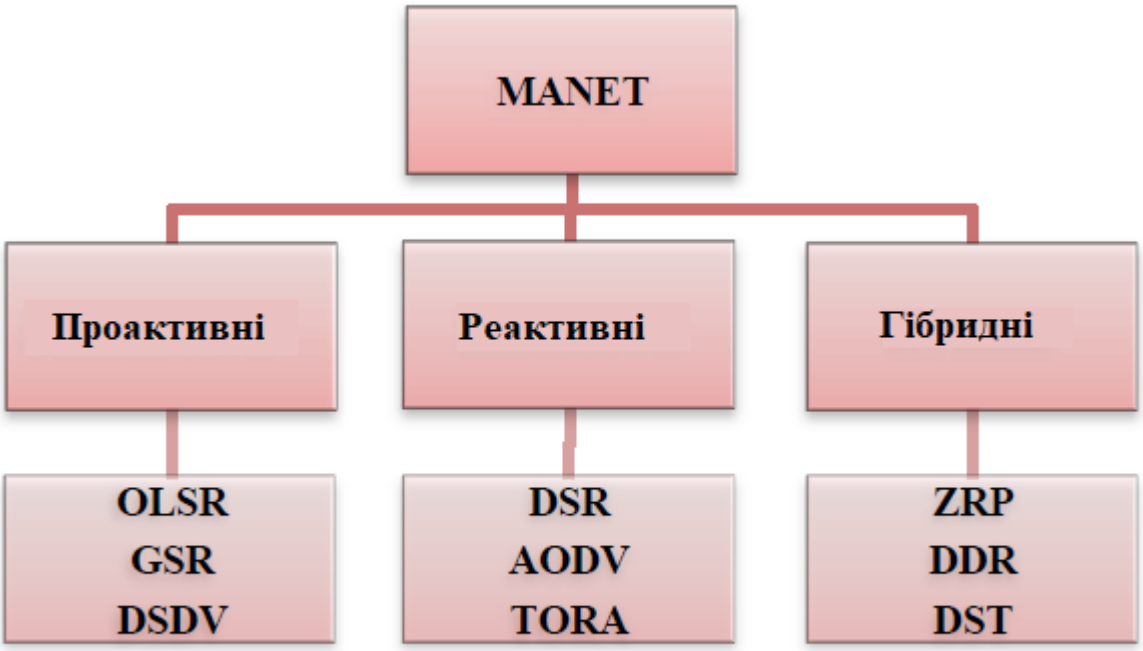

Рис. 1.2. Групи протоколів маршрутизації MANET

1.4.1 Проактивні протоколи маршрутизації

У протоколах маршрутизації, керованих таблицями, прийняті протоколи та сучасна маршрутизація послідовно до всіх вузлів підтримується на кожному вузлі, де, як і при маршрутизації на вимогу, маршрути створюються лише тоді, коли віддає перевагу хост-джерело. Вузли іноді шукають інформацію про маршрутизацію всередині мережі. Фіксована вартість цих протоколів можлива, оскільки вона вільна для профілів трафіку і має фіксовану верхню межу. Це перевага проактивних протоколів маршрутизації, наприклад OLSR, GSR, DSDV.

OLSR - це оптимізація алгоритму чистого зв'язку, використовує теорію багатоточкових реле (MPR) для переадресації управління трафіком, запропоновану для розподілу по всій мережі. Набір MPR вибирається таким чином, що він охоплює всі вузли, що знаходяться за два стрибки. OLSR працює з періодичною заміною таких повідомлень, як Hello messages та Topology Control (TC), лише через MPR. Параметрами, які OLSR використовує для контролю накладних витрат протоколу, є параметр Hello-interval, параметр інтервалу TC, параметр звітування MPR та параметр резервування TC

Протокол GSR базується на алгоритмі фіксованого стану зв'язку. GSR покращив спосіб послідовного розподілу в алгоритмі стану зв'язку, обмеживши повідомлення про оновлення лише серед проміжних вузлів. У GSR кожен вузол підтримує таблицю стану зв’язку на основі актуальної інформації, яка очікується від сусідніх вузлів, і час від часу обмінюється інформацією про стан зв’язку лише із сусідніми вузлами. Це значно зменшило кількість контрольних повідомлень, що передаються в мережі. Розмір оновлення повідомлення досить велике, і , як розмір мережі росте , вони отримають ще більше.

У протоколі DSDV кожен вузол підтримує послідовність маршрутів для всіх відомих пунктів призначення. Інформація про маршрутизацію час від часу оновлюється . Кожен вузол підтримує таблицю, яка містить інформацію про всі

існуючі пункти призначення, наступний вузол, що прибуває до пункту призначення, кількість стрибків для досягнення пункту призначення та порядковий номер. Вузли час від часу надсилають цю таблицю всім сусідам для підтримання топології, що додає додаткових витрат на мережу. Кожен вхід в таблиці маршрутизації позначений номером замовлення, присвоєним вузлом призначення. Номери серій дозволяють мобільним вузлам відрізняти застарілі маршрути від нових, таким чином уникаючи структури циклів маршрутизації.

1.4.2 Реактивні протоколи маршрутизації

Протоколи маршрутизації на вимогу "на вимогу" означає, що вони будують маршрути між вузлами лише за вибором вузлів-джерел. Він підтримує ці маршрути до тих пір, поки вони вимагаються джерелами. Реактивні (на вимогу) протоколи маршрутизації описують ідеальний характер спеціальної мережі, яка набагато динамічніша, ніж інфраструктурні мережі. Замість того, щоб час від часу оновлювати інформацію про маршрутизацію, реактивні протоколи маршрутизації оновлюють інформацію про маршрутизацію при появі потреби в маршрутизації, зменшуючи таким чином накладні витрати на управління, головним чином у мережах з високою мобільністю, де періодичне оновлення призведе до значних марних накладних витрат, наприклад AODV , DSR, TORA.

AODV - це суміш вектора на вимогу та відстані, тобто методологія маршрутизації від переходу до переходу. Коли вузол хоче знати маршрут до певного пункту призначення, він створює ЗАПИТ НА МАРШРУТ. Потім запит маршруту пересилається проміжними вузлами, які також виробляють зворотний маршрут для себе до пункту призначення. Коли попит досягає вузла з маршрутом до пункту призначення, він знову створює ВІДПОВІДЬ, що містить кількість стрибків , необхідних для досягнення пункту призначення. Усі вузли, які відіграють роль у

пересиланні цієї відповіді на вихідний вузол, створюють прямий маршрут до пункту призначення. Цей маршрут, що виробляється від кожного вузла від джерела до пункту призначення, є перехідним станом, а не повним маршрутом, як у маршрутизації джерела.

У динамічній маршрутизації джерела початковий вузол генерує запит маршруту (RREQ), який передається через пакет даних, і він визначає вузол джерела, а також пункт призначення. Згодом пакет відправляє алгоритмом заливки в MANET. Кожен вузол отримує пакет RREQ і не знає про маршрут до пункту призначення, тому об'єднайте його ім'я у списку, який розміщений у заголовку пакета, а потім транслюйте пакет. Якщо кожен вузол не може передати пакет даних іншим вузлам у MANET, тоді генерується пакет даних про помилку маршруту (RERR), який повторно передається по маршруту.

Тимчасово впорядкований алгоритм маршрутизації (TORA) є високоадаптивним, без циклу, розподіленим алгоритмом маршрутизації, заснованим на ідеї обміну посиланнями. Він використовує спрямовані ациклічні графіки (DAG), щоб пояснити маршрути як вгору, так і внизу. TORA передбачає чотири основні функції: створення, підтримка, стирання та оптимізація маршрутів. Оскільки кожен вузол повинен мати висоту, деякий вузол, який не має висоти , вважається пустим вузлом, а його висота - нульовою. Іноді вузли мають певні нові висоти, щоб поліпшити структуру зв’язку. Ця мета називається оптимізацією маршрутів.

1.4.3 Гібридні протоколи маршрутизації

Гібридні протоколи маршрутизації мають перевагу як проактивних, так і реактивних протоколів маршрутизації, щоб збалансувати затримку та контрольні витрати (з точки зору організації пакетів). Гібридні протоколи маршрутизації намагаються максимізувати прибуток від проактивної маршрутизації та реактивної

маршрутизації, використовуючи активну маршрутизацію в малих мережах (з метою зменшення затримки) та реактивну маршрутизацію у великомасштабних мережах (з метою зменшення витрат на контроль), наприклад ZRP, DST, DDR.

Протокол зонової маршрутизації (ZRP) У ZRP вузли керують зоною маршрутизації, яка визначає колекцію, необхідну кожному вузлу для активної підтримки мережевого з'єднання. Отже, для вузлів усередині зони маршрутизації маршрути є негайно доступними. Для вузлів, які лежать поза зоною маршруту, маршрути визначаються на вимогу (тобто реактивно), і він може використовувати будь-який протокол маршрутизації на вимогу для перевірки маршруту до необхідного пункту призначення.

Розподілене обширне дерево (DST) Вузли в мережі згруповані в ряд дерев. Кожне дерево має два типи вузлів; вузол маршруту та внутрішній вузол. Корінь контролює колекцію дерева і те, чи може дерево поєднуватися з новим деревом, а решта вузлів у кожному дереві є звичайними вузлами. Всі вузли можуть знаходитися в одному з трьох різних станів; маршрутизатор, об'єднати та налаштувати залежно від категорії завдання, яке він намагається виконати. DST пропонує дві стратегії припинення маршруту між парою джерела та цільової точки: Гібридне підтоплення дерева (HTF), Шаттл розподіленого обширного дерева (DST).

Розподілена динамічна маршрутизація (DDR) Спланував протокол маршрутизації на основі дерева без необхідності кореневого вузла. Дерева побудовані з використанням постійних маякових повідомлень, якими обмінюються лише найближчі вузли. Алгоритм РДР включає наступні шість фаз: (i) бажані вибори сусідів; (ii) внутрішньодерев'яна кластеризація; (iii) кластеризація між деревами; (iv) лісове будівництво; (v) іменування зон; та (vi) розділення зон.

Параметр	Проактивні	Реактивні	Гібридні
Вимоги до сховища	Високі	Залежить від кількості маршрутів	Залежить від розміру зони чи кластеру
Схема маршрутизації	На базі запитів	На базі таблиць	Комбінація двох
Підтримка мобільності	Підтримка маршрутів	Періодичні оновлення	Комбінація двох
Надлишок маршрутизації	Низький	Високий	Середній
Маршрутизаційна інформація	Збарігається в таблиці	Не збарігається	Залежить від вимог
Ємність зберігання	Загалом низька	Висока	Залежить від розміру зони
Філософія маршрутизації	Загалом лінійна	Лінійна	Ієрархічна
Затримка	Низька	Висока	Низька на локальному рівні

Рис. 1.3 Аналіз характеристик протоколів маршрутизації MANET

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі було розглянуто основні переваги та недоліки MANET, складнощі у роботі з ними. Було проаналізовано доступні протоколи маршрутизації MANET та представлено класифікацію протоколів маршрутизації в таких мережах. Було складено порівняльну таблицю основних характеристик. Протоколи поділяються на три основні категорії: проактивні (керовані таблицею), реактивні (за запитом), гібридні протоколи. Такий огляд протоколів є інструментальним для подальшої роботи над якістю сервісу, проектування оптимального (для певних випадків) алгоритму пошуку шляху.

РОЗДІЛ 2. ЯКІСТЬ СЕРВІСУ QOS У БЕЗДРОТОВИХ МЕРЕЖАХ БЕЗ ІНФРАСТРУКТУРИ

2.1 Стисла історія QoS

На початку 2000-х переважаючими видами трафіку в IP-мережах були голос та дані. Голосовий трафік передавався у реальному часі і включав постійну та передбачувану пропускну здатність та час прибуття пакетів. Трафік даних здійснювався не в режимі реального часу і включав непередбачувану (або нестримну) смугу пропускання та широкий і різний час прибуття пакетів. З цього часу різні типи відеотрафіку ставали дедалі важливішими для ділового спілкування та діяльності. Комплекс відеотрафіку включає кілька підтипів трафіку, таких як пасивне потокове відео, інтерактивне відео в режимі реального часу та відеоконференцій.

Відеотрафік може передаватися в режимі реального часу (але не завжди), використовує різні вимоги до пропускної здатності та включає різні типи пакетів з різною толерантністю до затримки та втрат, але той же досвід роботи з кінцевим користувачем (сесія).

Бездротовий доступ став невід'ємною частиною життя протягом останніх кількох років, і сьогодні безліч різних пристроїв блукає та реєструється у різноманітних державних та приватних бездротових мережах. Мережі доступу WiFi мають змінну характеристику пропускної здатності та пропускної здатності залежно від розташування та потужності кінцевого пристрою щодо точки доступу (AP) і засновані на повністю різній архітектурі рівня управління доступом до медіа (MAC), ніж типова 802.3 Ethernet.

Це призвело до цілого нового набору завдань QoS, крім проблем дротових мереж із фіксованою пропускною здатністю. Деякий період часу після первинного розгортання мережеві адміністратори використовують засоби QoS для управління трафіком в цілях забезпечення безпеки і бізнесу. Підприємство, як правило, хоче використовувати власні внутрішні навчальні відеоролики більш високої якості, ніж не пов'язане з бізнесом відео в Інтернеті, яке відтворює працівник, навіть якщо обидва відео використовують одну і ту ж технологію і з технічного боку є одним видом відео трафіку (збережене трансляційне або багатоадресне відео).

2.1.1 Основи та концепції QoS

Основною метою QoS є управління суперечками щодо мережевих ресурсів, щоб максимізувати якість сеансу для будь-якого типу операцій для кінцевих користувачів. Оскільки не всі пакети рівні, їх не слід обробляти однаково.

