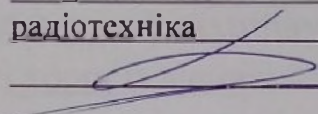


Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

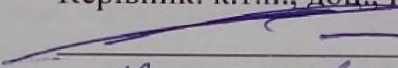
Бакалаврська кваліфікаційна робота на тему:

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ФУНКЦІОНУВАННЯ СПЕЦІАЛЬНИХ
МЕРЕЖ MANET В УМОВАХ ВИСОКОЇ ЩІЛЬНОСТІ КОРИСТУВАЧІВ

Виконав: студент 4-го курсу, групи ПЗТ-216
спеціальності 172 – Телекомунікації та
радіотехніка

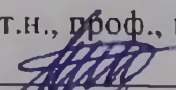
 Гамалєєв Д. Д.

Керівник: к.т.н., доц., професор каф. ІКСТ

 Барась С. Т.

« 12 » червня 2025 р.

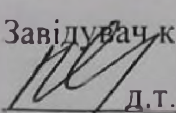
Рецензент: д.т.н., проф., професор каф. ІРТС

 Семенов А.О.

« 12 » червня 2025 р.

Допущено до захисту

Завідувач кафедри ІКСТ

 д.т.н., проф. Кичак В.М.

« 12 » червня 2025 р.

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем та технологій
Рівень вищої освіти перший (бакалаврський)
Галузь знань 17 – Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма – Програмне забезпечення телекомунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри ІКСТ

д.т.н., професор В.М. Кичак

«5» 05 2025 року

З А В Д А Н Н Я **НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ**

Гамалєсву Дмитру Дмитровичу

(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів

керівник роботи Барась Святослав Тадіонович, канд. техн. наук, доцент.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНТУ від “20” березня 2025 року № 97

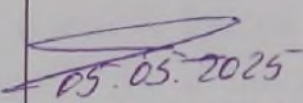
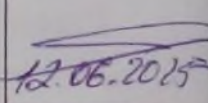
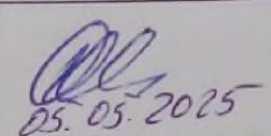
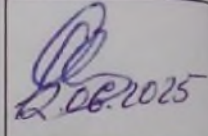
2. Строк подання здобувачем роботи: 09 червня 2025 року

3. Вихідні дані до роботи: Робочі частоти 2,4 та 5 ГГц, 800-900 МГц; адаптація до стандарту 802.11s; протоколи маршрутизації OLSR, AODV, DSR, TORA, MAODV; множинний доступ з ортогональним частотним розділенням каналів – до 9 користувачів на діапазоні 20 МГц; базовий механізм енергозбереження; моделювання мережі з 4 вузлів.

4. Зміст розрахунково-пояснювальної записки роботи (перелік питань, які потрібно розробити): вступ, загальна характеристика радіомережі MANET, протоколи багатошляхової маршрутизації в MANET, множинний доступ з ортогональним частотним розділенням каналів, механізми енергозбереження, підвищення стійкості передачі даних в мережах MANET, охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): архітектура - режим з точкою доступу, архітектура - режим без точки доступу, топологія мережі MANET, протоколи маршрутизації MANET, OFDMA у низхідному каналі, передача OFDMA по висхідній лінії зв'язку, діаграма базового механізму енергозбереження, результати моделювання: динаміка швидкості передачі на першому вузлі, вільний простір у буфері третього вузла.

6. Консультанти розділів роботи

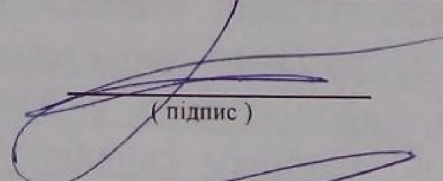
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання пр
Спеціальна частина	Барась С. Т., професор кафедри ІКСТ	 05.05.2025	 12.06.2025
Охорона праці	Дембіцька С. В. проф. каф. БЖДПБ	 05.05.2025	 12.06.2025

7. Дата видачі завдання «05» травня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

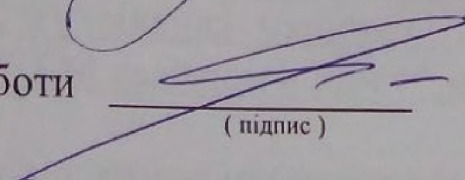
№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	При
1	Формування та затвердження теми та індивідуального завдання бакалаврської кваліфікаційної роботи (БКР)	06.05.2025р.	
2	Виконання спеціальної частини БКР. Перший рубіжний контроль виконання БКР	19.05.2025р.	
3	Виконання спеціальної частини БКР. Другий рубіжний контроль виконання БКР	02.06.2025р.	
4	Виконання розділу «Охорона праці»	06.06.2025р.	
5	Нормоконтроль БКР	09.06.2025р.	
6	Попередній захист БКР	10.06.2025р.	
7	Рецензування БКР	11.06.2025р.	
8	Захист БКР	13.06.2025р.	

Студент


(підпис)

Гамалєєв Д. Д.

Керівник роботи


(підпис)

Барась С. Т.

АНОТАЦІЯ

УДК 621.391.8

Гамалєєв Д. Д. Дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів. Бакалаврська кваліфікаційна робота зі спеціальності 172 – телекомунікації та радіотехніка, освітня програма – програмне забезпечення телекомунікаційних систем. Вінниця: ВНТУ, 2025. 99 с.

На укр. мові. Бібліогр.: 37 назв; рис.: 23; табл. 9.

Робота присвячена дослідженню ефективності алгоритмів маршрутизації, технологій множинного доступу до каналів передачі та енергозбереження у безпроводній мережі радіодоступу MANET, яка працює в умовах значної щільності користувачів.

Метою дослідження є оцінка ефективності алгоритмів функціонування спеціальних мереж MANET при виконанні ними тактичних задач в умовах високої щільності користувачів.

Основними завданнями роботи є аналіз характеристик самоорганізованої мережі MANET, дослідження у такій мережі ефективності протоколів багатошляхової маршрутизації, оцінка ефективності множинного доступу з ортогональним частотним розділенням каналів, аналіз діючих механізмів енергозбереження.

Робота містить шість розділів. У першому розділі виконано аналіз характеристик радіомережі MANET та сфер її застосування.

У другому розділі досліджені протоколи багатошляхової маршрутизації в MANET.

У третьому розділі дана оцінка множинного доступу в умовах значної щільності користувачів.

У четвертому розділі виконано аналіз механізмів енергозбереження.

У п'ятому розділі розглянуті питання підвищення стійкості передачі даних у мережах MANET.

У шостому розділі виконано розрахунки, які стосуються охорони праці та безпеки життєдіяльності.

Ключові слова: мережа MANET, алгоритми маршрутизації, множинний доступ, енергозбереження, моделювання, охорона праці.

ABSTRACT

Gamaleev D. D. Research of algorithms of functioning of special networks MANET in conditions of high density of users. Bachelor's qualification work in specialty 172 – telecommunications and radio engineering, educational program – software of telecommunications systems. Vinnytsia: VNTU, 2025. 99 p.

In Ukrainian. Bibliography: 37 titles; fig.: 23; tab. 9.

The work is devoted to research of efficiency of routing algorithms, technologies of multiple access to transmission channels and energy saving in wireless radio access network MANET, which operates in conditions of significant density of users.

The purpose of the research is to assess efficiency of algorithms of functioning of special networks MANET when they perform tactical tasks in conditions of high density of users.

The main objectives of the work are to analyze the characteristics of a self-organized MANET network, to study the effectiveness of multipath routing protocols in such a network, to evaluate the effectiveness of multiple access with orthogonal frequency division of channels, and to analyze existing energy saving mechanisms.

The work contains six sections. The first section analyzes the characteristics of the MANET radio network and its areas of application.

The second section examines multipath routing protocols in MANET.

The third section evaluates multiple access under conditions of significant user density.

The fourth section analyzes energy saving mechanisms.

The fifth section considers issues of increasing the stability of data transmission in MANET networks.

The sixth section performs calculations related to occupational health and safety.