Функції QoS реалізують систему керованої несправедливості в мережі. Деякі сесії мають пріоритет над іншими сесіями; чутливі до затримок собі ssions обходу черг пакетів , які займають сеанси менш чутливі до затримки; коли queuin г буфер переповнення, пакети будуть впали на сеансах , які можуть оговтатися від втрати або на тих , які можуть бути усунені з мінімальним впливом на бізнесі. Щоб звільнити місце для пакетів, що належать до сесій з високим діловим впливом, які не можуть терпіти втрати, не впливаючи на досвід кінцевого користувача, іншими сеансами *керують* (тобто пакети вибірково відкладають або відкидають, коли виникає суперечка) на основі прийнятих рішень щодо політики якості. в мережі.

2.1.2 Моделі QoS: IntServ та DiffServ

Перша спробу стандартизувати QoS було проведено в середині 1990-х років, коли IETF опублікував RFC інтегрованих служб (IntServ) (RFC 1633, 2211 і 2212). Ці

RFC зосереджені на протоколі сигналізації, який називається протоколом економії ресурсів (RSVP). RSVP сигналізує про вимоги до пропускної здатності та затримки для кожного сеансу повторного прослуховування диска кожному вузлу вздовж шляху (логічної схеми) від кінцевої точки відправлення до кінцевої точки прийому. Спочатку RSVP вимагав, щоб кожен вузол прислухався до своїх резервацій, що було вкрай недоцільно в Інтернеті, на якому співіснують сервери, комутатори та маршрутизатори кожного опису, вінтажу та постачальника. RSVP також вимагає, щоб кожен вузол підтримував стан потоку. Для вирішення цих проблем незабаром з'явився інший набір стандартів - модель диференційованих послуг (DiffServ) - як друга спроба стандартизувати QoS (RFCs 2474, 2597, 2598, 3246, 4594). Модель DiffServ описує різні способи поведінки, які повинні бути прийняті кожним сумісним вузлом. Вузли можуть використовувати будь-які доступні функції (власні чи інші) на вибір постачальника для відповідності. Пакетні маркування, такі як IP старшинство, диференційовані коди послуг (DSCP), були визначені поряд з конкретним за шаг поведінками (PHBs) для основних типів трафіку.

У міру того, як моделі IntServ та DiffServ еволюціонували, загальна популярність одного методу порівняно з іншим коливалася вперед і назад із адвокатами з обох сторін. Хоча інтелектуальні дебати залишаються невирішеними (будь-яка модель забезпечує цілісне рішення), реалізації QoS на сьогоднішніх мережевих архітектурних принципах зупинилися в основному на моделі DiffServ , іноді включаючи надмірне число вибраних функцій IntServ. Однак поширення змінної ширини смуги частот Acces S зв'язків, такі як 802.11 бездротові мереж і збільшення обсягів затриманого і джиттер трафіку , чутливе (відео), для яких IntServ модель має чудові можливості, призвело до у відродження RSVP в сучасних мережах. У IntServ і DiffServ моделі концептуально конкурентні, але на виявляється, що вони доповнюють один одного. Тому ці моделі часто спільно розгортаються в реалізаціях QoS мереж. IntServ - єдиний інструмент з динамічною інформацією про мережу для прийняття рішень щодо контролю за пропускною спроможністю (AC), що робить це практичним для мережевих ліній

зв'язку, де пропускна здатність має високу ціну; з іншого боку, DiffServ є набагато гнучкішим та масштабованішим, і як такий може бути широко розповсюдженим через мережу, щоб забезпечити відповідність PHB на кожному вузлі.

Існує чимала кількість літератури щодо понять QoS, технологій та особливостей. Тому мета цього розділу не в тому, щоб повторювати, як працюють ці інструменти, а в тому, щоб дати короткий огляд ключових доступних інструментів і показати, як вони взаємодіють між собою та яку комбінацію інструментів можна використовувати для досягнення оптимальних рішень проектування якості обслуговування мережі. Як правило, інструменти QoS поділяються на такі категорії:

- **Інструменти класифікації та маркування:** Сеанси, або потоки, аналізуються, щоб визначити, до якого класу трафіку вони належать і, отже, склад пакетів у потоці . Після визначення пакети маркуються так, що аналіз відбувається лише обмежену кількість разів, як правило, на крайньому рівні мережі. Пакет може перетинати декілька різних мереж до точки призначення, і тому перекласифікація та повторне маркування досить часто зустрічається в точках передачі при вході в нову мережу.
- **Інструменти надзору, маркировки та формування:** Різним класам трафіку відводиться певна частина мережевих ресурсів (що може виражатися в абсолютних або відносних відсотках). Коли трафік перевищує доступні мережеві ресурси, деякий трафік може бути вибірково випущений, затриманий або перенаправлений, щоб уникнути перевантажень . Сесії відстежуються, щоб переконатись, що вони не використовують більше свого виділеного місця, і якщо вони використовують, рух трафіку припиняється (надзор), сповільнюється (формвання) або перемаркірується (маркировка).
- **Інструменти планування або управління перевантаженнями:** Коли рівень перевищення доступних мережевих ресурсів перевищує доступ, трафік чекає в черзі на наявність ресурсів.

- **Інструменти, що стосуються зв’язків:** Деякі типи зв’язків вимагають спеціальної обробки та інструментів, таких як фрагментація та методи чергування. Деякі посилання також мають угоди про смугу пропускання (нижчі за фізичну швидкість), які не слід перевищувати, і якщо сплеск трафіку перевищує ці межі, він формується (або сповільнюється) відповідно до угоди.

2.2 Аналіз якості сервісу у MANET

Існування якості обслуговування (QoS) є підтвердженням, даним в рамках порядку дій заздалегідь встановлених обмежень щодо виконання організації для замовника в тій мірі, в висновок до кінця відкласти оцінки, доступний межа передачі, ймовірність нещастя посилки тощо. Існують різні програми та адміністрації які вимагають певного забезпечення якості. Узгодження різних можливостей системного рівня, включаючи спрямування, організацію та безпеку, необхідну для потужної діяльності універсальної ad hoc мережі. На сьогоднішній день аналітики стандарту MANET вільно займаються питаннями якості та безпеки. В даний час як частини безпеки, так і QoS впливають протилежним чином на загальний стан системи, якщо розглядати її окремо. Це може вплинути на роботу QOS та безпеки а також можуть вплинути на основні та базові адміністраційні вимоги MANET.

Безпека та QoS є надзвичайно важливою областю досліджень у MANET, тим не меньш вони до сих пір досліджуються без будь-якої значної міри кооперації.

Проблеми поєднання QoS та безпеки як одиночного параметра дуже гостро постають у MANET. У цьому напрямку не було зроблено жодних спроб, які могли б дозволити об'єднання QoS та безпеки як цільного набору параметрів в MANET. При написанні QoS під безпекою мається на увазі оцінка якості, проте метод змішування не

перевірявся. Можливість безпеки, оцінка якості обслуговування була запропонована в якості теоретичної категорії.

Перспективою цієї думки є те, що інструменти безпеки та організації якості розглядаються в має більш розширити безпеку і хід дії кількісних факторів безпеки були розпізнаний , що може бути використано для кількісної оцінки надійності.

Нашою основною точкою дотику до бази на цій моделі було зосередження уваги на мобільності системи замість мобільності концентраторів, виводячи розвиток цілих підмереж по відношенню один до одного, тоді як окремі клієнти спочатку асоціювались з одним таким підпунктом, систему може подібним чином переміщено на різні території. Одним з розмежувань є зони бойових дій, що об'єднують водні кораблі, літаки та сухопутні війська. У цій "системі систем" підмережі (наприклад, суднові каркаси) пов'язані між собою методами для природної універсальної віддаленої системи (наприклад, між рухомими понтонами). Клієнти будуть в першу чергу пов'язані з їх будинками рамки поки є дозвіл для переміщення між просторами. Труднощі за таких обставин приєднуються до взаємодії на різних етапах, підтримання приналежності до безпеки та розповсюдження підходів до забезпечення якості обслуговування .

2.2.1 Обробка пакетів в ad hoc мережах

AODV використовує 3 інформаційні композиції: запити маршруту (RREQ), відповіді маршруту (RREP) та помилки маршруту (RERR). Ці записи отримуються за допомогою UDP, і після цього підключається звичайна обробка заголовків IP. Запитуючий хаб використовує свою IP-адресу як IP-адресу оригінатора для повідомлень. Для трансляції повідомлень використовується адреса зв'язку обмежена IP (255.255.255.255), тобто повідомлення не надсилається безцільно. У будь-якому випадку, AODV вимагає кілька повідомлень (наприклад, RREQ), щоб бути поширеними цілком по мережі. Як справлятися з розповсюдженням таких RREQ,

демонструє TTL у заголовку IP, таким чином не виникає необхідності у перериванні. Статус з’єднання демонструється на наступному стрибку по динамічному курсу та перевіряється хабом. У будь-який момент, коли розм’якшення зв’язку розпізнається за динамічним курсом, повідомлення використовується для сповіщення різних хабів про те, що сталася відмова підключення, що з хабом є RERR. Це показує лише ті хаби, до яких можна дійти через розірваний зв’язок, наприклад. У тому випадку, якщо в точці B відбудеться розрив з'єднання, у цей момент повідомлення RERR покаже, що хаб D більше не є досяжним цілями, які вже не виконуються через хаб B.

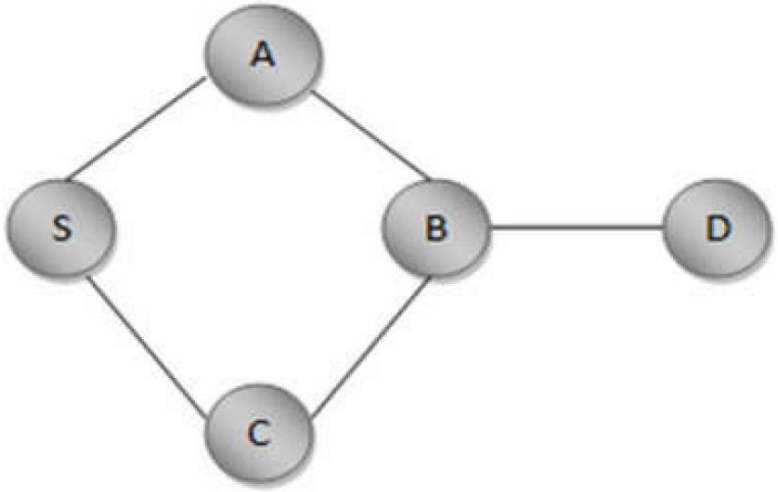

Рис 2.1. Індикація повідомлення RERR

Для розширення можливостей цього компонента кожен хаб має "попередній вигляд", який містить інформацію щодо IP-адреси для кожного з його найближчих сусідів, які можуть використовувати його як наступний стрибок для досягнення мети. Дані, що відображаються у попередньому запуску, фактично отримуються в процесі обробки повідомлення RREP за віком, яке повинно бути відправлене до центру списку попередників.

Якщо RREP має нульовий префікс довжини, в цій точці відправник з RREQ, який запитано в даному RREP включений серед попередників звичайно не дуже для конкретної мети. Протокол маршрутизації AODV управляють таблицями

маршрутизації, зберігаючи дані для коротких курсів, які зроблені для зберігання кшляхів до хабів відправляючих RREQs.

AODV використовує супровідні поля з кожним розділом таблиці маршруту:

- IP-адреса цільового хабу
- Номер послідовності цільового хабу
- Дійсний банер з порядковим номером призначення.
- Інші банери та рульові банери.
- Мережевий інтерфейс
- Кількість стрибків
- Наступний хоп
- Список попередників
- Термін служби (час закінчення або час стирання курсу)

QoS мають пошаровий вигляд, який містить 3 розділи:

- Користувач
- Додаток
- Мережа

a) Рівень додатку QoS: Цей шар контролює, наскільки добре бажання користувача, такі як чистий голос, відео без преривання, і так далі виконані. Цей рівень також відображає приклад посадки та прихильність до затримок транспортування . На цьому рівні виконуються наскрізні конвенції (RTP / RTCP), зображення та кодування, що стосуються додатків (FEC, чергування) .

b) QoS мережевого рівня : Цей рівень має чотири змінні якості:

- Швидкість передачі - Швидкість, з якою рух передачі повинен передаватися системою.
- Бездіяльність - затримка, яку може витримати один додаток, передаючи одиночку пакет інформації.
- Джиттер – зміна інертності.
- Втрати - рівень втраченої інформації.

2.2.2 Характеристика MANET з позиції QoS

MANET включає компактні каскади (наприклад, комутатор з різними хостами та віддаленими конкретними пристроями), що просто наводяться як "центральні точки", яким дозволено переміщатися дискретно. Центральні точки можуть бути розташовані в літаках, на кораблях, вантажних автомобілях, автомобілях або на них, можливо, на людях чи невеликих гаджетах, і можуть бути різними хостами на комутаторі. MANET є самостійними та децентралізованими. Структура може працювати сама по собі, або може мати шлюзи та взаємодіяти з мережею зі сталою структурою. Вузли оснащені дистанційними передавачами і отримувачами з використанням дроти, які можуть бути всенаправленими (транзитними), однонапрямленими (точка-точка), або їх сумішами.
У певний момент часу, залежно від позицій центральних точок, а також контурів їх передавача та одержувача, рівні управління передачею та рівні пропускною здатністю спільного каналу, віддалений доступ як самоствердний, багатогранний Ця унікально підібрана топологія може змінюватися з часом, коли вузли переміщаються або змінюють параметри їх передачі та збору. Отже, MANET має кілька помітних атрибутів:

- Динамічні топології: Вузли можуть переміщатися самостійно, таким чином, топологія системи може змінюватися випадково та надзвичайно швидко, що може зруйнувати як однонапрямлені. Так і двонапрямлені з’єднання.
- Примусове з’єднання з обмеженою пропускною здатністю: бездротові з’єднання Wi-Fi продовжуватимуть зменшувати обмеження, ніж їхні партнери. Подібним чином, визнана пропускна здатність віддалених зв’язків, що відображає наслідки різного доступу, розмитості, галасу та обструкції, і так далі, регулярно значно менша, ніж швидкість передачі. Одним із наслідків загальнонизьких обмежень для координації зв’язків є те, що зупинка зазвичай є стандартним, а не рідкісним випадком, тобто, відповідно до попиту на програми, мабуть, наближатиметься чи перевищуватиметься. Оскільки гнучка структура часто є, по суті, розширенням

усталеного середовища, адаптовані клієнти з унікальним іменем потребують певної організації. Ці запити будуть продовжувати збільшуватись у міру того, як зростатиме шум.