Keywords: MANET network, routing algorithms, multiple access, energy saving, modeling, occupational safety.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП	6
1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА РАДІОМЕРЕЖІ MANET	8
1.1 Класифікація безпроводних мереж	10
1.2 Побудова мережі MANET	11
1.3 Сфери застосування MANET	13
1.4 Важливі аспекти функціонування мережі MANET	16
1.4.1 Стандарти	16
1.4.2 Програмне забезпечення	19
1.4.3 З'єднання MANET з Інтернет.....	20
1.4.4 Повністю автономна MANET	22
1.5 Висновки до розділу	25
2 ПРОТОКОЛИ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ В MANET ...	26
2.1 Протокол OLSR	28
2.2 Протокол AODV	30
2.3 Протокол DSR	33
2.4 Протокол TORA	35
2.5 Протокол MAODV	36
2.6 Оцінка ефективності протоколів маршрутизації в мережі MANET	37
2.7 Висновки до розділу	45
3 МНОЖИННИЙ ДОСТУП З ОРТОГОНАЛЬНИМ ЧАСТОТНИМ РОЗДІЛЕННЯМ КАНАЛІВ	47
3.1 Висновки до розділу	54
4 МЕХАНІЗМИ ЕНЕРГОЗБЕРЕЖЕННЯ	55
4.1 Базовий механізм енергозбереження	56
4.2 Target Wake Time	59
4.3 Технологія Wake-Up Radio	61
4.4 Висновки до розділу	62

5	ПІДВИЩЕННЯ СТІЙКОСТІ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ MANET.....	64
5.1	Транспортні протоколи в мережах MANET.....	64
5.2	Керування передачею та надійність в мережах MANET.....	66
5.3	Моделювання роботи протоколу передачі даних у мережі MANET.....	69
5.4	Висновки до розділу	73
6	ОХОРОНА ПРАЦІ	74
6.1	Технічні рішення щодо безпечного виконання роботи.....	75
6.2	Технічні рішення з гігієни праці та виробничої санітарії.....	77
6.2.1	Мікроклімат.....	77
6.2.2	Склад повітря робочої зони.....	78
6.2.3	Виробниче освітлення.....	79
6.2.4	Виробничий шум.....	80
6.2.5	Виробничі випромінювання.....	81
6.3	Пожежна безпека.....	82
6.3.1	Технічні рішення системи запобігання пожежі	82
6.3.2	Технічні рішення системи протипожежного захисту.....	83
6.4	Висновки до розділу.....	85
	ВИСНОВКИ	86
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	88
	Додаток А (обов'язковий) - Ілюстративний матеріал	92
	Додаток Б – Протокол перевірки кваліфікаційної роботи	99

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- AODV - Ad-hoc On-demand Distance Vector (протокол динамічної маршрутизації для мобільних ad-hoc мереж (MANET) та інших безпроводних мереж)
- BSS – Base Station Subsystem (підсистема базових станцій)
- DSR - Dynamic Source Routing (протокол маршрутизації для MANET з топологією mesh)
- DTIM - Delivery Traffic Indication Map (доставка карти індикації трафіка)
- GRPH - Group Hello (групі привіт)
- IBSS (Independent Basis Service Set) (базовий набір служб)
- MAC – Media Access Control (керування доступом)
- MACT - Multicast Activation (багатоадресна активація)
- MANET - Mobile ad hoc network (безпроводна децентралізована самоорганізована мережа, вузлами якої є випадкові мобільні пристрої)
- MAODV - Multicast AODV (реактивний протокол маршрутизації)
- MP - Mesh Point (вузол комірчастої мережі)
- NAV — (віртуальна зайнятість середовища)
- NOMA - Non-orthogonal multiple access (неортогональний множинний доступ)
- OFDM - orthogonal frequency division multiplexin (ортогональне мультиплексування із частотним розділенням)
- OFDMA - orthogonal frequency division multiple access (ортогональний множинний доступ із частотним поділом)
- OLSR - Optimized Link State Routing (протокол маршрутизації, оптимізований для мобільних однорангових мереж)
- OMA - Orthogonal multiple access (ортогональний множинний доступ)
- PSM - Power Save Mode (режим енергозбереження)
- RREP - Route Reply (маршрут відповіді)
- RREQ - Route Request (запит маршруту)
- RTS - Request To Send (запит на передачу)

RUs - Resource Units (ресурсні блоки)

SD - Signal detection (виявлення сигналу)

SIFS – Short Interframe Space (часовий інтервал, короткий міжкадровий простір)

SON - self-organization network (самоорганізовані мережі)

STA – Stations (безпроводні станції)

TIM – Traffic Identification Message (періодичне сповіщення)

TIM - Traffic Indication Map (карта індикації трафіка)

TORA - Temporally-Ordered Routing Algorithm (протокол маршрутизації, який повністю використовує топологію зони маршрутизації)

TWT – Target Wake Time (цільовий час пробудження)

WAP – Wireless Access Point (точка безпроводного доступу)

WMN - Wireless mesh network (безпроводні mesh-мережі)

WUR - Wake-Up Radio (радіомодуль для пробудження, вторинний малопотужний модуль)

ГДК - гранично допустима концентрація

ЕМП - електромагнітне поле

КПО – коефіцієнт природного освітлення

МБС - мережі мобільних базових станцій

МК (КМ) – мобільний користувач

ПК – персональний комп'ютер

ВСТУП

Актуальність теми. Мобільні мережі Ad Hoc, як показують дослідження [1-5], найчастіше використовуються для налагодження зв'язку в умовах бойових дій. Це включає забезпечення комунікації між піхотинцями, наземним і повітряним транспортом, причому більшість учасників мережі переміщуються з різною швидкістю. У таких динамічних і непередбачуваних ситуаціях традиційні мережі з фіксованою інфраструктурою не здатні гарантувати стабільний зв'язок. Системні адміністратори мають обмаль часу для оперативного реагування та переналаштування мережі. Натомість, мережі MANET зазвичай не потребують адміністрування. Тимчасові мережі Ad Hoc є оптимальним рішенням, коли створення стаціонарної інфраструктури неможливе або недоцільне. Прикладами такого застосування можуть бути конференції як тимчасове рішення, а також віддалені або важкодоступні локації. Швидкість розгортання мереж Ad Hoc робить їх критично важливими під час рятувальних операцій після катастроф і стихійних лих [2-4].

На відміну від мереж з ієрархічною структурою та централізованим керуванням, однорангові мережі без інфраструктури (MANET) складаються з рівноправних вузлів. Кожен вузол оснащений необхідним програмно-апаратним забезпеченням для прямої передачі даних між джерелом і отримувачем за наявності фізичного шляху. Такий підхід дозволяє розподілити навантаження та збільшити загальну пропускну здатність мережі. Передача даних можлива навіть між вузлами, що знаходяться поза прямою радіовидимістю – у цьому випадку пакети ретранслюються проміжними вузлами, які мають зв'язок з обома абонентами. Такі мережі з багаторазовою ретрансляцією називаються багатострибковими (multihop). Ключовими проблемами при розробці таких мереж є маршрутизація пакетів, масштабування, адресація пристроїв і підтримка зв'язку при змінній топології. В умовах високої щільності користувачів важливими стають питання ефективного доступу до каналів передачі та енергозбереження. Тому

актуальним є дослідження комплексу алгоритмів, що використовуються в мережах MANET, яке й проводиться в цій роботі.

Аналіз останніх досліджень. Відомо, що сучасні принципи організації зв'язку і технічне оснащення підрозділів зв'язку ЗСУ не дозволяють цілком задовольнити потреби управління військами в умовах сучасного бою. Основними недоліками існуючої системи зв'язку тактичної ланки управління є: низька мобільність вузлів зв'язку пунктів управління; невиконання вимог продуктивності, надійності, розвідзахищеності, забезпечення радіозв'язку між мобільними абонентами тощо. Тобто розробка нових підходів по створенню системи зв'язку тактичного рівня, яка б відповідала вимогам сьогодення, є актуальною науковою проблемою [6]. Це стосується таких алгоритмів і технологій як протоколи маршрутизації, OFDMA, Resource Units, Target Wait Time (TWT), Wake-Up Radio (WUR) [3-6].

Мета та постановка задачі. Метою даної бакалаврської кваліфікаційної роботи є оцінка ефективності алгоритмів функціонування спеціальних мереж MANET при виконанні ними тактичних задач в умовах високої щільності користувачів.

Задачами бакалаврської кваліфікаційної роботи є:

- аналіз загальних характеристик радіомережі MANET;
- дослідження протоколів багатошляхової маршрутизації та оцінка їх ефективності;
- аналіз функціонування алгоритму OFDMA в мережі MANET;
- оцінка механізмів енергозбереження;
- моделювання підвищення стійкості передачі даних в мережах MANET;
- розрахунки параметрів з охорони праці.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на науковій конференції ВНТУ у 2025 році.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА РАДІОМЕРЕЖІ MANET

Різні версії стандарту Wi-Fi 802.11 визначають фізичний (PHY) та MAC (Medium Access Control) рівні. При цьому верхні рівні є спільними як для бездротових, так і для провідних локальних мереж. Фізичний рівень відповідає за спосіб передачі даних, швидкість та методи модуляції. Підрівень MAC контролює розподіл каналу, визначаючи, яка станція передаватиме наступною, а також принципи використання спільного каналу, механізми аутентифікації та шифрування. Оскільки стандарт 802.11 розроблявся як бездротовий Ethernet, він використовує пакетну передачу з 48-бітними адресами, подібно до звичайних мереж Ethernet. Завдяки комітету IEEE 802 забезпечується сумісність усіх стандартів, що дозволяє легко інтегрувати бездротові мережі 802.11 з провідними мережами Ethernet.

Стандарт 802.11 передбачає два основні режими організації мережі:

- з використанням базової станції (точки доступу AP). У цьому режимі зв'язок між пристроями відбувається виключно через AP, яка також може забезпечувати вихід у зовнішні провідні мережі, наприклад, для доступу до Інтернету, рис. 1а. Такі мережі називаються структурованими або інфраструктурними та часто використовуються для передачі мультимедійного контенту. Мережа може включати кілька точок доступу, об'єднаних провідною мережею Ethernet, утворюючи набір зон покриття, що перетинаються, рис. 1б. Точки доступу можуть мати доступ до Інтернету через бездротову мережу WiMAX.