- Дія, пов’язана з енергоспоживанням: Деякі або більшість основних вузлів у MANET можуть покладатися на свої батареї чи інші подібні засоби. Щодо центральних точок, найбільш базовим критерієм структури ділянки може бути безпека.
- Обмежена фізична безпека: Мобільні віддалені фреймворки, як правило, більш підвержено фізичній небезпеці, ніж сталі мережі. Тривала правдоподібність прослуховування крадькома має бути розглянута в окремому порядку. Існуючі стратегії безпеки зв’язків раз у раз асоціюються з віддаленими структурами для зменшення ризиків безпеки. Як плюс, децентралізована ідея управління фреймворком в MANET надає додаткову силу проти саботажу конкретної фізичної частини мережі, що виходить за межі уніфікованих методологій. Крім того, деякі віртуальні системи (наприклад, переносні військові системи або, навпаки, системи паркувальних майданчиків) можуть бути в міру експансивними (наприклад, десятки або сотні центрів на територію управління). Вимога до універсальності не є надзвичайною для MANETS. Незважаючи на це, у світлі попередніх якостей, системи, необхідні для досягнення універсальності, ймовірно є. Ці якості становлять підозри та клопоти щодо виконання конвенційних схем, що виходять за межі вимог до проектувальників мереж зі статичними топологіями.

2.2.3 Виклики проектування MANET

Один з головних недоліків MANET походить від їх відкритого спільного проектування. На відміну від дротових каркасів, які мають перемикачі, кожен зручний центр у мережі може заповнюватись як перемикач та передавати групи для різних центральних точок. Віддалений канал доступний як для чесних користувачів так для агрессорів. Тому в MANET немає однозначної лінії впевненості з точки зору безпеки. Точка ув'язнення, яку егретиепід всередині, щоб розібратися із зовнішнім світом, вітер темніє. Немає спеціально представленого путі / закладу, де ми могли б пройти особливий курс дій щодо безпеки. Найкращі універсальні пристосування та дані безпеки системи, які вони зберігають, - це безсильні угоди або фізичний улов, особливо гаджети низького класу із слабкими гарантіями. Зловмисники можуть проникнути в систему через ці перекриті хаби, які представляють слабкі місця зв’язку і спричиняють доміно вплив розривів безпеки в рамках. Обмеження активів рядкових елементів у MANET складають ще один нетривіальний тест на контур безпеки. Віддалений канал передачі потужність зобов'язана і розподілятися між різними системами управління речовинами. Розрахунок здатність портативного концентратора додатково орга GED. Наприклад, деякі гаджети низького класу , наприклад, КПК, ледве можуть виконати обчислення серйозних підписів, таких як відхилений криптографічний розрахунок. Оскільки стільникові телефони регулярно харчуються від акумуляторів , вони можуть мати надзвичайно обмежені життєві активи. Універсальність віддаленого середовища та концентратора створює набагато більше потоку в MANET, порівняно з дротовими системами. Топологія системи надзвичайно унікальна, оскільки концентратори якомога частіше приєднуються до системи або виходять із неї, і меандр у системі буде повністю один. Віддалений канал так само піддається імпедансам і помилкам, демонструючи нестабільні якості, що стосується ємності передачі даних та відстрочки. Незважаючи на такий прогрес, багатофункціональні клієнти можуть попросити будь-коли, де завгодно будь-які

переваги безпеки, коли вони рухаються, починаючи з одного місця, а потім на наступне. Вищевикладене на честі MANET безпомилково представляє захист для побудови багатоповерхових механізмів безпеки, які забезпечують як широке забезпечення, так і привабливе виконання системи. Для початку механізм безпеки повинен розподілятися навхрест на численні окремі сегменти і залежати від їх сукупної енергетичної впевненості, щоб забезпечити цілісну систему. Ділянка безпеки, яку отримує кожен пристрій, повинна працювати в межах своїх власних обмежень активів, формулюючи можливості обчислення, пам’ять, ліміт кореспонденції та життєздатність. По-друге, механізм безпеки повинен проходити через окремі рівні конвенційного стеку, причому кожен шар додається до лінії захисту. Жодна одношарова домовленість не може завадити кожному одиничному потенційному нападу. По-третє, механізм безпеки повинен порушити небезпеку з боку двох країн-партнерів, які здійснюють напади на віддалений канал та топологію системи, та інсайдерів, які вникають у фреймворк через торгувані гаджети та отримують доступ до певної структури у формуванні. По-четверте, механізм безпеки повинен охоплювати кожну з трьох частин уникнення, визнання та реагування, які працюють, щоб захистити структуру від зминання. Щоб підсумувати ситуацію, механізм безпеки повинен бути розумним та поміркованим у надзвичайно потужній та обмеженій ресурсами організаційній ситуації.

2.2.4 Маршрутизація у MANET з точки зору QoS

Універсальна ad hoc мережа (MANET), яку час від часу називали портативною робочою системою, - це система самовпорядкування стільникових телефонів, пов’язаних за допомогою віддалених з’єднань. В кінці дня, MANET є певною групою взаємопов’язаних хабів, що бажають говорити один з одним, але не мають сталої структури або заздалегідь встановленної топології дистанційних з’єднань. Кожен хаб в MANET вільний рухатись у напрямку до будь-якого шляху і відповідно змінюватиме

свої з'єднання з різними гаджетами більшу частину часу. Кожен хаб має завдання поступового пошуку інших вузлів з якими вони можуть обмінюватися інформацією напряму. Через обмеження передачі прапорів в усіх вузліх, не всі вузли можуть прямо говорити один з одним. Кожен вузол повинен рухатись випадковим чином до за власною потребою, і таким чином бути перемикачем. Основний тест у побудові MANET полягає у підготовці кожного пристрою до постійного збереження даних, необхідних для надійного обміну інформацією. На цьому шляху хаби повинні передавати посилки на користь різних хабів з конкретною кінцевою метою передавати інформацію по системі. Критичною складовою імпровізованих систем є те, що коригування доступності та якості зв’язку відстежується з увагою до переносимості вузла та контролю за управління потужністю. Працювати навколо ad hoc мереж можна з використанням будь-яких бездротових інновацій, в тому числі інфрачервоного, радіо і т.д. Як правило, кожен вузол оснащено передавачем і комунікатором для спілкування з іншими вузлами.

Відсутність усталеного фундаменту в MANET представляє кілька видів труднощів. Найбільше випробування серед них – це маршрутизація. Маршрутизація – це спосіб визначення шляхів у системі за якими необхідно посилати інформацію. Спеціально призначена конвенція маршрутизації - це традиція або стандарт, який контролює, як хаби обирають, який підхід до обміну інформацією між гаджетами в динамічний системі. У імпровізованих системах хаби не стартують зі знаннями топології системи і повинні визначити її самостійно. Основна думка полягає в тому, що кожен вузол може повідомити про свою сутність і повинні підлаштовуватися під заяви спілкуватися зі своїми сусідами. Кожен хаб дізнається про найближчі вузли та про те, як з ними зв’язатись, і може заявити, що він також може зв’язатися з ними. Процедура маршрутизації, як правило, координує спираючись на таблиці маршрутизації, котрі зберігають записи маршрутів до різних цільових точок мережі.

2.2.4.1 Реактивні протоколи маршрутизації

У ситуаціях з обмеженнями у передачі та контролі даних є зручними тримати систему у стані спокою до появи активності. Реактивні протоколи маршрутизації не слідкують за маршрутами, а обирають їх за наявності потреби. Реактивні протоколи прокладують маршрути за вимогою, наповняючи систему пакетами запиту маршруту. Ці протоколи мають такі переваги:

- Немає величезних витрат на підтримку суцільну таблицю маршрутизації як у проактивних протоколах.
- Швидка реакція на перебудову топології та розташування вузлів.

Дійсно, навіть реактивні протоколи перетворились на стандарт контролю маршрутизації MANET. Тим не меньш , вони мають наступні недоліки:

- Високий час інертності при знаходженні маршруту.
- Непотрібне затоплення повідомленнями може спричинити зупинку системи.

Для MANET існують чисельні протоколи реактивної маршрутизації. Найбільш відомі у галузі: AODV, DSR та DYMO.

Спеціальний вектор відстані за запитом (AODV) є традицією управління гнучкими мобільними мережами (MANET) та різноманітними віддаленими мережевими структурами. Це реагуюча маршрутизаційна традиція, що означає, що вона будує маршрут лише за запитом. З іншого боку, найбільш відомі протоколи управління Інтернетом є проактивними, що означає, що вони знаходять координаційні курси безперешкодно щодо використання цих способів. AODV є, як випливає з назви, є векторним протоколом. AODV уникає залежності від проблеми нелімітованої якості інших векторних протоколів через використання плану повторного використання маршрутів. В AODV мережа знаходиться у стані спокою до тих пір, поки

маршрутизація не потрібна. У той момент вузол, якому необхідний зв’язок робить запрос на з’єднання. Інші вузли AODV передають це повідомлення та записують вузол, від якого вони почули, роблячи короткочасні маршрути до початкового вузла.

Переваги

Перевагою цієї традиції є те, що курси створюються за запитом та номери цільового збору використовуються для пошуку останнього курсу до мети. Затримка при налаштуванні сусідства нижча. Цей протокол не робить додаткового розвитку для зв’язку з існуючими асоціаціями. Більше того, листування за векторним напрямком просте і не вимагає великої кількості пам’яті.

Недоліки

AODV вимагає більших шансів на розвиток приналежності та встановлення прихованої ассоціації. Більше того, широко привабливі центри можуть спровокувати суперечливі напрямки, якщо номер вихідного плану значною мірою старий і прямі центри мають вище, але не останнє цільове число у цьому напрямку.

ВИСНОВКИ ДО РОЗДІЛУ 2

Значною проблемою організації контролю за якістю сервісу є принципова неможливість своєчасного (в ідеалі – миттєвого) збору та опрацювання повної апріорної інформації про параметри та стан мережі. Навіть коли б ми мали повну інформацію про параметри та стан кожного мережного та термінального вузла – ми принципово не можемо мати інформацію про активність мережних абонентів – коли увійшов у мережу, коли зробив запит на з'єднання з тим чи іншим мережним вузлом; яка миттєва та усереднена інтенсивність запитів впродовж сеансу; коли завершив з'єднання, коли вийшов з мережі тощо. Більш того, ми не маємо інформації навіть про миттєву кількість абонентів у мережі. Таким чином для аналізу та оптимізації характеристик бездротових мереж без інфраструктури необхідно застосовувати методи теорії імовірностей та математичної статистики.

РОЗДІЛ 3. РОЗРОБКА МЕТОДУ ПОШУКУ ОПТИМАЛЬНОГО МАРШРУТУ ІЗ ЗАБЕЗПЕЧЕННЯМ НАСКІЗНОЇ ЯКОСТІ СЕРВІСУ

3.1 Розрахунок компромісу між надійністю, затримкою та пропускною здатністю у бездротових мережах з випадковим множинним доступом

Вибух зв’язку машина-машина (M2M) відкриває можливість реалізації безлічі додатків, що вимагають надзвичайно низької затримки та надвисокої надійності. LTE, фактично стандарт для стільникових мереж 4G, постулюється як кандидат на підтримку M2M.

Основна проблема, що стосується використання мережі LTE, стосується її здатності відповідати суворим обмеженням надійності та затримки без шкоди для доставки традиційних програм.

У цій роботі ми досліджуємо три основні показники ефективності (KPI) мереж LTE для зв'язку M2M, а саме - затримку, надійність та пропускну здатність. Ескіз компромісів між трьома KPIs показаний на рис. 3.1 У бездротовій системі важко одночасно виконувати суворі вимоги щодо надійності, затримки та пропускної здатності. LTE значною мірою призначений для максимізації потужностей системи для широкосмугових даних, де найважливішим показником KPIs є середній показник користувача. Середній показник корисного користування, як правило, максимізується завдяки агресивному використанню повторних передач, а також умовно-методичним складанням планування радіоканалів. Ціна, яку потрібно заплатити за таке поліпшення надійності та пропускної здатності, - це деградація з точки зору затримки, у деяких пакетів із підвищеним ризиком виникнення потенційно довгих затримок. У той же час, повторна передача та інші механізми контролю помилок, що передбачають деяку накладну вартість, мають витрати у вигляді збільшення затримки. Питання, на яке ми

хочемо відповісти, полягає в тому, чи здатна мережа доставити корисний набір розмірі біт A в межах B мс з максимальною затримкою C мс та надійністю D%, де типові значення надвисокої надійності становлять 99,999% або 99,99966% (він же шість-сигма). Ми обмежуємо обсяг статті до процедур низхідної лінії зв'язку та PHY / MAC, тобто ми не включаємо процедури вищого рівня, такі як управління радіопосиланнями (RLC) та повторна передача протоколу управління передачею (TCP) в бюджеті KPIs. Дія вищих шарів може бути додана поверх нього, щоб отримати кінцеві показники продуктивності. Існує три основні підходи до вирішення проблеми: аналітичні моделі, напів аналітичні моделі та моделювання.

Аналітичні результати дають нам корисну інформацію про компроміси серед параметрів. Однак нинішні стільникові системи є дуже складними з багатьма різними елементами, що сприяють розслідуванню KPIs. У цьому сенсі прагнення моделювати до останньої деталі часто призводить до математично нерозв'язних проблем. Альтернативою є створення припущень, обмеження обсягу результатів, якщо ці припущення викинуть важливі аспекти реалізму. Тоді доцільно провести статистично достовірні моделювання, які доповнюють аналітичне дослідження та надають показники цікавих KPI.