- без базової станції (Ad Hoc). Цей режим передбачає прямий зв'язок між рівноправними бездротовими клієнтами, утворюючи незалежний базовий набір служб IBSS. Такі мережі називаються самоорганізованими безпроводними мережами Ad Hoc (від англійського "for this purpose" - цільові), рис. 1.2.

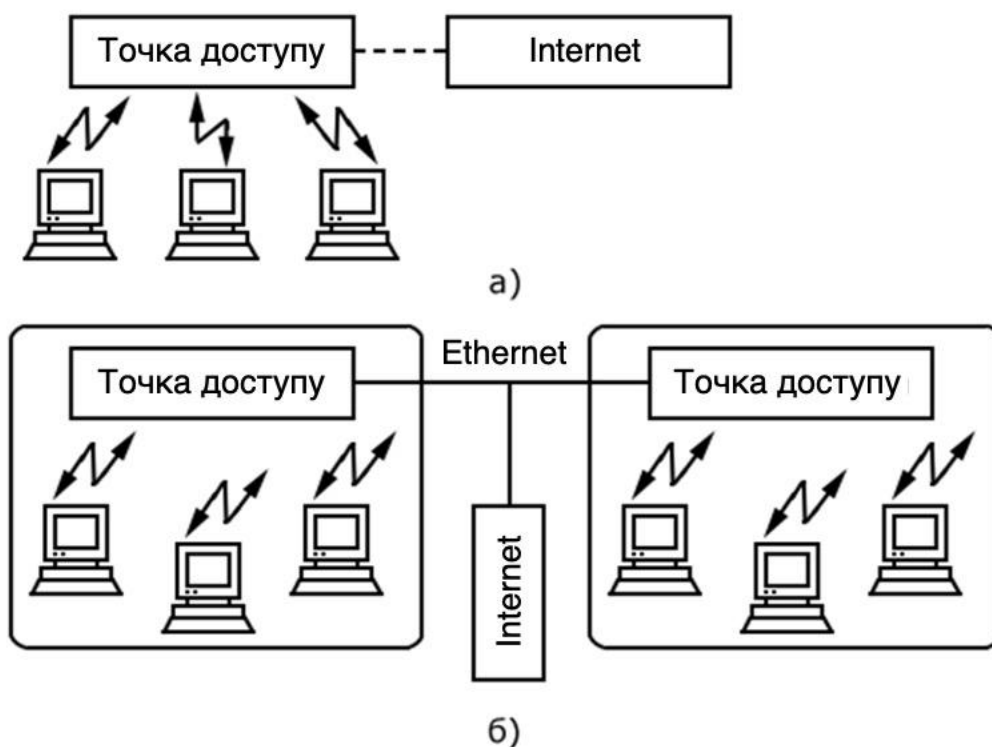


Рисунок 1.1 – Режим з точкою доступу

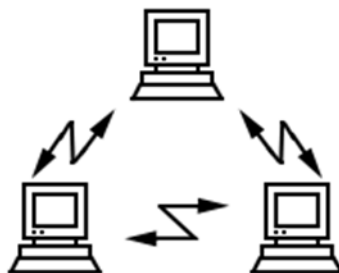


Рисунок 1.2 – Режим без точки доступу (мережа Ad Hoc)

Мобільна мережа Ad Hoc (MANET) являє собою розподілену систему, що складається з мобільних пристроїв, обладнаних приймально-передавачами [7], які здатні динамічно формувати тимчасові мережі. В MANET мобільні пристрої виконують подвійну роль: вони є як кінцевими станціями, так і мережевими вузлами, які функціонують як маршрутизатори.

Стандарт 802.11s розроблено для бездротових mesh-мереж (WMN). Основна відмінність між WMN і MANET полягає в тому, що WMN додатково включає окрему опорну мережу (backbone) з маршрутизаторів, яка, як правило,

є фіксованою. Обидва типи мереж – MANET і WMN – є багатострибковими (multihop) і можуть оперативно розгортатися в екстрених ситуаціях [8].

1.1 Класифікація безпроводних мереж

Одним зі способів класифікації безпроводних мереж є поділ на мережі з централізованою інфраструктурою та самоорганізовані мережі.

Інфраструктурна мережа використовує точку доступу для керування обміном даними в межах зони її покриття. Точка доступу визначає, яким вузлам дозволено встановлювати зв'язок і коли. Цей режим є найбільш поширеним. У таких мережах безпроводні пристрої не можуть безпосередньо взаємодіяти один з одним – їм потрібен дозвіл від точки доступу, яка контролює всі взаємодії та забезпечує рівний доступ до мережі для всіх пристроїв.

На відміну від них, самоорганізовані мережі (SON) дозволяють будь-якій парі вузлів обмінюватися даними без необхідності централізованої інфраструктури. Вузли в SON можуть одночасно виступати як кінцеві пристрої та маршрутизатори. З'єднання на великі відстані встановлюються за допомогою спеціальних протоколів маршрутизації через проміжні вузли-маршрутизатори. Таке з'єднання називається багатетапним або багатокроковим (multihop), де кожен етап являє собою участь одного вузла-маршрутизатора в передачі.

Найпростішим прикладом самоорганізованої мережі є ad-hoc мережа, яка створюється шляхом об'єднання двох або більше бездротових клієнтів без використання точки доступу. У мережі ad-hoc усі клієнти є рівноправними, що спрощує обмін файлами та інформацією між пристроями, оскільки не потребує витрат і складнощів, пов'язаних з придбанням та налаштуванням точки доступу.

До класу SON відносять такі мережі:

- мобільні цільові (спеціальні) Ad Hoc мережі – Wireless Mobile Ad Hoc Network (MANET);
- безпроводні сенсорні мережі – Wireless Sensor Network (WSN);

- безпроводні mesh-мережі Wireless Mesh Network (WMN). Ці мережі називають також комірковими мережами.

- автомобільні безпроводні мережі Vehicular Ad Hoc Network (VANET).

Вузли зазначених мереж взаємно формують мережу та їм властиво пошук і знаходження один одного. Якщо має місце вихід з ладу будь-якого вузла, то можуть встановлюватися нові маршрути для передачі повідомлень.

Дане дослідження торкається мереж MANET.

1.2 Побудова мережі MANET

Mobile Ad-hoc NETwork (MANET) – це безпроводна, децентралізована та самоорганізована мережа, вузлами якої є мобільні пристрої, що можуть довільно змінювати своє положення. Керування цими пристроями здійснюється без використання базових станцій або опорних вузлів, як показано на рис. 1.3.

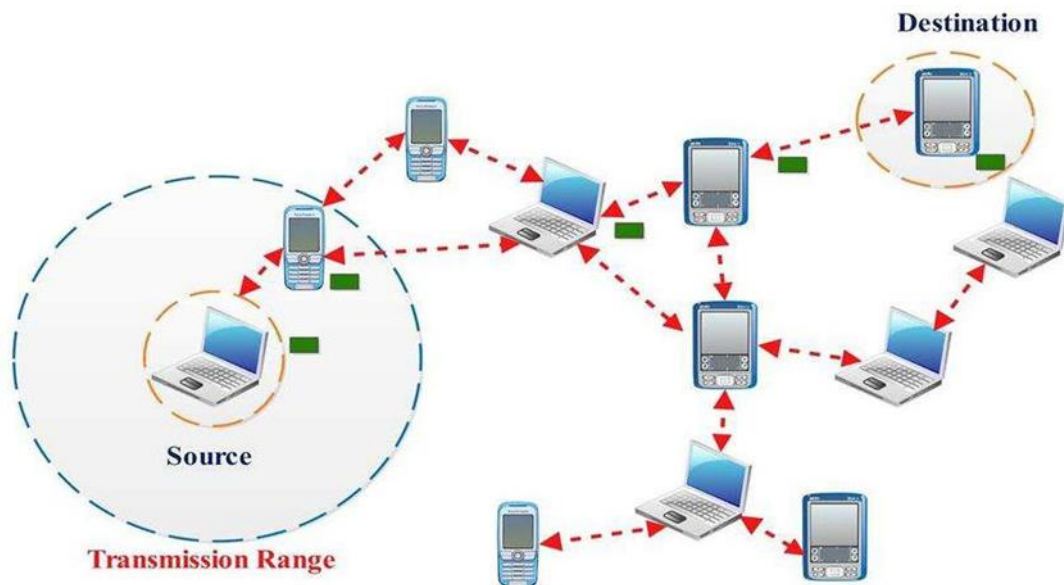


Рисунок 1.3 – Топологія мережі MANET

MANET є розподіленою системою, що складається з мобільних терміналів, оснащених приймально-передавачами [5], які здатні динамічно формувати тимчасові мережі. У таких мережах мобільні пристрої виконують

функції не лише кінцевих станцій, але й мережесих вузлів, відповідальних за маршрутизацію трафіку.

Зазвичай, такі мережі не потребують адміністрування. Передача даних між терміналами, що знаходяться поза зоною прямого радіозв'язку, відбувається через послідовність проміжних маршрутизаторів. На відміну від мереж з точкою доступу, MANET є багатокроковою (multihop) і може бути підключена до фіксованої мережі за допомогою шлюзів.

Мережі MANET характеризуються низкою особливостей [1]:

- Висока динамічність топології: Мобільність вузлів додає ще один рівень складності до змін у структурі мережі, оскільки зв'язок може обриватися не лише через перешкоди або вимкнення пристроїв, але й через їх переміщення.
- Обмеженість енергоресурсів: При розробці протоколів і обладнання необхідно враховувати енергоспоживання мобільних пристроїв, оскільки їхні джерела живлення можуть мати обмежений запас.

Водночас, MANET-мережі мають певні переваги над безпроводними мережами традиційної архітектури [1]:

- Стійкість до змін інфраструктури: Відсутність централізованої інфраструктури робить мережу менш вразливою до її пошкоджень або змін.
- Простота та швидкість розгортання: MANET можуть бути швидко розгорнуті без необхідності попереднього встановлення складної інфраструктури.
- Можливість передачі на великі відстані: Завдяки багатокроковій передачі, зв'язок може бути встановлений між віддаленими вузлами без збільшення потужності передавачів.
- Швидка реконфігурація: Мережа здатна оперативно адаптуватися до змін умов, наприклад, при виникненні сильних перешкод.

Для MANET-мереж існує кілька основних класів проблем [2], серед яких: забезпечення завадостійкості та безпеки переданих даних, обмежена загальна

пропускна здатність мережі та ефективність використовуваних методів маршрутизації.

Особливо актуальною є проблема роботи безпроводних систем в умовах високої щільності користувачів. Велика кількість пристроїв, що підключаються до мережі, може призвести до погіршення якості обслуговування, збоїв зв'язку та зниження продуктивності. Важливо зазначити, що вплив високої щільності користувачів накладається на інші типові проблеми, характерні для роботи пристроїв Wi-Fi.

1.3 Сфери застосування MANET

Мобільні мережі Ad Hoc найчастіше розглядаються як засіб налагодження зв'язку під час бойових дій або рятувальних операцій після катастроф чи стихійних лих. Більшість розвинених країн світу вивчають перспективи застосування самоорганізованих радіомереж у контексті систем зв'язку тактичного та оперативно-тактичного рівнів у військових підрозділах [8].

Сучасні тактичні мережі зв'язку характеризуються такими особливостями:

- Динамічна топологія: Вузли мережі є мобільними, схильними до знищення та відмов. Радіоканали нестабільні, мають обмежену дальність зв'язку та пропускну здатність через вплив радіоелектронної протидії противника, взаємних перешкод, умов поширення радіохвиль тощо.
- Обмежені енергоресурси: Абоненти, оснащені радіотерміналами з акумуляторними батареями, мають обмежену потужність і час передачі.
- Значна розмірність мереж: Спостерігається висока щільність користувачів, яка може сягати сотень або тисяч елементів.
- Неоднорідність елементів мережі: Елементи відрізняються за мобільністю (танк, солдат, вертоліт, літак) та рівнем продуктивності (мобільна базова станція, мобільний абонент).

Водночас, основні технічні вимоги до систем зв'язку наступного покоління включають:

- Інтеграцію всіх видів трафіку (голос, дані, відео, відеоконференція).
- Повну мобільність усіх абонентів та елементів мережі.
- Забезпечення заданої якості обслуговування (QoS) на значних географічних територіях в умовах застосування як звичайної, так і зброї масового ураження (ядерної, біологічної, хімічної).
- Гарантовану конфіденційність усіх видів інформації.
- Мінімальну участь людини в процесах планування та управління зв'язком.

Проведений аналіз можливих варіантів побудови архітектури мереж тактичної ланки показав переваги використання мобільних радіомереж (MANET) порівняно зі стільниковими або транкінговими мережами, як ілюструє рисунок 1.4.

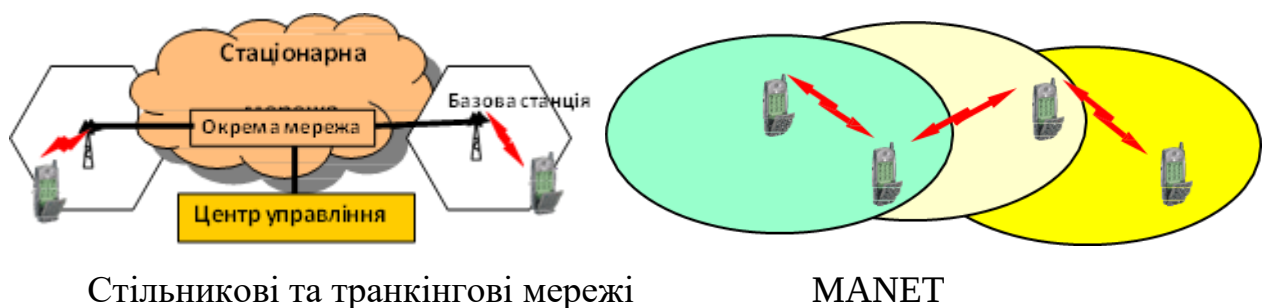


Рисунок 1.4 – Побудова стільникових (транкінгових) та мобільних мереж

Таблиця 1.1 ілюструє ключові відмінності між стільниковими, транкінговими та мобільними радіомережами.

MANET являє собою динамічну, самоорганізовану мережеву архітектуру без базових станцій та фіксованих маршрутів передачі інформації [3]. Вузлом такої мережі є термінал, оснащений радіомодемом (наприклад, переносний комп'ютер, персональний секретар, сенсорний пристрій, робот), який виконує функції як кінцевого пристрою, так і маршрутизатора. Для цих мереж

характерна випадкова топологія, мобільність усіх елементів, принцип передачі інформації на основі комутації повідомлень (пакетів) та децентралізований тип управління.

Таблиця 1.1 – Відмінності між стільниковими, транкінговими та мобільними радіомережами

Характеристика	Стільникові мережі	Транкінгові мережі	Мобільні радіомережі
Архітектура	Фіксована стільникова: фіксовані зони обслуговування, стаціонарні базові станції		Відсутність фіксованої інфраструктури, кожен вузол являє собою ретранслятор (маршрутизатор) повідомлень
	Використання стаціонарної мережі загального користування	Використання фіксованої мережі для з'єднання базових станцій	
Тип топології	Статична (базові станції статичні)		Випадкова, високо динамічна, адаптація топології до умов функціонування
Час розгортання	Дуже великий	Значний	Швидке розгортання, самоорганізація мережі, легке нарощування
	Необхідний етап проектування (планування) мережі	Необхідний етап планування мережі	
Тип управління	Централізований, наявність окремої (виділеної) мережі управління		Децентралізований, не має виділеної мережі управління
Мобільність	Мобільні тільки абоненти в межах зон покриття стаціонарними базовими станціями		Мобільні всі елементи мережі
Живучість	Дуже низька		Дуже висока
Розвідзахищеність	Низька		Висока
Швидкість перед.	Мала – GPRS (од.-дес. Кб/с)		Висока до Гб/с
Сфера застосування	Тилові підрозділи, антитерористичні операції		Поле бою, надзвичайні ситуації

Мобільна складова системи зв'язку призначена для забезпечення обміну інформацією між усіма військовими підрозділами, що діють у тактичній зоні, незалежно від їхньої підпорядкованості та виконуваних завдань. Її архітектура передбачається неоднорідною та ієрархічною, що складається з трьох основних рівнів, як показано на рисунку 1.5:

1. Мобільні радіомережі низової ланки управління.
2. Мережі мобільних базових станцій (МБС), що формують опорну мережу.
3. Повітряна мережа на базі безпілотних літальних апаратів [9].

Додатковий нульовий рівень можуть утворювати сенсорні мережі (мережі телеметрії). Створення кожного рівня спрямоване на покращення загальних показників якості функціонування всієї системи зв'язку. Важливо зазначити, що кожен рівень мобільної компоненти використовує власний піддіапазон частот.

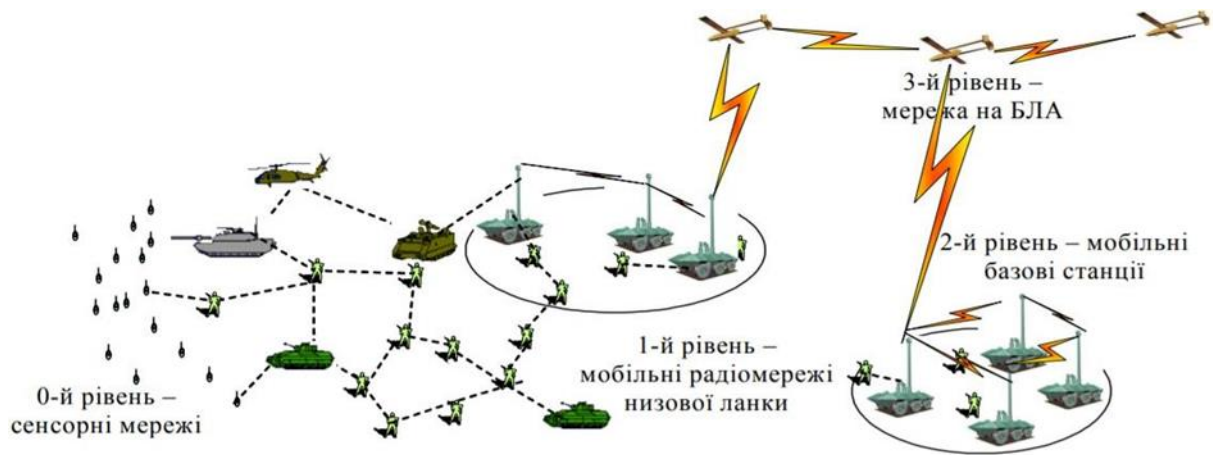


Рисунок 1.5 - Перспективна архітектура мобільної компоненти зв'язку

Перший рівень – це об'єднання MANET низової ланки управління. Мобільні учасники мережі (солдати, танки, вертольоти тощо) обладнані радіотерміналами з приймально-передавальними модулями, які виконують функції маршрутизації. Інформаційний обмін між учасниками відбувається безпосередньо або з використанням ретрансляції (маршрутизації) повідомлень. У ролі ретранслятора (маршрутизатора) може виступати будь-який мобільний учасник цього ж рівня або мобільна базова станція (МБС) – елемент другого рівня ієрархії, якщо вона знаходиться в зоні радіозв'язку.