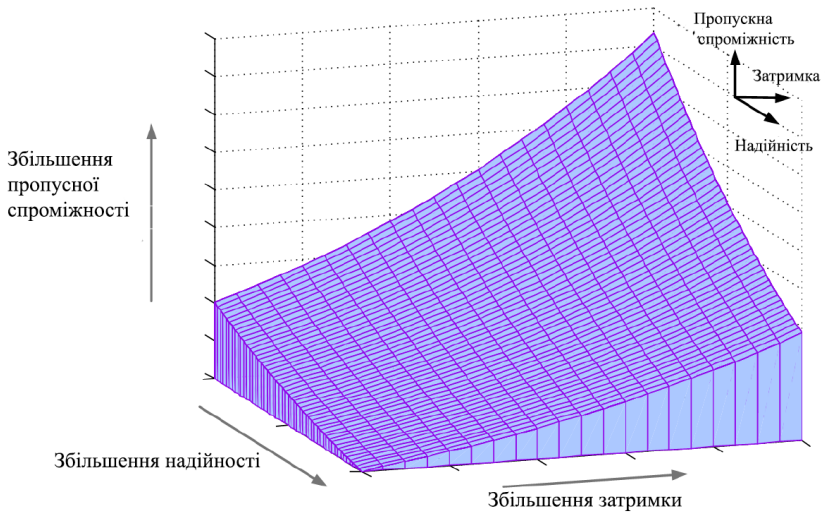

Рис. 3.1. Модель залежності основних показників якості сервісу

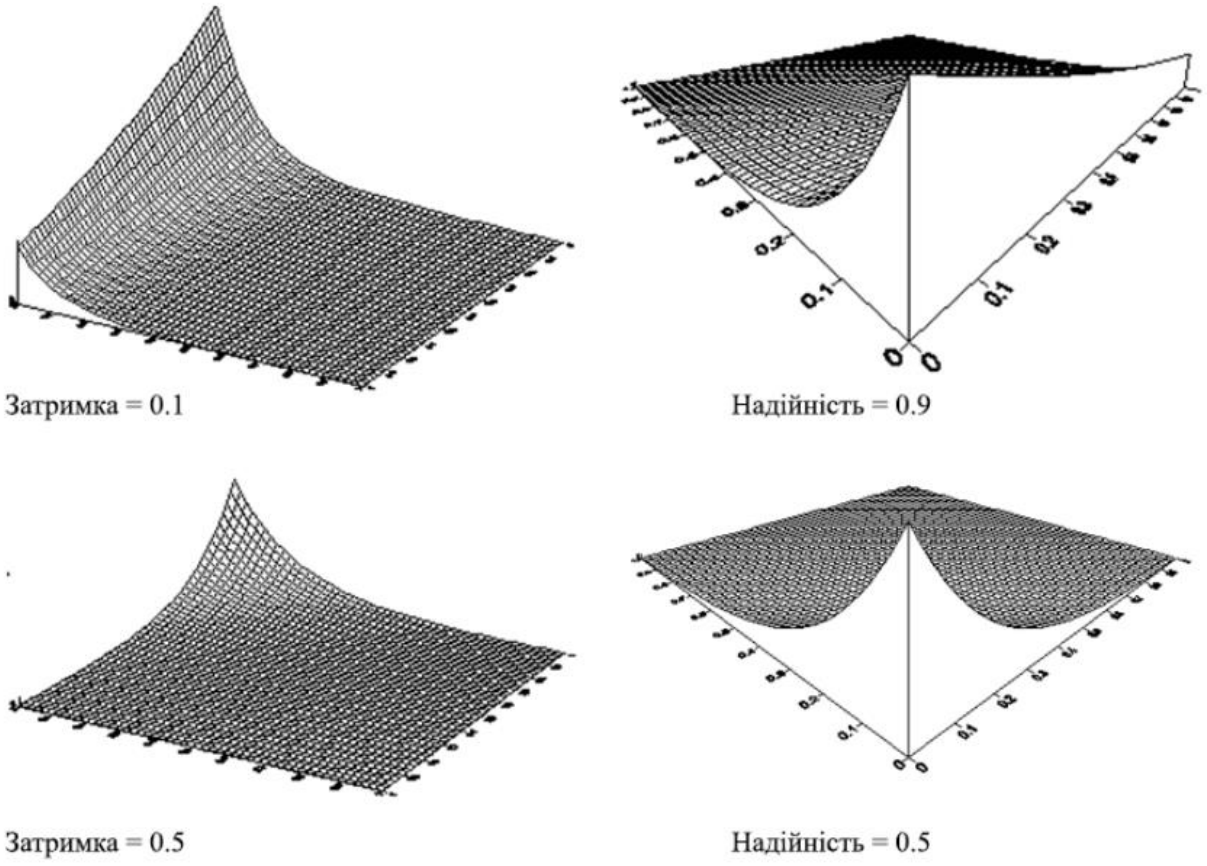

Рис. 3.2. Демонстрація динаміки залежності показників якості

Надійність у сенсі надійності доставляння – без втрат та перекручень бітів

Між тим, напіваналітичні моделі представляють середину, використовуючи часткове використання результатів моделювання як вхід до аналітичних виразів.

Що стосується аналітичного дослідження, ми використовуємо ефективні теорії пропускної здатності та ефективної ємності. Функція ефективної пропускної здатності для заданого джерела, що змінюється часом, визначається як мінімальна швидкість обслуговування, необхідна для доставки даних шляхом виконання певних вимог затримки, виражена у вигляді обмеження статистичної затримки. Аналогічно, ефективна ємність визначається як максимальна постійна швидкість передачі даних,

яку може підтримувати даний сервіс, що змінюється у часі, дотримуючись обмеження затримки. Обидві концепції можуть бути спільно використані для аналізу бездротової системи з випадковим трафіком та коливаннями каналів.

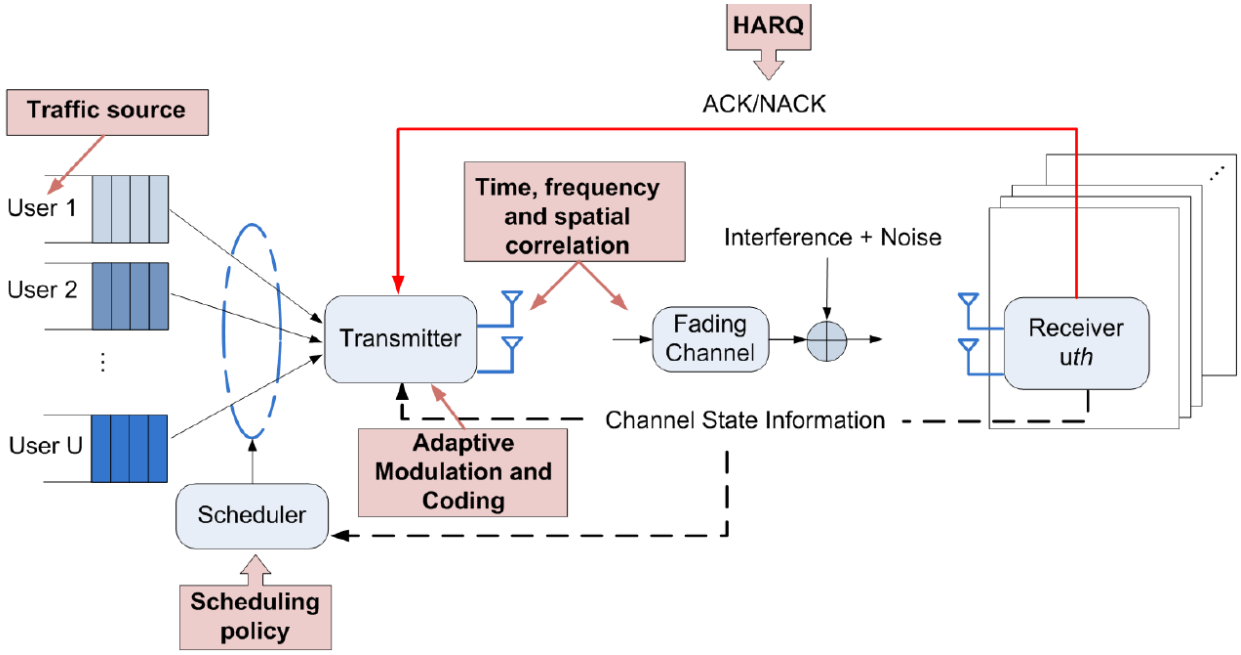

Рис. 3.3. Демонстрація динаміки залежності показників якості

З часу їх впровадження ефективна пропускна здатність та ефективна ємність викликають великий інтерес, і кілька досліджень показали, що моделі здатні оцінювати показники QoS в різних сценаріях.

Решта статті упорядкована наступним чином. Спочатку ми даємо огляд процедур PHY / MAC, що впливають на затримку та надійність роботи LTE. У розділі III ми пропонуємо спільне використання ефективної пропускної здатності та теорії ефективного потенціалу як аналітичної або напіваналітичної бази для дослідження компромісів серед KPI. Розділ IV обговорює використання моделювання на рівні системи та декілька джерел недосконалості в системі.

3.1.1 Огляд моделі мережі

Ескіз моделі системи LTE показаний на рис 3.3, який ми використовуємо для обговорення різних джерел, що сприяють KPI, що цікавлять мережу 4G. Дані від різних користувачів надходять із програми більш високого рівня та зберігаються в буферах передачі користувача. Дуже проста і поширена модель для змінного трафіку передбачає кінцеву корисну навантаження на користувача та користувачів, які прибувають відповідно до процесу Пуассона.

Коли користувач закінчує передачу корисного навантаження, виклик припиняється. Більш реалістичні моделі подібного трафіку для мережі передачі даних передбачають, що пакети, що чергуються з тишами, і деяке співвідношення між пакетами в межах пакету. Взагалі, кореляція та бурхливість у джерелі руху є шкідливими для затримки роботи.

Періодично планувальник розподіляє ресурси каналу для користувачів на основі заповнення буфера, інформації про стан каналу (CSI), про яку повідомляють користувачі, очікувані повторні передачі та інші фактори. LTE підтримує дисципліни планування обізнаних QoS та радіоканалів. Механізми, відомі QoS, можна використовувати для визначення пріоритетності планування критично важливих за часом повідомлень з метою зменшення затримки в черзі передавачів таких повідомлень. Однак уникнення затримок черги не може бути гарантоване при великих пропонованих навантаженнях, що наближаються до межі ємності комірок (або навіть перевищують її).

На передавачі застосовуються методи адаптивної модуляції та кодування (AMC) (також адаптація посилання), так що розмір сузір'я та швидкість кодування динамічно змінюються з метою використання різноманітності каналів та з цільою надійності у вигляді швидкості помилок BLock (БЛЕР). Таким чином, більш надійна модуляція та більш агресивне кодування застосовуються, коли надійність ставиться під загрозу.

Природно, що зниження БЛЕР має витрати в плані зниження спектральної ефективності.

LTE використовує часове, частотне та просторове різноманіття для максимізації спектральної ефективності. У той же час система страждає від часу, частоти та просторової кореляції, і три інгредієнти погіршують показники затримки. Користувачам, яким надається доступ до безпдротового каналу, виділяються ресурси передачі на підкадрі (1 мс) та роздільній здатності блоку фізичних ресурсів (PRB), де один PRB складається з 12 суб несучих, що відповідає частоті пропускної здатності 180 кГц. Бездротовий канал є часовим варіантом і може бути представлений стохастичною моделлю, що фіксує певні часово-частотні кореляційні властивості.

Невизначеності, пов'язані з мінливістю радіоканалу, зменшуються за допомогою методів MIMO із замкнутим циклом (наприклад, просторове різноманіття). Сьогоднішні LTE-реалізації реалізують в основному 2x2 MIMO (тобто різноманітність 4-го порядку), хоча стандарт в принципі підтримує до 8x8 MIMO. Крім того, широкосмугові характеристики LTE (до 20 МГц на носія та 100 МГц з агрегацією несучої) також пропонують різноманітність частот, що допомагає зменшити мінливість ефективного радіоканалу.

На приймачі потрібний сигнал для UE піддається як адитивному тепловому шуму, так і часовим варіантам і частотно-селективним перешкодам. Серед інших, пережиті втручання залежать від активності планування сусідніх комірок (тобто залежно від навантаження інших клітин), а також від місця розташування користувача. Використання вдосконалених алгоритмів приймача з можливостями пом'якшення перешкод поліпшує SINR виявлення після зменшення чутливості продуктивності

до випадковості в інтерференції. Сьогодні LTE в основному покладається на лінійні приймачі мінімальної середньої квадратичної помилки (MMSE) з поєднанням відхилень перешкод (IRC), тоді як триває стандартизація більш розвинених мережевих приймачів з можливостями скасування нелінійних перешкод.

Крім того, деякі методи, що підтримуються в LTE для координації міжклітинних перешкод (ICIC) та узгодженої багатоточки (CoMP), мають тенденцію до збільшення мінливості інтерференції, що ставить під сумнів традиційні рамки адаптації зв'язку.

HARQ - це механізм виправлення помилок, заснований на повторній передачі. Одержувач виробляє або ACK, у випадку передачі без помилок, або NACK, якщо виявлені деякі помилки. Після отримання повідомлення NACK потрібний пакет буде відправлений знову. LTE підтримує гібридний автоматичний повторний запит (HARQ) з м'яким поєднанням. Затримка між двома передачами HARQ на одному каналі зупинки і очікування становить 8 мс. Ця затримка 8 мс в основному є результатом наявності 1 мс підкадру та певних вимог обробки терміналу для LTE.

3.1.2 Розрахунок меж компромісу між характеристиками якості

В аналітичній базі два випадкові процеси моделюють джерело руху трафіку (процес джерела) та згасаючий канал із пов'язаними процедурами адаптації каналу зв'язку (процес каналу). Для простоти ми припускаємо лише одного користувача, але

теорію можна узагальнити для багатокористувацьких систем. Фізичний час, поділений на одиниці, іменовані періодами символів, і представлений дискретною одиницею часу передачі, n.

З одного боку, джерело трафіку має миттєву швидкість джерела a [n], це означає, що кожен символ джерела генерує [n] біти, які зберігаються в черзі користувача. З іншого боку, кожен символ, c [n] біти видаляються з черги і передаються в ефір, будучи c [n] миттєвою швидкістю каналу.

У цій моделі рідини не розглядається жодна упаковка.