1.4 Важливі аспекти функціонування мережі MANET

1.4.1 Стандарти

Функціонування мереж MANET регламентується кількома основними стандартами і протоколами, які сприяють ефективному обміну даними та комунікації в умовах мобільних, безпроводних мереж. Ці стандарти та

протоколи разом дозволяють забезпечити надійний зв'язок і ефективно функціонування мереж MANET, що є важливим для різних застосунків, таких як військові, аварійні та інші специфічні мобільні мережі.

Стандарт IEEE 802.11 (Wi-Fi) є основою для безпроводних локальних мереж (WLAN) і використовується в MANET для забезпечення зв'язку між мобільними пристроями. Зокрема, Wi-Fi має великий вплив на з'єднання в межах MANET.

Стандарт IEEE 802.15.1 (Bluetooth) для безпроводних персональних мереж (WPAN), який також може використовуватися в MANET для комунікації між мобільними пристроями на коротких відстанях.

Але річ у тому, що IEEE 802.11 не розроблявся для мереж типу MANET. Він розроблявся для mesh-мереж (див. вище визначення) та має ієрархічний принцип побудови. Те саме стосується технології Bluetooth, де завжди є один координатор, який роздає тайм-слоти та керує доступом до каналу. Абоненти завжди спілкуються через координатора. Координатори можуть утворювати між собою scatternet, але реально це не працює. Bluetooth 4.0, відомий як Bluetooth Low Energy, взагалі призначений для передачі «раз на годину» пакетів довжини не більше 20 байт прикладних даних [4]. Тож він фізично не підходить для високошвидкісних сервісів.

Стандарт IEEE 802.16 (Wimax) забезпечує широкосмуговий безпроводний доступ до Інтернету та може бути застосований для забезпечення зв'язку в більш великих MANET або в гібридних мережах.

Набір рекомендацій щодо проектування та функціонування MANET IETF RFC 2501 описує основні концепції, протоколи та технології для забезпечення комунікацій в умовах, коли мережа постійно змінюється через рух мобільних пристроїв.

Найбільш рекомендовані протоколи маршрутизації також відносяться до групи стандартів цієї технології. Протокол маршрутизації для MANET AODV (Ad-hoc On-demand Distance Vector), який дозволяє ефективно передавати дані в мережах, які динамічно змінюються. AODV визначає процес пошуку маршруту

за запитом та забезпечує ефективне керування маршрутизацією в мережах з мобільними вузлами.

Ще один протокол маршрутизації для MANET OLSR (Optimized Link State Routing), який працює на основі стану лінії зв'язку. Він дозволяє швидко визначати оптимальні маршрути і забезпечує стабільність маршрутизації в умовах змінюваної топології мережі.

Протокол маршрутизації DSR (Dynamic Source Routing) на основі джерела, який використовує інформацію про маршрути без необхідності підтримувати таблиці маршрутизації на кожному вузлі. Це дозволяє кожному вузлу визначати шлях для передачі даних до кінцевої точки.

Протокол маршрутизації TORA (Temporally-Ordered Routing Algorithm), орієнтований на адаптивність до змін у топології, використовуючи тимчасову орієнтацію для формування маршруту.

Прийнято ділити протоколи маршрутизації на проактивні (табличні), реактивні (зондові) та їх гібриди. Є багато робіт [6-9], де пропонуються десятки протоколів маршрутизації для радіомереж, що самоорганізуються. Проблема, однак, полягає в тому, що реально розроблені протоколи маршрутизації мереж MANET або не реалізовані фізично в мові C, або орієнтовані на досягнення оптимального використання мережевих ресурсів за квазістатичних умов роботи мережі, тобто коли топологія змінюється повільно чи взагалі не змінюється. Останнє є актуальним для таблично-орієнтованих протоколів типу OLSR, DSDV, WRP, BATMAN, Babel тощо.

Ці протоколи мають на увазі наявність у маршрутних таблицях інформації про всю мережу відразу. Коротше кажучи, вони постійно будують маршрути до всіх відомих їм вузлів, незалежно від того, чи потрібен нам цей абонент чи ні. Отже, створюється необхідність у генерації неінформативного трафіку у мережі.

Зондові протоколи AODV, DSR, SSR, TORA, передбачають маршрутизацію за запитом. До того ж через несиметричні канали маршрутизація повинна підтримувати режим побудови безлічі маршрутів як від

адресата до одержувача, так і у зворотному напрямку. А це підтримують лише протоколи DSR та TORA.

1.4.2 Програмне забезпечення

Для функціонування мереж MANET необхідне спеціалізоване програмне забезпечення, яке забезпечує ефективну маршрутизацію, управління зв'язком, моніторинг стану мережі та забезпечення безпеки. Основні типи програмного забезпечення та протоколів, що використовуються в MANET.

1. Програмне забезпечення для маршрутизації.

Враховуючи, що в MANET мережа змінюється динамічно, важливо мати протоколи маршрутизації, які адаптуються до змін у топології мережі. Найпоширенішими для мережі MANET, як було зазначено вище, вважаються протоколи AODV, OLSR, DSR, TORA.

2. Програмне забезпечення для моніторингу та управління мережею.

Популярний мережевий аналізатор Wireshark, який використовується для моніторингу трафіку в MANET. Він дозволяє відслідковувати пакети даних, що передаються по мережі, і аналізувати проблеми з маршрутизацією, пропускнуою здатністю, затримками тощо.

Потужний симулятор мереж NS-3 (Network Simulator 3), який дозволяє моделювати поведінку MANET, тестувати різні протоколи маршрутизації та оптимізації. NS-3 широко використовується в академічних і дослідницьких цілях для аналізу ефективності різних рішень для MANET.

Популярний симулятор для моделювання мереж OMNeT++, включаючи і MANET. Він дозволяє створювати складні мережеві топології і тестувати протоколи маршрутизації, вплив мобільності вузлів та інші аспекти.

Програмне забезпечення для тестування і моніторингу мобільних мереж MONROE (Mobile Network Observatory), яке допомагає вивчати характеристики MANET, зокрема, ефективність маршрутизації, стабільність зв'язку та інші параметри.

3. Програмне забезпечення для безпеки мережі.

Безпека в MANET є критичним аспектом, оскільки ці мережі часто працюють в умовах безпроводної передачі даних і відкритого середовища. Для забезпечення безпеки використовуються різні рішення.

Протокол IPsec (Internet Protocol Security), що забезпечує шифрування та автентифікацію в IP мережах. У MANET він може бути використаний для забезпечення конфіденційності і цілісності переданих даних.

Протокол безпеки для протоколу маршрутизації AODV SEAD (Secure Efficient Ad hoc Distance Vector, який використовує криптографічні механізми для запобігання атакам, таким як фальшиві маршрути.

Протокол безпеки для MANET Ariadne, який забезпечує автентифікацію та захист від атак на маршрутизацію, таких як атаки типу «середина шляху».

Протокол безпеки Authenticated Routing for Ad hoc Networks (ARAN), що використовує сертифікати для підтвердження автентичності маршруту в мережах MANET.

4. Програмне забезпечення для управління мобільністю та взаємодії

Програмні моделі Mobility Model Simulator для симуляції мобільності вузлів у MANET, що дозволяють оцінити вплив мобільності на продуктивність мережі, такі як зміни в маршрутах або втрати пакунків.

Ці програмні рішення і протоколи є основною частиною ПО для ефективного функціонування MANET. Вони дозволяють досліджувати, тестувати, а також розгорнути реальні мережі у різних сферах застосування, таких як надзвичайні ситуації, військові операції, логістика та моніторинг.

1.4.3 З'єднання MANET з Інтернет

Зв'язок між мережею MANET та Інтернетом є важливою частиною використання таких мереж, оскільки часто потрібно забезпечити доступ до глобальних ресурсів, сервісів або комунікацію з іншими мережами. Однак, через специфіку MANET, де немає сталих точок доступу або центральної інфраструктури, реалізація цього зв'язку вимагає певних технічних рішень.

Ось кілька можливих варіантів для з'єднання MANET з Інтернетом.

1. Шлюзи (Gateways) між MANET та Інтернетом.

Один із найбільш поширених способів з'єднання MANET з Інтернетом — використання шлюзів, які служать точкою доступу для мережі MANET до глобальних мереж, таких як Інтернет. Шлюзи виконують роль мосту між MANET і більш традиційною інфраструктурою, що дозволяє передавати дані через Інтернет.

Мобільний шлюз. Мобільні пристрої або маршрутизатори, що є частиною MANET, можуть діяти як шлюзи. Вони отримують дані з мережі MANET, маршрутизують їх до Інтернету (через 3G/4G/5G, Wi-Fi або інші канали зв'язку) і навпаки. Це може бути, наприклад, мобільний смартфон або ноутбук, який підключений до Інтернету через мобільного оператора, і одночасно працює в мережі MANET як шлюз.

Динамічне використання шлюзів. У MANET маршрутизація та з'єднання можуть змінюватися через мобільність вузлів. Тому шлюзи повинні бути динамічними й адаптуватися до змін у топології мережі.

2. Mesh-мережі та Інтернет.

Mesh-мережі (наприклад, IEEE 802.11s) дозволяють створювати дистрибутивні безпроводні мережі, які з'єднуються через точку доступу або шлюз до Інтернету. Такі мережі можуть ефективно з'єднувати MANET з Інтернетом через декілька вузлів, що підтримують маршрутизацію трафіку між MANET і Інтернетом. Mesh-шлюзи можуть підключати всю mesh-мережу до Інтернету, забезпечуючи підключення до глобальної мережі через один або кілька шлюзів.

3. Адаптивні протоколи маршрутизації для підключення до Інтернету.

Для ефективної інтеграції MANET з Інтернетом використовуються спеціалізовані протоколи маршрутизації, що дозволяють динамічно виявляти шляхи до шлюзів та керувати трафіком між MANET та Інтернетом. Mobile IP дозволяє пристроям, які змінюють своє місцезнаходження, зберігати свою постійну IP-адресу, що дозволяє здійснювати зв'язок через Інтернет, навіть коли пристрій переміщується по мережі MANET. Це дозволяє зберегти зв'язок з

Інтернетом, незважаючи на мобільність вузлів. Інколи, щоб з'єднати MANET з Інтернетом, можна використовувати стандартні IP-протоколи з додатковими механізмами, які забезпечують маршрутизацію та керування трафіком між MANET та Інтернетом. Такі протоколи, як AODV чи OLSR, можуть бути налаштовані для динамічного пошуку шлюзів у мережі.

4. Використання концепції "Delay-Tolerant Networks" (DTN).

У випадках, коли зв'язок між MANET та Інтернетом не є постійним або стабільним (наприклад, у віддалених районах чи під час катастроф), застосовується концепція Delay-Tolerant Networks (DTN). У DTN можуть бути використані спеціалізовані протоколи для зберігання та передачі даних, коли зв'язок доступний.

Протокол Bundle Protocol (BP), який використовується в DTN для тимчасового зберігання та маршрутизації повідомлень до їхнього кінцевого місця призначення, коли з'єднання з Інтернетом відновлюється.

Зв'язок MANET з Інтернетом передбачає використання шлюзів, мобільних точок доступу або мобільних мереж для маршрутизації трафіку. Варіанти залежать від специфіки мережі, її мобільності, доступних технологій (наприклад, Wi-Fi, 3G/4G/5G), а також особливостей безпеки та продуктивності. Інтеграція MANET з Інтернетом вимагає особливої уваги до маршрутизації, адаптивності мережі та забезпечення стабільного з'єднання.

1.4.4 Повністю автономна MANET

Мережа MANET може бути повністю відокремленою від інших мереж, зокрема від Інтернету або інших зовнішніх інфраструктур. Це є однією з особливостей та переваг MANET — її можливість працювати незалежно від централізованих систем, зв'язку через інфраструктуру або наявності стаціонарних точок доступу. Ось як це може бути організовано.

1. Повністю автономна MANET.

У випадку, коли MANET не має підключення до зовнішніх мереж, вона функціонує як ізольована мережа, де всі пристрої взаємодіють тільки між

собою, без доступу до Інтернету або інших зовнішніх ресурсів. Це може бути корисно в ряді специфічних сценаріїв:

- військові операції, коли потрібна мережа, яка повністю ізольована для забезпечення безпеки і конфіденційності комунікацій.

- тимчасові або аварійні мережі - у випадку природних катастроф, де мережі не можуть бути підключені до Інтернету або централізованих точок доступу.

- мережі в умовах високої мобільності - якщо мережа MANET розгортається в середовищі з високою мобільністю, де немає стабільного доступу до зовнішніх мереж.

У такій ситуації всі дані передаються виключно між вузлами MANET, а маршрутизація, комунікація і управління мережею здійснюються без залучення зовнішніх ресурсів.

2. Механізми забезпечення роботи MANET без Інтернету.

Маршрутизація. Вузли MANET можуть використовувати протоколи маршрутизації, що адаптуються до змін у топології без необхідності підключення до Інтернету. Такі протоколи, як AODV, DSR, OLSR або TORA, дозволяють передавати дані по мережі на основі місцевих знань про топологію і мобільність вузлів.

Автономність вузлів. Всі пристрої в MANET можуть діяти як маршрутизатори та кінцеві точки, передаючи дані від одного до іншого без необхідності в централізованих серверах чи точках доступу.

Безпека і шифрування. Безпека даних у повністю ізольованій MANET може бути забезпечена за допомогою локальних методів шифрування і автентифікації без потреби в централізованих системах управління.

3. Використання в специфічних умовах.

Польові дослідження та наукові експедиції. MANET може бути використана для збору даних в умовах, де неможливо підтримати традиційну інфраструктуру (наприклад, в дикій природі, під час досліджень на великій території).

Тимчасові мережі на заходах. Наприклад, на великих спортивних заходах або концертах, де необхідно організувати локальну мережу для передавання даних, але без підключення до Інтернету чи зовнішніх мереж.

Мережі для забезпечення безпеки. Для передачі конфіденційної інформації в умовах, коли забезпечення абсолютної безпеки є пріоритетом і неможливо дозволити з'єднання з зовнішніми мережами (наприклад, у військових або урядових операціях).

4. Особливості та виклики ізоляції.

Хоча MANET може працювати як повністю відокремлена мережа, є кілька важливих аспектів, які треба враховувати.

Обмеження в доступі до ресурсів. Вузли в ізольованій MANET не зможуть отримувати доступ до зовнішніх ресурсів, таких як хмарні сервіси, веб-сайти чи віддалені сервери. Це може обмежувати її застосування для таких завдань, як оновлення програмного забезпечення чи підключення до глобальних баз даних.

Нестабільність і відмовостійкість. В разі відсутності зовнішніх точок доступу чи резервних каналів зв'язку, ізольовані MANET можуть бути менш стійкими до мережевих проблем, таких як збій маршрутизаторів або втрата зв'язку між вузлами.

5. Технічні рішення для повної ізоляції.

Для того, щоб підтримувати повну ізоляцію MANET від зовнішніх мереж, можна впровадити такі технології:

Контроль доступу. За допомогою фільтрації трафіку, контрольованих точок доступу та механізмів автентифікації можна обмежити взаємодію з зовнішніми мережами.

Фізичні заходи. В ізольованих мережах може бути використана спеціальна апаратна інфраструктура, яка фізично відокремлює MANET від інших мереж (наприклад, використання окремих радіоканалів).

Мережа MANET може бути повністю відокремленою від інших мереж, працюючи як автономна система, де всі вузли взаємодіють між собою без

необхідності підключення до Інтернету чи інших зовнішніх ресурсів. Це може бути корисно в специфічних сценаріях, таких як надзвичайні ситуації, польові дослідження, військові операції або на заходах, де потрібно організувати швидкий і безпечний зв'язок. Однак, ізоляція також накладає певні обмеження, такі як відсутність доступу до зовнішніх ресурсів або інформації.

1.5 Висновки до розділу

Мережі MANET представляють собою тип безпроводних мереж, в яких пристрої можуть безпосередньо з'єднуватися один з одним без централізованого контролю чи інфраструктури. Такі мережі набувають особливої значущості в умовах високої щільності користувачів.

В умовах високої щільності користувачів, де централізовані мережі не можуть уникнути перевантаження або технічних проблем (наприклад, через обмежену пропускну здатність базових станцій), мережі MANET дозволяють створювати тимчасову інфраструктуру, де кожен пристрій може виступати як ретранслятор для інших пристроїв. Це дозволяє масштабувати мережу в міру зростання кількості користувачів, не потребуючи додаткових інвестицій у фізичну інфраструктуру.

MANET може ефективно працювати без необхідності в централізованих точках доступу, що особливо важливо у випадку стихійних лих, масових заходів або в умовах бойових дій.

Мережі MANET автоматично адаптуються до змін у середовищі. В умовах високої щільності користувачів мережі можуть динамічно адаптуватися до нових топологій, пов'язаних з переміщенням абонентів або зміною їх кількості. Це дозволяє оптимізувати використання ресурсів мережі, знижуючи затримки та забезпечуючи більш ефективний обмін даними.