Передача через певні канали (наприклад, релеївські канали) не може виконати жодної детермінованої вимоги затримки. У цьому випадку зручніше виразити вимогу затримки через імовірнісне обмеження затримки (Dt, e), де цільова затримка є Dt, а ймовірність перевищення Dt позначається e.

Що стосується надійності, с [n] фіксує адаптивну швидкість передачі та всі процедури PHY / MAC, пов'язані з мінімізацією ймовірності втрати пакетів, таких як AMC та HARQ. Таким чином, вибирається більш щільне сузір'я і більша швидкість кодування, коли стан каналу користувача хороший, збільшуючи с [n]. Після прибуття пакету NACK відповідні повторно передані пакети мають пріоритет, знижуючи с [n].

B. Ефективна пропускна здатність та функціональна потужність

Ефективна пропускна здатність джерела виражає мінімальну постійну швидкість обслуговування, необхідну для даного процесу прибуття, щоб гарантувати ймовірнісне обмеження затримки. Математично,

$$E_A(\nu) = \lim_{n\to\infty} \frac{1}{n \cdot \nu} \log \mathrm{E}\left[e^{\nu A[n]}\right] \quad \forall \nu \geq 0\,, \qquad (1)$$

при цьому A [n] - накопичена швидкість джерела, тобто кількість бітів, генерованих джерелом від 0 до n - 1, $A[n] = \sum_{m=0}^{n-1} a[n]$; і E [·] - очікування.

Двоїста до ефективної пропускної здатності, ефективна ємність канального процесу виражає максимальну швидкість приходу, яку канал може підтримувати, виконуючи обмеження затримки. Математично,

$$E_C(\nu) = \lim_{n\to\infty} \frac{1}{n \cdot \nu} \log \mathrm{E}\left[e^{\nu C[n]}\right] \quad \forall \nu \geq 0\,, \qquad (2)$$

де $C[n] = \sum_{i=0}^{n} c[i]$ накопичена швидкість передачі.

C. Перетин двох кривих

Криві ефективної пропускної здатності та ефективної ємності зображені на рис. 3.3 В обох випадках високе значення параметра ν вказує на більш сувору вимогу затримки - нижчий Dt або ε -, а невелике значення ν символізує слабкі вимоги до затримки. Отже, крива ефективної пропускної здатності джерела трафіку зростає з ν,

починаючи завжди зі середньої швидкості джерела і прагнучи до пікової швидкості джерела як ν → ∞.

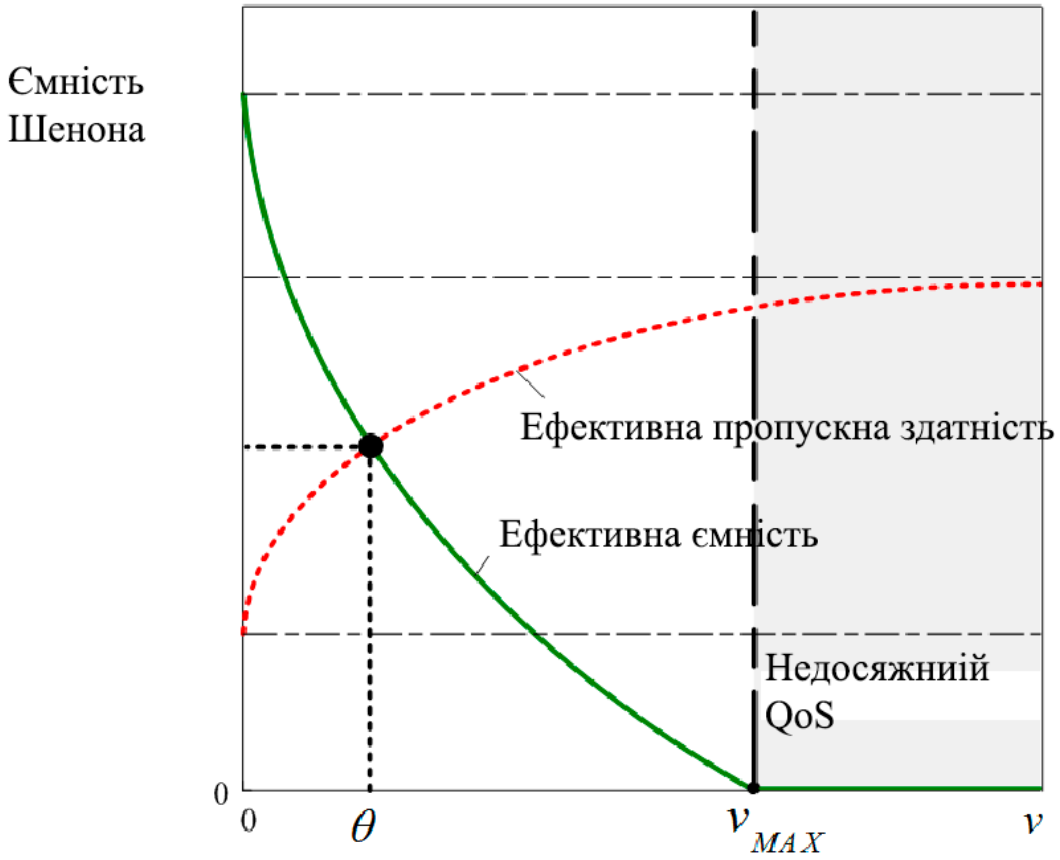

Рис. 3.4. Функція ефективних пропускної здатності та ємності

Пропускна спроміжність каналу {\displaystyle C} C, маюча на увазі теоретичну верхню межу швидкості передачі даних, які можна передавати за допомогою сигналу {\displaystyle S} S через аналоговий канал зв'язку, що підвержено аддитивному гауссівському шуму N, {\displaystyle N} дорівнює

$C = B\log_2\left(1+\frac{S}{N}\right)$, де C – пропускна спроміжність каналу, біт/с; {\displaystyle B} B – полоса пропускання каналу, Гц; {\displaystyle S} S – повна потужність сигналу

в полосі пропускання (энергия), Вт аба В²; {\displaystyle N} N – повна пропускна здатність, Вт или В²; S/N {\displaystyle S/N} – відношення енергії сигналу до спектральної плотності шуму (SNR):

$$q = \left(S/N\right) = \frac{2E_s}{N_0}$$

З іншого боку, ефективна ємність каналу починається від ємності Шеннона, коли ν = 0, без накладення обмежень затримки, і зменшується асимптотично при ν. У випадку каналів Релея крива досягає нуля в певній точці, позначеній на рис. 3.4 як νMAX. Більш високі значення ν означають вимоги QoS, які не є досяжними каналом, незалежно від джерела трафіку. Якщо ми поєднаємо обидві криві, робочу точку системи можна визначити відповідною до перетину двох кривих. Ця точка називається показником QoS θ.

Показник QoS θ фіксує гарантії статистичної затримки (Dt, ε) , і він символізує точку, в якій і джерело трафіку, і канал здатні задовольнити вимогу затримки.

Зв'язок між θ та вимогами явної затримки задається формулою

$$\varepsilon = \Pr\left(D \geq D^t\right) \cup e^{-\theta \cdot E_A(\theta) D^t} \quad \to \infty$$

Обчислення рівнянь (1) та (2) взагалі важко. Для ефективної функції пропускної здатності в літературі досліджено кілька моделей руху, де, серед інших, розглядаються періодичні, гауссові та ввімкнено / вимкнені процеси, а також мультиплексування кількох джерел.

Для математично нездатних джерел також існують методи для оцінки ефективної пропускної здатності, див. оцінка Дембо в або підхід на основі моделювання в [20].

Що стосується ефективної ємності, то припустимо одноканальну та одиночну антенну систему, тобто існує лише кореляція часу.

У цьому випадку накопичену швидкість передачі можна розділити на блоки k символів, передбачаючи внутрішньоблокову кореляцію, але не міжблочну кореляцію,

$$C[n] = \sum_{i=0}^{\frac{n}{k}-1} C_i[k]$$

при $$C_i[k] = \sum_{m=0}^{k-1} c[k \cdot i + m]$$.

Щоб нехтувати міжблоковою кореляцією, вибір k повинен бути тісно пов'язаний з кореляцією каналу. Якщо канал сильно корелює, довші блоки потрібно відмовити, щоб прийняти незалежні блоки. Якщо розмір блоків k досить великий, то C [n] - це сума досить великої кількості незалежних випадкових величин, і застосовується теорема центрального граничного значення. Потім записується ефективна функціональна спроможгість каналу

$$E_C(\nu) = \frac{\mu_k}{k} - \frac{\nu}{2}\frac{\sigma_k^2}{k}$$

де μ_k та σ_k^2 - середнє значення та дисперсія швидкості передачі в блоці,

$$\mu_k = \mathrm{E}\left[C_i(k)\right]$$
$$\sigma_k^2 = \mathrm{E}\left[C_u^2(k)\right] - \mu_k^2.$$

З стаціонарним і ергодичним процесом C [n] середнє значення кожного блоку дорівнює середньому значенню процесу без кореляції, і його можна легко отримати для класичних моделей каналів, таких як Релея або Накагамі. Оцінка дисперсії блоків є більш складною, оскільки вона є результатом багатоваріантного розподілу

E. Узагальнення та напіваналітичний підхід

Для простоти обговорення в попередньому підрозділі не враховує частотної чи просторової кореляції, але кілька досліджень у літературі стосувалися цих аспектівКрім того, доступні також роботи, що включають різні елементи PHY / MAC, що відповідають швидкості передачі даних, як кодування / декодування або процес HARQ та пов'язаний з ним внесок у затримку.

Однак проблема інтеграції всіх цих елементів у єдину аналітичну модель є величезною. Натомість, напіваналітичний підхід для канального процесу використовує емпіричну статистику, витягнуту з моделювання. Вибіркові значення підключаються до (5), отримуючи

$$E_C(\nu) = \frac{\mu_k}{k} - \frac{\nu}{2}\frac{\sigma_k^2}{k}$$

де μ_k та σ_k^2 – вибіркові середнє значення та дисперсія. Для їх отримання накопичена швидкість передачі розбивається на блоки довжиною k і статистичні дані вимірюються за тривалої реалізації канального процесу за допомогою моделювання.

3.1.3 Приклад компромісу між характеристиками якості

Приклад компромісу між пропускною здатністю, затримкою та надійністю за допомогою ефективної пропускної здатності та ефективної рамки пропускної здатності проілюстрований на рис. 3.4. Джерело трафіку є постійним (що передбачає постійну ефективну пропускну здатність), а канал - некорельований процес Релея з однією несучою та одиночною антеною передачі / прийому. Ми припускаємо адаптивну модуляцію зі схемами QAM до 64QAM та заданою швидкістю бітових помилок (BER). Це означає, що пропускна здатність максимізується при збереженні цільової BER шляхом вибору належної модуляції QAM для заданої миттєвої якості каналу. Ні кодування, ні HARQ не використовуються. Максимально досяжна швидкість побудована як функція цільової затримки (вимоги затримки) в обмеженні. Різні рядки представляють різні значення e, починаючи від 1,0 (тобто не вимагаючи затримок) до 0,05. Надійність, відображена в вимозі до BER, варіюється від 10−2 to 10−4.

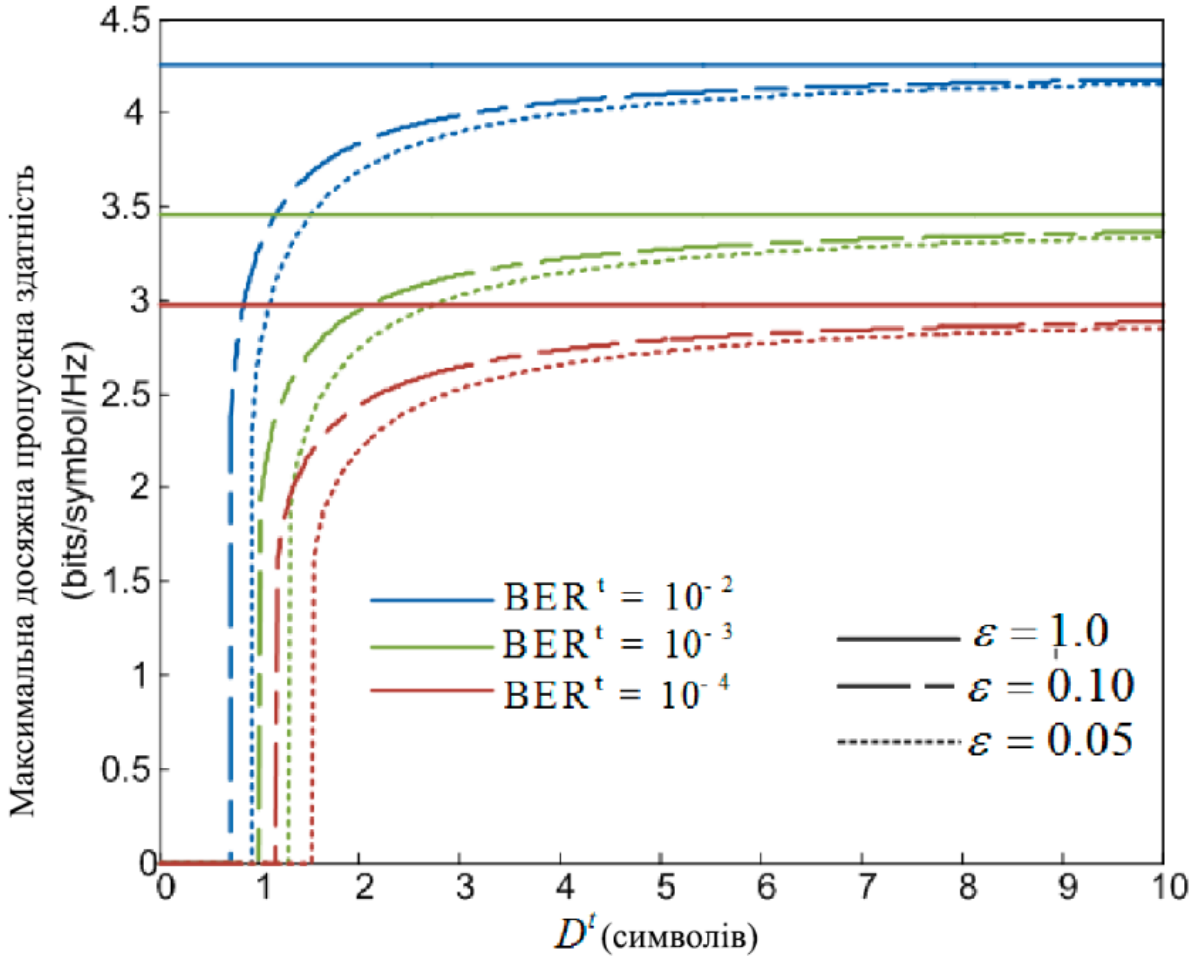

Рис. 3.5. Демонстрація динаміки залежності показників якості

Для жорстких вимог до затримки максимально досяжна пропускна здатність наближається до нуля, обмежуючись системними факторами, наприклад, наприклад, довжина підкадру. У міру послаблення затримки обмеження (вище Dt або вище e) досяжна швидкість зростає в регіоні, де переважає компроміс між навантаженням і затримкою. Помітно, що при e = 1 швидкість нечутлива до іншого параметра затримки, Dt, а досяжна швидкість досягає ємності каналу Шеннона, що, природно, є верхньою межею для розглянутої моделі каналу. Також спостерігається, як пропускна здатність збільшується в міру послаблення обмежень надійності через збільшення рівня модуляції в адаптивній схемі модуляції. Поведінка така ж, якщо додано кодування, з

низьким значенням коефіцієнта помилок, що передбачає нижчу швидкість кодування і, отже, нижчу швидкість передачі даних.