2 ПРОТОКОЛИ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ В MANET

Протоколи маршрутизації класифікуються за різними ознаками, серед яких найбільш значущим є спосіб визначення маршруту між відправником та одержувачем. За цією ознакою протоколи поділяються на три основні групи: проактивні, реактивні та гібридні (комбіновані), як показано на рисунку 2.1.

У реактивних протоколах, таких як Dynamic Source Routing (DSR), Ad hoc On-demand Distance Vector routing (AODV) та Temporally Ordered Routing Algorithm (TORA), запит на маршрут надсилається лише за потреби. Це означає, що коли вузол хоче встановити зв'язок з іншим вузлом, він ініціює широкомовне розсилання запиту шляху та очікує відповіді від кінцевого вузла.

На противагу цьому, проактивні протоколи, наприклад, OLSR, постійно оновлюють свою інформацію про маршрутизацію, підтримуючи актуальне відображення топології мережі.

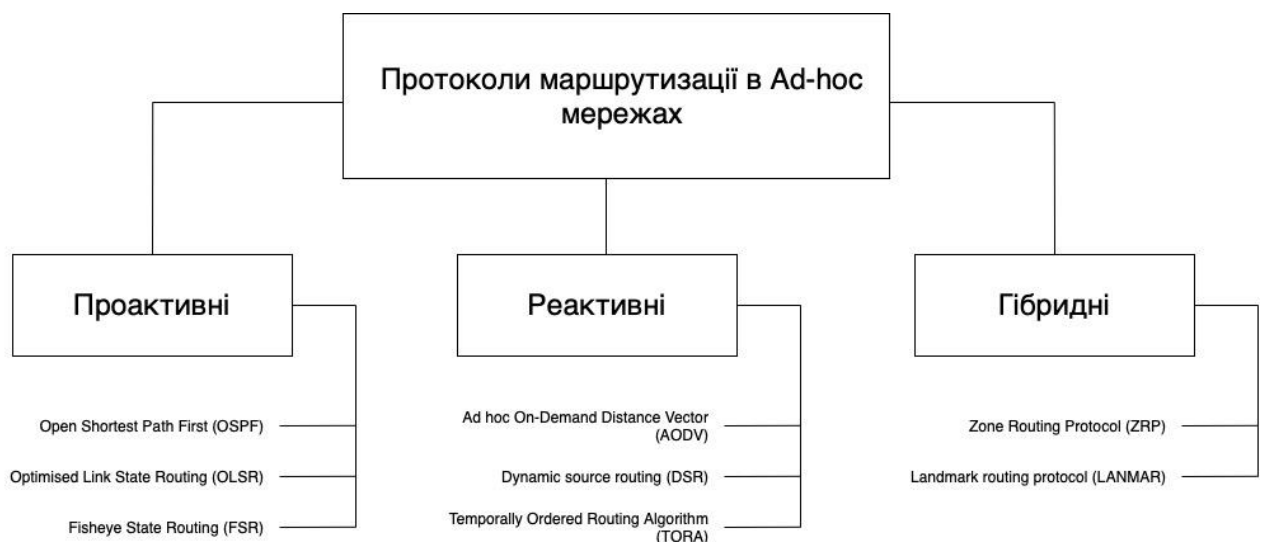


Рисунок 2.1 – Протоколи маршрутизації MANET

Проактивні (таблично-орієнтовані) протоколи передбачають наявність на кожному вузлі таблиці маршрутизації, що містить інформацію про шляхи до всіх інших абонентів мережі. Вузли періодично обмінюються керуючими повідомленнями для підтримки актуальності та цілісності даних про структуру

мережі. Прикладами таких протоколів є OLSR, DSDV та B.A.T.M.A.N. Однак, зі збільшенням мобільності та кількості вузлів у мережі, їх використання призводить до швидкого зростання навантаження на мережу та споживання енергії кожним вузлом.

Реактивні (за запитом) протоколи не потребують попереднього створення таблиць маршрутизації. Вузол ініціює пошук шляху до потрібного адресата лише тоді, коли виникає необхідність у зв'язку. Для встановлення з'єднання вузол може використовувати вже існуючий маршрут або створити новий, використовуючи інформацію про доступні канали. Основним недоліком цієї групи протоколів є збільшення затримки на пошук першого маршруту при зростанні мобільності та кількості вузлів у мережі [9]. До реактивних протоколів належать DSR, AODV та TORA.

На практиці також застосовуються гібридні протоколи, які поєднують підходи проактивних та реактивних протоколів на різних рівнях ієрархії. Вони визначають не лише метод пошуку маршруту, але й спосіб поділу мережі на ієрархічні структури або домени. Недоліками гібридних протоколів є відносна складність їхньої реалізації та потенційне зниження ефективності маршрутизації, пов'язане з необхідністю кластеризації мережі. Прикладом гібридного протоколу є HWMP.

В Ad-hoc мережах застосовуються два основні типи маршрутизації: одношляхова та багатошляхова. Характерною особливістю Ad-hoc мереж є їхня самоорганізація, завдяки якій кожен вузол може виступати як джерелом власної інформації, так і ретранслятором загального потоку даних. Відповідно, між будь-якою парою вузлів у такій мережі зазвичай існує кілька можливих шляхів. Суть багатошляхової маршрутизації полягає в наданні вузлу можливості вибору оптимального маршруту з доступних варіантів. Використання багатошляхових протоколів є більш ефективним з точки зору балансування навантаження в мережі та забезпечення стійкості до збоїв під час передачі трафіку. Такий підхід дозволяє оптимально використовувати пропускну

здатність каналу зв'язку та підвищити загальну продуктивність мережі, а також забезпечує її відмовостійкість і надійність передачі [7].

За останні роки було запропоновано та розроблено значну кількість багатошляхових протоколів і методів маршрутизації для Ad-hoc мереж. Враховуючи задані умови функціонування, для використання в мережах MANET доцільними та ефективними будуть проактивний протокол OLSR та реактивні протоколи DSR, AODV і TORA.

2.1 Протокол OLSR

Протокол OLSR (Optimized Link-State Routing Protocol) призначений для виявлення сусідніх вузлів та підтримки зв'язку з ними, розповсюдження інформації про сусідні з'єднання по всій мережі, визначення найкоротших маршрутів на основі доступної маршрутної інформації та поетапної ретрансляції пакетів.

Для виявлення сусідніх вузлів та підтримки з'єднань (два вузли вважаються сусідами, якщо вони знаходяться в зоні стійкого прийому один одного), кожен вузол мережі періодично (з інтервалом HELLO_INTERVAL) здійснює широкомовну розсилку HELLO-повідомлень. Ці повідомлення містять адреси сусідніх вузлів та інформацію про встановлені з ними з'єднання. Якщо протягом часу NEIGHB_HOLD_INTERVAL вузол не отримує жодного HELLO-повідомлення від свого сусіда, з'єднання з цим вузлом вважається розірваним.

Важливо зазначити, що HELLO-повідомлення не ретранслюються по всій мережі, тому за їх допомогою кожен вузол отримує мережеву інформацію лише в межах свого двокрокового оточення.

Визначимо поняття сусідів: вузол n є однокроковим сусідом вузла x , якщо x знаходиться в зоні стійкого прийому n . Вузол d , який не є однокроковим сусідом x , називається двокроковим сусідом x , якщо d є однокроковим сусідом хоча б одного однокрокового сусіда x .

Для розповсюдження інформації про зв'язки з однокроковими сусідами по всій мережі, вузли періодично (з інтервалом TC_INTERVAL) передають широкомовні TOPOLOGY_CONTROL (TC) повідомлення. Інформація про з'єднання між двома вузлами, отримана з TC-повідомлення від певного вузла-джерела, оновлюється при кожному новому TC-повідомленні від цього вузла. Якщо вузол-джерело TC перестає розсилати інформацію про дане з'єднання або якщо минув інтервал TOP_HOLD_INTERVAL з моменту отримання останнього TC від цього вузла, інформація про з'єднання видаляється.

Усі широкомовні повідомлення ретранслюються із застосуванням випадкової затримки – джиттера, який за замовчуванням обирається рівномірно з діапазону $[0, \text{HELLO_INTERVAL}/4)$.

На основі інформації, отриманої з HELLO та TC-повідомлень, кожен вузол створює орієнтований граф, що відображає бездротову мережу з його точки зору. У цьому графі для кожного вузла мережі визначається найкоротший маршрут, який представляє собою послідовність ретрансляторів. Адреса кінцевого отримувача та адреса першого ретранслятора утворюють запис у таблиці маршрутизації.

При необхідності передати пакет кінцевому отримувачу, вузол знаходить відповідний запис у своїй таблиці маршрутизації та пересилає пакет на вказану адресу ретранслятора. Отримавши пакет, ретранслятор виконує аналогічну процедуру. Важливо зазначити, що маршрут, який використовує ретранслятор, може відрізнятися від маршруту відправника, оскільки кожен вузол має власне уявлення про топологію мережі.

Отже, пакет передається послідовно через ретранслятори доти, доки не досягне кінцевого отримувача, або ж буде відкинутий у випадку виявлення зациклення маршруту.

Важливою особливістю протоколу OLSR, яка сприяє зменшенню завантаженості мережі під час широкомовних розсилок, є використання так званих MPR-ретрансляторів (MultiPoint Relays). Кожен вузол обирає з множини своїх однокрокових сусідів, з якими встановлено двосторонній зв'язок, MPR-

ретранслятори таким чином, щоб кожен його двокроковий сусід був однокроковим сусідом принаймні одного з обраних MPR-ретрансляторів.