Аналітична база, представлена в Розділі III, дає змогу добре зрозуміти основні механізми, що впливають на KPI. Одне спостереження полягає в тому, що в середовищі для багатьох користувачів три KPI можуть бути гарантовані лише за частку навантаження в системі та за рахунок більших затримок для решти користувачів, які доклали найкращих зусиль у мережі. Більше того, основні процедури, що стосуються дослідження, можуть бути включені до системної моделі, щоб отримати гарне наближення до кінцевих значень. Однак спрощення та ідеалізація обмежують сферу суто аналітичних досліджень при роботі з дуже складними системами, як це стосується LTE.

Моделювання рівня може моделювати не тільки всі відповідні елементи, але й різні джерела недосконалості. Окрім випадкових елементів, описаних у Розділі II, кілька джерел недосконалості на рівні PHY / MAC також важливі для показників затримки та надійності. Наприклад, AMC використовує отриманий зворотний зв'язок CSI, який зазнає різних недосконалостей, таких як недосконаліть вимірювань, кількісна оцінка, затримка звітності та помилки прийому. Усі вони можуть бути представлені випадковим процесом, що по суті означає, що існує певна ймовірність того, що AMC, обрана базовою станцією, відхиляється від ідеально потрібного вибору. Крім того, на продуктивність HARQ впливає випадковість, пов'язана з іноді рідкісним неправильним виявленням ACK / NACK на базовій станції з терміналів. Складова мінливість усіх джерел недосконалості, визначених у таблиці, дійсно може призвести до довгих хвостів затримки передачі, хоча з низькою ймовірністю.

3.2 Розробка моделі MANET з оптимальним маршрутом доставки

Протоколи маршрутизації abstract-many були запропоновані без урахування ефекту нижніх шарів. Тут пропонується модифікований Ad-Hoc On Demand вектор відстані маршрутизації на основі Bit Error Rate (MAODV-BER), де знаходження шляху AODV було модифіковано для досягнення стабільного маршруту шляхом отримання Bit Error Rate (BER) інформації від фізичного шару за допомогою міжшарового підходу. Через використання мультимедійних додатків у мобільних ad hoc мережах MANET необхідна сувора якість обслуговування. Отже, для виконання QoS додаються вимоги до пропускної здатності та затримкиу до кожного повідомлення маршруту. Нарешті, обраний шлях із мінімальним BER, а також мінімальним числом стрибків та які відповідають вимогам QoS.

Бездротовий зв'язок завдяки своїй всюдисущій природі є основною сферою досліджень у світі спілкування. Через різну природу пропускної здатності та суворе QoS з обмеженим часом автономної роботи ad hoc мережі виникають обмеження підтримки мультимедійного зв'язку. MANET як ad hoc мережа - це розподілена мережа, де маршрутизація найкоротшого шляху не підходить, оскільки вона вибирає мінімальний маршрут підрахунку стрибків, який є не найкращим показником. Більшість протоколів маршрутизації, такі як AODV, DSDV, DSR тощо, використовують кількість переходів як метрику для вибору маршруту в MANET, тому ці маршрути, вибрані з урахуванням кількості переходів, можуть бути не якісним показником, оскільки ці посилання зазвичай мають погану якість SNR, вищу частоту помилок кадру (FER), низьку пропускну здатність тощо. Окрім наявності мультимедійного трафіку в MANET, пошук можливого маршруту та виконання багатьох обмежень (наприклад, пропускна здатність, затримка, тощо) зв’язку створює головну проблему QoS маршрутизації та одночасного ефективного використання мережевих ресурсів.

Для оптимізації бездротових мереж слід враховувати що проблеми, що виникають внаслідок зв'язку та вимоги до якості обслуговування, генеруються з програми. Вимоги, що генеруються з додатків, можна задовольнити, прийнявши швидкість, потужність та кодування на фізичному рівні, враховуючи умову для поточного каналу та мережі. Таким чином, для досягнення максимальної можливої адаптивності знання повинні ділитися між усіма шарами. Це називається перехресним дизайном. У цьому дослідженні вимоги до пропускної здатності та затримки QoS додатків вивчаються шляхом модифікації існуючих AODV, а міжшаровий дизайн використовується для надання інформації про фізичний рівень, тобто BER, для мережевого рівня. Повідомлення RREQ і RREP з AODV додаються до наступних шарів: 1) Пропускна здатність 2) Затримка та 3) BER, а також HELLO модифікується, щоб мати доступну пропускну здатність, яка використовується для оновлення таблиці маршрутизації в проміжних вузлах.

3.2.1 Інтеграція методів QoS та протоколу маршрутизації AODV

Було проведено кілька робіт з інтеграції QoS з AODV, а також зроблено метод крос-шару для надання інформації BER мережевому рівню. А. Актер та Т. Сангуанкотчакорн запропонували NQoS AODV для підтримки кількох обмежень QoS . Тут повідомлення про запит маршруту (RREQ), повідомлення про відповідь маршруту (RREP) модифіковані для забезпечення якості обслуговування відповідно до вимог програми. H. Sun та HD Hughes запропонували адаптивну маршрутизацію QoS, де DSR модифікований для функції маршрутизації, а місцеві статистичні обчислення проводяться за допомогою міжшарового механізму з урахуванням різних параметрів від фізичного рівня до мережевого рівня і, нарешті, на основі цих знань, в адаптивному QoS приймається рішення про маршрутизацію. У MAODV (модифікований AODV) маршрут обрано з якомога коротшою довжиною стрибка, який має кращу якість зв'язку, тобто шляхом вибору шляху з меншим наскрізним BER.

3.2.2 Алгоритм MAODV-BER

У запропонованому алгоритмі маршрутизації MAODV-BER політика маршрутизації AODV використовується для пошуку маршруту від джерела до пункту призначення. Кожен проміжний вузол розширений, щоб містити додаткову таблицю маршрутизації, яка містить інформацію про смугу пропускання та BER. У цій роботі ми пропонуємо алгоритм маршрутизації , який бере BER посилання з фізичного рівня і буде наданий мережевому рівню як параметр для розрахунку надійного шляху. BER визначатиметься за SNR. Аналогічним чином, вимога щодо якості обслуговування надаватиметься додатком мережевого рівня. Рівень MAC приймає необхідні параметри з мережевого рівня, щоб задовольнити обмеження QoS, які накладаються рівнем програми. Повідомлення RREP додається із необхідною пропускною здатністю та доступною пропускною здатністю, тоді як HELLO змінено, щоб містити доступну пропускну здатність. Кожен вузол підтримує таблицю, в якій інформація про список вузлів до яких він має з'єднання, була підтримуватися . Ця таблиця називається сусідньою таблицею, і повідомлення HELLO періодично передаються для оновлення інформації про сусідів у цій таблиці. Розрахунок BER проводиться на фізичному рівні, і ця інформація використовується для розрахунку частоти помилок кадру (FER), яка надається мережевому шару для пошуку стабільного маршруту. FER можна розрахувати, використовуючи наступне рівняння.

$$P_e^m L = (1 - 1 - P_b^m)^{8L}$$

Де, P_b^m - розрахункова ймовірність BER для кожного режиму PHY m, P_e^m - частота помилок кадру для L- байтового кадру і m дорівнює m = 1, 2, 3 та 4 для 1, 2, 5.5 та 11 Мбіт /с відповідно PHY.

А. Маршрутизуючий алгоритм

У запропонованому алгоритмі маршрутизації MAODV-BER виявлення маршруту та переадресація пакетів виконуються з наступними кроками:

1. Коли вузол намагається надіслати пакети, повинен бути відомий шлях до пункту призначення, таким чином перевіряється таблиця маршрутизації. Якщо необхідні QoS та BER задовольняються, вузол резервує ресурс і передає пакети.
2. Якщо маршруту немає, а вимога QoS та BER не задовольняються, вузол транслює повідомлення RREQ, використовуючи протокол маршрутизації AODV.
3. Проміжні вузли отримують ці пакети RREQ, якщо вони задовольняють всім вимогам, RREP надсилається назад до джерела.
4. Коли RREQ надсилається, воно надсилається з мінімальним BER, а проміжні вузли з вищим BER замінять свої значення, але вище значення не повинно перевищувати порогове значення 0,001.
5. Коли RREP відправляється назад до джерела, кожен проміжний вузол перевіряє та порівнює свою доступну пропускну здатність із полем пропускної здатності повідомлення RREP і ставить мінімум цих двох значень у RREP та відправляє до джерела.
6. Отримавши RREP, джерело порівнює затримку з вимогами та передає дані за обраним шляхом, а також відкидує повторювані пакети RREP, отримані з інших можливих шляхів.
7. Обирається шлях із мінімальним BER та найнижчим числом стрибків, що задовольняє вимогам QoS .

Таким чином, у цій запропонованій схемі ми підтримуємо поріг BER на рівні 0,001. Для пошуку ефективного шляху, по-перше, BER повинен бути задоволений, як і інші вимоги QoS на цих шляхах. Якщо всі ці вищезазначені умови не виконуються, тоді пакети передаються як негарантований трафік. Якщо трапляються розриви маршруту, повідомлення RERR надсилається джерелу, а альтернативний шлях

вибирається шляхом надсилання RREQ. В іншому випадку, якщо тайм-аут у буфері не відбувається, він вибирається з буфера.

3.2.3 Параметри моделі MANET

У цьому дослідженні було проведено порівняльний аналіз запропонованого алгоритму маршрутизації MAODV-BER з AODV. Різні параметри, такі як середня наскрізна (end-to-tnd) затримка, Packet Delivery Ratio (PDR), Control Overhead (CO) і пропускна здатність аналізуються. Для імітації запропонованого протоколу маршрутизації використовується burst трафік. Для забезпечення достовірності всі результати моделювання будуються з 95% інтервалом гарантії. Кількість вузлів дорівнює 50 з парами 25s-d з часом паузи 0 секунд. Кожна точка даних усереднюється з 10 циклів моделювання з однаковим сценарієм руху.

Під час моделювання розглядаються такі три показники ефективності:

1. Середня кінцева затримка: затримка між тимчасовим моментом, за який пакет даних виникає у вихідному вузлі, та моментом часу, коли він досягає пункту призначення.
2. Коефіцієнт доставки пакетів (PDR): відношення кількісті пакетів даних, отриманих одержувачем, до кількості пакетів даних, надісланих джерелами.
3. Control Overhead: кількість контрольних пакетів, виміряних за одиницю часу. Він задається в кбіт, мбіт.
4. Пропускна здатність: кількість успішно переданих бітів даних за одиницю часу. Вимірюється в кбіт/с, мбіт/с, гбіт/с.

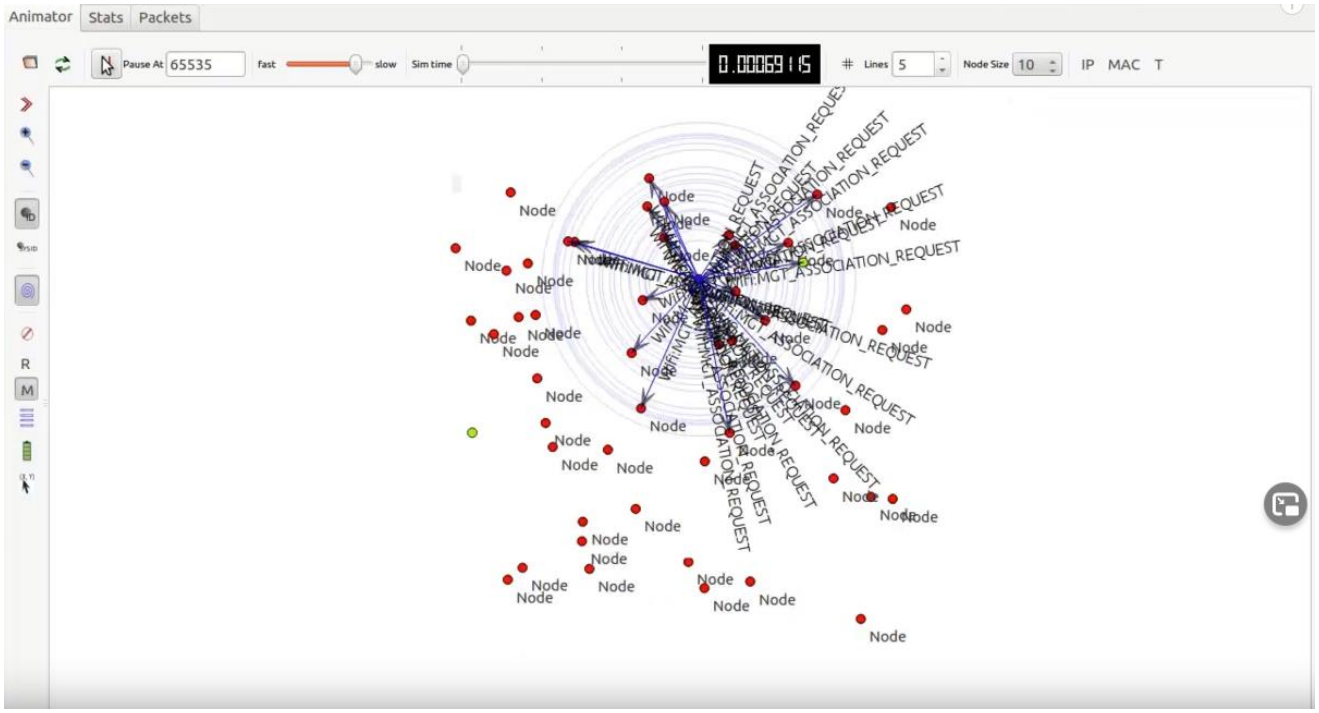

Рис. 3.6. Топологія моделюємої мережі у NS-3

3.2.4 Моделювання та результати

NS2 використовується для оцінки параметрів продуктивності. Пакети різного розміру генеруються для аналізу пакетного трафіку. Для підтримки якості обслуговування таблиця маршрутизації ведеться в кожному проміжному вузлі.

Для аналізу пакетного трафіку, швидкість руху вузлів варіюється від 1 до 20 м/с при пропонованому навантаженні 100 кбіт/с на пару.

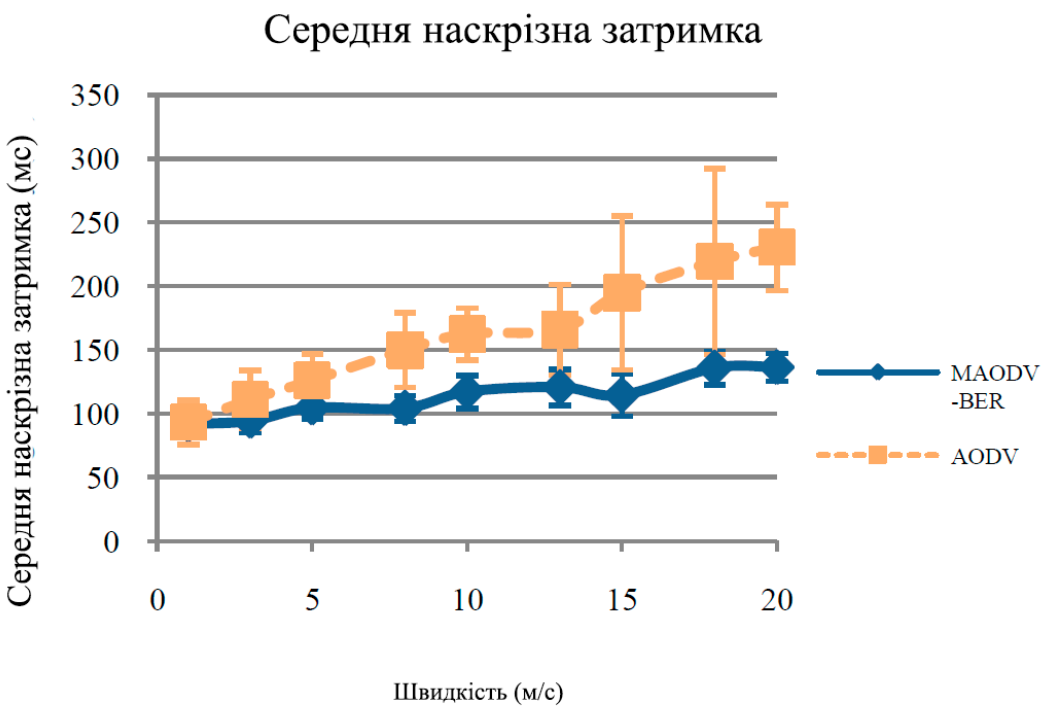

Рис. 3.7. Графік зміни середньої наскрізної затримки

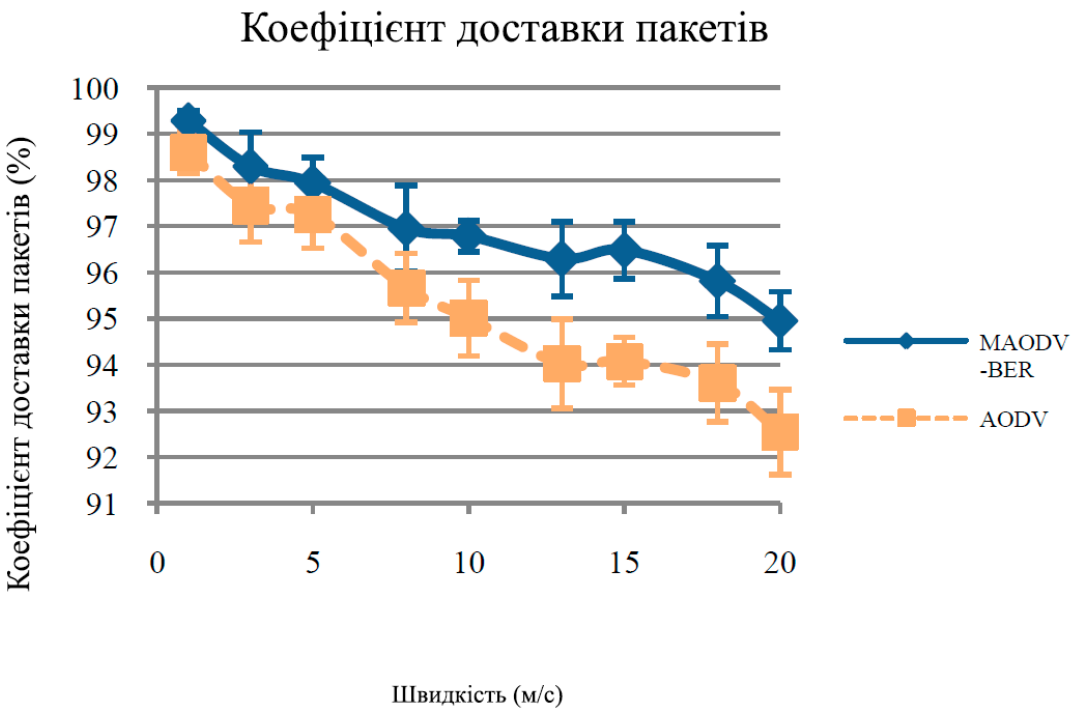

Рис. 3.8. Графік зміни коефіцієнту доставки пакетів

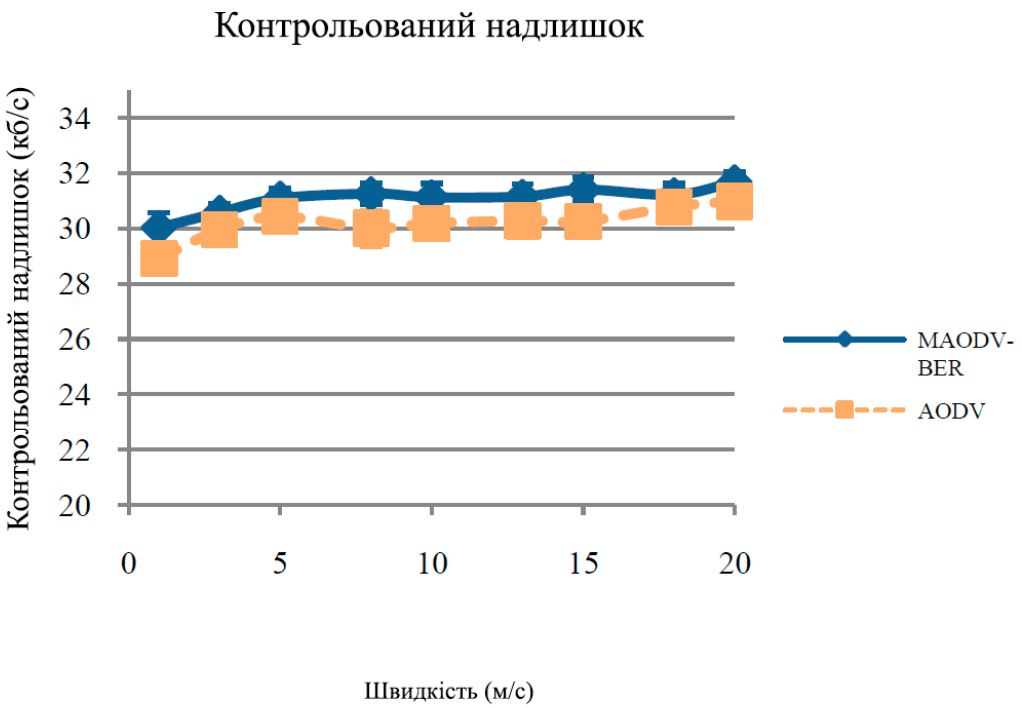

Рис. 3.9. Графік зміни надлишку контролю

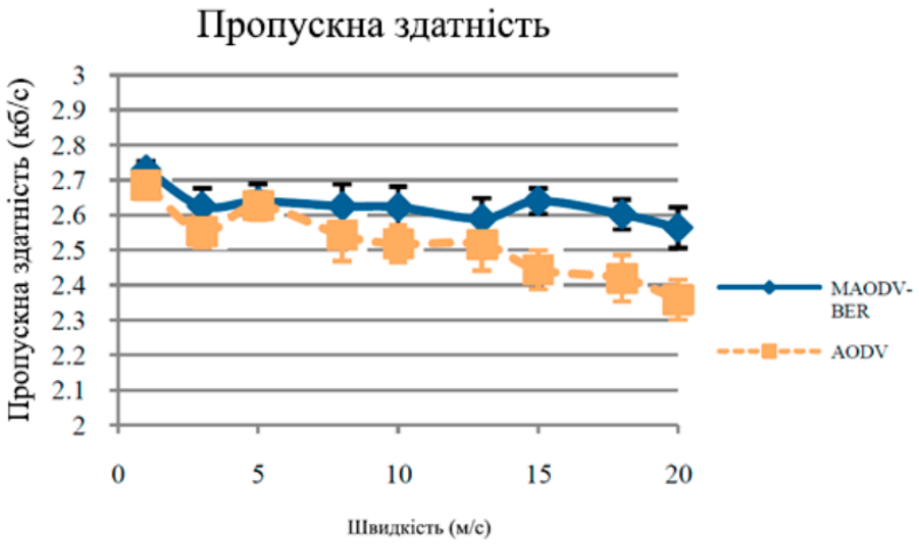

Рис. 3.10. Графік зміни пропускної здатності

Відповідно до результатів моделювання, показаних на всіх вищенаведених графіках, середня наскрізна затримка нижча, але PDR і пропускна здатність вищі, ніж типовий AODV з однаковим обсягом накладних витрат на управління, як типовий AODV, оскільки запропонований алгоритм маршрутизації вибирає шлях, що задовольняє QoS, а також вимоги BER. Зі збільшенням швидкості вузлів траплятиметься збій маршруту, оскільки вузол може лежати за межами передачі. Це спричиняє часту зміну маршруту, для вибору стабільного маршруту потрібно створити більше контрольних пакетів. Через це пакети повинні чекати в черзі протягом тривалого часу, поки відбувається ремонт локальних зв'язків. Це довге очікування в черзі призводить до зниження коефіцієнта доставки пакетів із збільшенням кінцевої затримки. Але у випадку запропонованого MAODV-BER, буде обрано стабільний маршрут, враховуючи BER каналу, що призводить до пошуку стабільного маршруту з низькою відмовою маршруту. BER буде мінімальним, якщо потужність передачі висока. Таким чином, врахування низького BER призводить до низької втрати даних, що в кінцевому рахунку збільшує PDR, і дані не повинні чекати в черзі, що призводить до низької затримки.

Чим більше число помилок маршруту, тим більше буде потрібно генерувати контрольних повідомлень. Отже, у випадку типового AODV існує багато збоїв маршруту, що призводить до збільшення витрат на управління, як показано на рис. 3.8 Враховуючи випадок запропонованого MAODV-BER, для оновлення сусідів та пошуку стабільних шляхів потрібно створити більше повідомлень HELLO, який призводить до незначного збільшення витрат на управління, ніж типовий AODV, як показано на рис. 3.9 Збільшення помилок маршрутизації призводить до збільшення втрати пакетів, що в кінцевому рахунку зменшує PDR, і, нарешті, це також впливає на пропускну здатність. Як показано на рис. 3.9, із збільшенням швидкості вузлів пропускна здатність запропонованого MAODV-BER залишається вищою, ніж типовий AODV, через вищу доставку пакетів з меншими втратами, оскільки запропонований алгоритм розглядає стабільний маршрут.

ВИСНОВКИ ДО РОЗДІЛУ 3

Під час аналізу було виявлено, що запропонований алгоритм маршрутизації MAODV-BER добре працює із змінною швидкістю. Завдяки вибору стабільного маршруту до пункту призначення, враховуючи показники BER та QoS, продуктивність мережі покращується. При використанні базового AODV головним завданням протоколу було знайти маршрут із мінімальною кількістю стрибків. Це означає, що стабільність маршруту не враховувалася, що призводить до втрати даних. Таким чином, використовуючи MAODV-BER, враховується шлях із низьким рівнем BER та QoS відповідно до програми, що призводить до високої пропускної здатності. Нарешті, ми можемо зробити висновок, що з використанням MAODV-BER може бути прокладений стабільний маршрут з більшою кількістю пакетів даних, а втрата даних через часті збої маршруту в MANET може бути мінімізована. Компроміс використання запропонованої системи полягає в тому, що вона повинна підтримувати таблицю маршрутизації, яка вимагає місця в пам'яті та збільшення витрат на контрольні повідомлення для коректної маршрутизації. Розрахунок BER кожної лінії також збільшує витрати на управління.

ВИСНОВКИ

З розвитком мережевих технологій потреба у бездротових мережах постійно зростає. Питання надання якісного сервісу залишається відкритим уже багато років і особливо гостро воно постає у проектуванні мереж з мобільними топологіями. Не дивлячись на свою гнучкість, такі мережі мають ряд недоліків та складностей у їх проектуванні.

У ході виконання дипломної роботі було оброблено значну кількість наукового матеріалу, охарактеризовано основні сильні та слабкі сторони мобільних мереж без інфраструктури, категоризовано протоколи маршрутизації таких мереж. Було розглянуто питання маршрутизації у контексті контролю якістю сервісу.

Було побудовано модель бездротової мережі без інфраструктури MANET та досліджено контроль якості за триплетом якості сервісу пропускна спроможність – затримка – рівень бітових помилок. Змодельовано бездротову мережу MANET на базі наукового програмного забезпечення NS-3 та проаналізовано алгоритми пошуку оптимального шляху. Під час аналізу змодельваної мережі було виявлено, що запропонований алгоритм маршрутизації MAODV-QoS добре працює із змінною швидкістю. Завдяки вибору стабільного джерела форми маршруту до пункту призначення, враховуючи показники QoS, продуктивність мережі покращується.

В цілому, можна стверджувати, що мети, яку було встановлено перед початком дослідження було досягнуто. Результати даної роботи можна використовувати при подальшому більш детальному дослідженні надання якості сервісу у бездротових мережах без інфраструктури.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ – М.: Высшая школа, 1989. – 364 с
2. Столлингс В. Современные компьютерные сети. 2-е изд. – СПб.: Питер, 2003. – 783 с.
3. Вегешна Ш. Качество обслуживания в сетях IP. – М.: Вильямс. – 2003. – 368с.
4. Szigeti T. End-to-End QoS Network Design, 2nd ed. / Tim Szigeti, Robert Barton, Christina Hattingh, Kenneth Briley, Jr. - Cisco Press, 800 East 96th Street, Indianapolis, IN 46240, 2013. - 1090 pp.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
6. Tanenbaum, A.S. Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 pp.;
7. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 538 pp.;
8. Kurose J.F. Computer Networking: A Top-Down Approach, 7th Ed / James F. Kurose, Keith W. Ross. - Pearson Education, Inc., 2017. - 864 pp.

ДОДАТОК А

Код програми:

```
#include <fstream>
#include <iostream>
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
#include "ns3/mobility-module.h"
#include "ns3/aodv-module.h"
#include "ns3/olsr-module.h"
#include "ns3/dsdv-module.h"
#include "ns3/dsr-module.h"
#include "ns3/applications-module.h"
#include "ns3/yans-wifi-helper.h"

using namespace ns3;
using namespace dsr;
NS_LOG_COMPONENT_DEFINE ("manet-routing-compare");

class RoutingExperiment
{
public:
 RoutingExperiment ();
 void Run (int nSinks, double txp, std::string CSVfileName);
 //static void SetMACParam (ns3::NetDeviceContainer & devices,
 // int slotDistance);
 std::string CommandSetup (int argc, char **argv);
private:
```

```
 Ptr<Socket> SetupPacketReceive (Ipv4Address addr, Ptr<Node> node);
 void ReceivePacket (Ptr<Socket> socket);
 void CheckThroughput ();

 uint32_t port;
 uint32_t bytesTotal;
 uint32_t packetsReceived;

 std::string m_CSVfileName;
 int m_nSinks;
 std::string m_protocolName;
 double m_txp;
 bool m_traceMobility;
 uint32_t m_protocol;
};

RoutingExperiment::RoutingExperiment ()
 : port (9),
 bytesTotal (0),
 packetsReceived (0),
 m_CSVfileName ("manet-routing.output.csv"),
 m_traceMobility (false),
 m_protocol (2) // AODV
{
}

static inline std::string
PrintReceivedPacket (Ptr<Socket> socket, Ptr<Packet> packet, Address senderAddress)
```

```
{
 std::ostringstream oss;

 oss << Simulator::Now ().GetSeconds () << " " << socket->GetNode ()->GetId ();

 if (InetSocketAddress::IsMatchingType (senderAddress))
 {
 InetSocketAddress addr = InetSocketAddress::ConvertFrom (senderAddress);
 oss << " received one packet from " << addr.GetIpv4 ();
 }
 else
 {
 oss << " received one packet!";
 }
 return oss.str ();
}

void
RoutingExperiment::ReceivePacket (Ptr<Socket> socket)
{
 Ptr<Packet> packet;
 Address senderAddress;
 while ((packet = socket->RecvFrom (senderAddress)))
 {
 bytesTotal += packet->GetSize ();
 packetsReceived += 1;
 NS_LOG_UNCOND (PrintReceivedPacket (socket, packet, senderAddress));
 }
```

```
}

void
RoutingExperiment::CheckThroughput ()
{
 double kbs = (bytesTotal * 8.0) / 1000;
 bytesTotal = 0;

 std::ofstream out (m_CSVfileName.c_str (), std::ios::app);

 out << (Simulator::Now ()).GetSeconds () << ","
 << kbs << ","
 << packetsReceived << ","
 << m_nSinks << ","
 << m_protocolName << ","
 << m_txp << ""
 << std::endl;

 out.close ();
 packetsReceived = 0;
 Simulator::Schedule (Seconds (1.0), &RoutingExperiment::CheckThroughput, this);
}

Ptr<Socket>
RoutingExperiment::SetupPacketReceive (Ipv4Address addr, Ptr<Node> node)
{
 TypeId tid = TypeId::LookupByName ("ns3::UdpSocketFactory");
 Ptr<Socket> sink = Socket::CreateSocket (node, tid);
```

```
 InetSocketAddress local = InetSocketAddress (addr, port);
 sink->Bind (local);
 sink->SetRecvCallback (MakeCallback (&RoutingExperiment::ReceivePacket, this));

 return sink;
}

std::string
RoutingExperiment::CommandSetup (int argc, char **argv)
{
 CommandLine cmd (__FILE__);
 cmd.AddValue ("CSVfileName", "The name of the CSV output file name",
m_CSVfileName);
 cmd.AddValue ("traceMobility", "Enable mobility tracing", m_traceMobility);
 cmd.AddValue ("protocol", "1=OLSR;2=AODV;3=DSDV;4=DSR", m_protocol);
 cmd.Parse (argc, argv);
 return m_CSVfileName;
}

int
main (int argc, char *argv[])
{
 RoutingExperiment experiment;
 std::string CSVfileName = experiment.CommandSetup (argc,argv);

 //blank out the last output file and write the column headers
 std::ofstream out (CSVfileName.c_str ());
 out << "SimulationSecond," <<
```

```
 "ReceiveRate," <<
 "PacketsReceived," <<
 "NumberOfSinks," <<
 "RoutingProtocol," <<
 "TransmissionPower" <<
 std::endl;
 out.close ();

 int nSinks = 10;
 double txp = 7.5;

 experiment.Run (nSinks, txp, CSVfileName);
}

void
RoutingExperiment::Run (int nSinks, double txp, std::string CSVfileName)
{
 Packet::EnablePrinting ();
 m_nSinks = nSinks;
 m_txp = txp;
 m_CSVfileName = CSVfileName;

 int nWifis = 50;

 double TotalTime = 200.0;
 std::string rate ("2048bps");
 std::string phyMode ("DsssRate11Mbps");
 std::string tr_name ("manet-routing-compare");
```

```
int nodeSpeed = 20; //in m/s
int nodePause = 0; //in s
m_protocolName = "protocol";

Config::SetDefault ("ns3::OnOffApplication::PacketSize",StringValue ("64"));
Config::SetDefault ("ns3::OnOffApplication::DataRate", StringValue (rate));

//Set Non-unicastMode rate to unicast mode
Config::SetDefault ("ns3::WifiRemoteStationManager::NonUnicastMode",StringValue
(phyMode));

NodeContainer adhocNodes;
adhocNodes.Create (nWifis);

// setting up wifi phy and channel using helpers
WifiHelper wifi;
wifi.SetStandard (WIFI_STANDARD_80211b);

YansWifiPhyHelper wifiPhy;
YansWifiChannelHelper wifiChannel;
wifiChannel.SetPropagationDelay ("ns3::ConstantSpeedPropagationDelayModel");
wifiChannel.AddPropagationLoss ("ns3::FriisPropagationLossModel");
wifiPhy.SetChannel (wifiChannel.Create ());

// Add a mac and disable rate control
WifiMacHelper wifiMac;
wifi.SetRemoteStationManager ("ns3::ConstantRateWifiManager",
"DataMode",StringValue (phyMode),
```

```
"ControlMode",StringValue (phyMode));

wifiPhy.Set ("TxPowerStart",DoubleValue (txp));
wifiPhy.Set ("TxPowerEnd", DoubleValue (txp));

wifiMac.SetType ("ns3::AdhocWifiMac");
NetDeviceContainer adhocDevices = wifi.Install (wifiPhy, wifiMac, adhocNodes);

MobilityHelper mobilityAdhoc;
int64_t streamIndex = 0; // used to get consistent mobility across scenarios

ObjectFactory pos;
pos.SetTypeId ("ns3::RandomRectanglePositionAllocator");
pos.Set ("X", StringValue ("ns3::UniformRandomVariable[Min=0.0|Max=300.0]"));
pos.Set ("Y", StringValue ("ns3::UniformRandomVariable[Min=0.0|Max=1500.0]"));

Ptr<PositionAllocator> taPositionAlloc = pos.Create ()->GetObject<PositionAllocator> ();
streamIndex += taPositionAlloc->AssignStreams (streamIndex);

std::stringstream ssSpeed;
ssSpeed << "ns3::UniformRandomVariable[Min=0.0|Max=" << nodeSpeed << "]";
std::stringstream ssPause;
ssPause << "ns3::ConstantRandomVariable[Constant=" << nodePause << "]";
mobilityAdhoc.SetMobilityModel ("ns3::RandomWaypointMobilityModel",
"Speed", StringValue (ssSpeed.str ()),
"Pause", StringValue (ssPause.str ()),
"PositionAllocator", PointerValue (taPositionAlloc));
mobilityAdhoc.SetPositionAllocator (taPositionAlloc);
```

```
mobilityAdhoc.Install (adhocNodes);
streamIndex += mobilityAdhoc.AssignStreams (adhocNodes, streamIndex);
NS_UNUSED (streamIndex); // From this point, streamIndex is unused

AodvHelper aodv;
OlsrHelper olsr;
DsdvHelper dsdv;
DsrHelper dsr;
DsrMainHelper dsrMain;
Ipv4ListRoutingHelper list;
InternetStackHelper internet;

switch (m_protocol)
{
case 1:
list.Add (olsr, 100);
m_protocolName = "OLSR";
break;
case 2:
list.Add (aodv, 100);
m_protocolName = "AODV";
break;
case 3:
list.Add (dsdv, 100);
m_protocolName = "DSDV";
break;
case 4:
m_protocolName = "DSR";
```

```
  break;
  default:
  NS_FATAL_ERROR ("No such protocol:" << m_protocol);
  }

  if (m_protocol < 4)
  {
  internet.SetRoutingHelper (list);
  internet.Install (adhocNodes);
  }
  else if (m_protocol == 4)
  {
  internet.Install (adhocNodes);
  dsrMain.Install (dsr, adhocNodes);
  }

  NS_LOG_INFO ("assigning ip address");

  Ipv4AddressHelper addressAdhoc;
  addressAdhoc.SetBase ("10.1.1.0", "255.255.255.0");
  Ipv4InterfaceContainer adhocInterfaces;
  adhocInterfaces = addressAdhoc.Assign (adhocDevices);

  OnOffHelper onoff1 ("ns3::UdpSocketFactory",Address ());
  onoff1.SetAttribute ("OnTime", StringValue
("ns3::ConstantRandomVariable[Constant=1.0]"));
  onoff1.SetAttribute ("OffTime", StringValue
("ns3::ConstantRandomVariable[Constant=0.0]"));
```

```
  for (int i = 0; i < nSinks; i++)
  {
  Ptr<Socket> sink = SetupPacketReceive (adhocInterfaces.GetAddress (i), adhocNodes.Get
(i));

  AddressValue remoteAddress (InetSocketAddress (adhocInterfaces.GetAddress (i), port));
  onoff1.SetAttribute ("Remote", remoteAddress);

  Ptr<UniformRandomVariable> var = CreateObject<UniformRandomVariable> ();
  ApplicationContainer temp = onoff1.Install (adhocNodes.Get (i + nSinks));
  temp.Start (Seconds (var->GetValue (100.0,101.0)));
  temp.Stop (Seconds (TotalTime));
  }

  std::stringstream ss;
  ss << nWifis;
  std::string nodes = ss.str ();

  std::stringstream ss2;
  ss2 << nodeSpeed;
  std::string sNodeSpeed = ss2.str ();

  std::stringstream ss3;
  ss3 << nodePause;
  std::string sNodePause = ss3.str ();

  std::stringstream ss4;
```

```
  ss4 << rate;
  std::string sRate = ss4.str ();

  //NS_LOG_INFO ("Configure Tracing.");
  //tr_name = tr_name + "_" + m_protocolName +"_" + nodes + "nodes_" + sNodeSpeed +
"speed_" + sNodePause + "pause_" + sRate + "rate";

  //AsciiTraceHelper ascii;
  //Ptr<OutputStreamWrapper> osw = ascii.CreateFileStream ( (tr_name + ".tr").c_str());
  //wifiPhy.EnableAsciiAll (osw);
  AsciiTraceHelper ascii;
  MobilityHelper::EnableAsciiAll (ascii.CreateFileStream (tr_name + ".mob"));

  //Ptr<FlowMonitor> flowmon;
  //FlowMonitorHelper flowmonHelper;
  //flowmon = flowmonHelper.InstallAll ();


  NS_LOG_INFO ("Run Simulation.");

  CheckThroughput ();

  Simulator::Stop (Seconds (TotalTime));
  Simulator::Run ();
  //flowmon->SerializeToXmlFile ((tr_name + ".flowmon").c_str(), false, false);

  Simulator::Destroy ();
 }
```