MPR-ретранслятори виконують ключову функцію у розповсюдженні маршрутної інформації та пересиланні широкомовних повідомлень. По-перше, кожен вузол за замовчуванням включає в ТС-повідомлення інформацію про двосторонні з'єднання лише з тими сусідами, які обрали його як MPR-ретранслятор. Це значно скорочує обсяг інформації про з'єднання, що розсилається мережею. По-друге, вузол Y пересилає широкомовне повідомлення, отримане від свого сусіда X , лише в тому випадку, якщо Y є MPR-ретранслятором вузла X . Такий механізм суттєво зменшує кількість пересилань при поширенні одного широкомовного повідомлення [8].

2.2 Протокол AODV

AODV (Ad hoc On-Demand Distance Vector) – це протокол вектора відстані, який активується лише за потреби. Вузли не ініціюють пошук або підтримку маршруту до тих пір, поки їм не знадобиться шлях до іншого вузла або поки вони не виступають у ролі проміжного вузла в передачі даних. Вузли, що не залучені до активних маршрутів, не зберігають інформацію про маршрутизацію та не беруть участі у формуванні таблиць маршрутизації. AODV використовує маршрутизацію від вузла до вузла, яка базується на динамічних таблицях, що підтримуються проміжними вузлами. Цей протокол схожий на DSR, проте DSR використовує маршрутизацію від джерела.

Для виявлення локальних з'єднань застосовуються локальні повідомлення "hello", що дозволяє скоротити час відгуку на запити маршруту та ініціювати оновлення за необхідності.

Маршрутам і записам у таблицях маршрутизації присвоюються порядкові номери, які використовуються для заміни застарілої інформації. Кожен вузол підтримує два лічильники: послідовний номер вузла та ідентифікатор широкомовного повідомлення (широкомовний ID).

Запит маршруту в AODV ініціюється, коли вузол хоче зв'язатися з іншим вузлом, але не має інформації про маршрут до нього. Вузол-джерело надсилає ширококомовний пакет запиту маршруту (RREQ) своїм безпосереднім сусідам. Структура цього пакета представлена на рисунку 2.2.

<i>type</i>	<i>flags</i>	<i>resvd</i>	<i>hopcnt</i>
<i>broadcast_id</i>			
<i>dest_addr</i>			
<i>dest_sequence_#</i>			
<i>source_addr</i>			
<i>source_sequence_#</i>			

Рисунок 2.2 – Поля пакету RREQ

Порядковий номер джерела в запиті маршруту вказує на актуальність зворотного шляху до відправника. Порядковий номер призначення відображає актуальність шляху до одержувача.

Кожен вузол, який отримує запит маршруту (RREQ), може або надіслати відповідь з маршрутом (RREP), або переслати RREQ своїм сусідам.

Поля *source_addr* та *broadcast_id* однозначно ідентифікують кожен RREQ.

Значення *broadcast_id* збільшується для кожного нового RREQ, що дозволяє приймачам виявляти та відкидати дублікати RREQ.

Якщо вузол не може відповісти на RREQ, він збільшує свій лічильник та зберігає інформацію, необхідну для підтримки зворотного маршруту (протокол передбачає двосторонні з'єднання) [5].

До цієї інформації належать:

- Ідентифікатор сусіднього вузла, від якого було отримано RREQ.
- IP-адреса призначення.
- IP-адреса джерела.

- Широкомовний ID.
- Порядковий номер вузла-джерела.
- Час закінчення терміну дії запису для зворотного маршруту.

Якщо вузол отримує RREQ і має актуальний маршрут до місця призначення, він надсилає одноадресний пакет відповіді маршруту (RREP) тому сусіду, від якого він отримав RREQ. Структура пакета RREP показана на рисунку 2.3.

<i>type</i>	<i>flags</i>	<i>rsvd</i>	<i>prsz</i>	<i>hopcnt</i>
<i>dest_addr</i>				
<i>dest_sequence_#</i>				
<i>source_addr</i>				
<i>lifetime</i>				

Рисунок 2.3 – Структура пакета RREP

Проміжні вузли пересилають перший отриманий RREP у напрямку до джерела, використовуючи збережені записи зворотного маршруту. Наступні пакети RREP відкидаються, якщо порядковий номер призначення (*dest_sequence_#*) не більший за попередній, або якщо він такий самий, але кількість стрибків (*hopcnt*) менша (що вказує на кращий маршрут). Зрештою, RREP досягає вузла-джерела, який може використовувати сусіда, що надіслав RREP, як наступний вузол для передачі даних до місця призначення. Зворотні маршрути видаляються у тих вузлах, які не отримують пакет RREP.

Зміна маршруту може бути спричинена втратою періодичних "hello"-повідомлень, збоєм на канальному рівні або помилкою при передачі пакета наступному вузлу (що може бути виявлено шляхом прослуховування ретрансляції, якщо це не кінцевий пункт призначення). Вузол, розташований вище за течією трафіку (у напрямку до джерела) і виявивши помилку, передає

пакет повідомлення про помилку маршруту (RERR) з оновленим порядковим номером призначення та кількістю стрибків, що дорівнює нескінченності (вказуючи на недоступність маршруту). Джерело (або інший вузол на маршруті) може ініціювати повторне побудування шляху, надіславши новий пакет RREQ.

2.3 Протокол DSR

DSR (Dynamic Source Routing) – це реактивний протокол динамічної маршрутизації, який, як випливає з назви, є одним з протоколів маршрутизації за запитом, що базується на принципі побудови маршруту від джерела, тобто на явній маршрутизації. Мережі, що використовують DSR, є повністю самоорганізованими та самоналаштовуваними. На відміну від AODV, DSR не використовує періодичне розсилання повідомлень, що сприяє зниженню навантаження на смугу пропускання, економії заряду акумуляторів мобільних пристроїв та запобіганню надмірно частому оновленню маршрутних даних і обміну великим обсягом інформації.

Протокол DSR використовує два основні механізми для пошуку маршруту та підтримки інформації про нього між вузлами: пошук маршруту та підтримка маршруту. DSR постійно оновлює свій кеш маршрутів для забезпечення доступності нових оптимальних шляхів. Механізм "пошук маршруту" використовується вузлом S, коли йому необхідно надіслати пакети вузлу D і він не має інформації про маршрут до нього. Пошук ініціюється відправкою широкомовного запиту RREQ. Під час цього процесу відбувається накопичення адрес проміжних пристроїв між відправником та одержувачем. Усі вузли, що обробляють широкомовний запит, беруть участь у цьому процесі, додаючи інформацію про свої адреси до заголовків пакетів маршрутизації.

Отже, вузли отримують інформацію про стан інших пристроїв та доступні маршрути, якщо через них проходять пакети. Маршрут вважається встановленим лише після успішного досягнення пакетом адресата, після чого

відправляється повідомлення-відповідь. Відповідь може бути надіслана або за вже відомим маршрутом, збереженим у пам'яті вузла-одержувача, або по ланцюжку вузлів, адреси яких записані в заголовку отриманого пакету-запиту. У цьому випадку висувається вимога до ліній зв'язку в мережі – вони повинні бути симетричними. Механізм "підтримка маршруту" дозволяє вузлу S виявляти зміни в топології мережі, які роблять поточний маршрут до D непридатним для використання через розрив з'єднання на шляху. У разі виявлення розриву між відправником та одержувачем, вузол-відправник намагається знайти альтернативний шлях або ініціює новий пошук маршруту за допомогою механізму DSR.

Протокол DSR містить засіб захисту від утворення петель. Вся інформація про пакет, включаючи дані про маршрутизацію, міститься в його заголовку. Завдяки цьому проміжні вузли можуть зберігати цю інформацію у своєму кеші та маршрутних таблицях для подальшого використання.

Отже, коли пристрій має потребу передати дані іншому пристрою, для якого відсутній відомий маршрут, він ініціює пакет RREQ, який розповсюджується мережею. Кожен вузол, отримавши RREQ, пересилає його своїм сусідам, якщо він не є кінцевим одержувачем і час життя пакета ще не вичерпано. Повторно отримані копії цього пакета не пересилаються. Перевірка на дублікати здійснюється за порядковим номером, який присвоюється вузлом-джерелом і записується в заголовку пакета. Цей номер запам'ятовується кожним вузлом, через який пакет проходив хоча б один раз, що повністю виключає утворення петель у маршрутах. Вузол-одержувач, отримавши RREQ, відповідає повідомленням RREP, направляючи його зворотним маршрутом або вже існуючим шляхом, збереженим у його кеші [9].

До недоліків протоколу DSR належить неможливість локального відновлення розірваних з'єднань за допомогою механізму підтримки маршруту. Застаріла інформація в кеші маршрутів може призвести до неузгодженостей при відновленні маршруту. Продуктивність протоколу знижується зі збільшенням швидкості переміщення вузлів. Крім того, використання методу

маршрутизації від джерела призводить до збільшення витрат часу на маршрутизацію зі зростанням довжини шляху.

2.4 Протокол TORA

Метод TORA (Temporally Ordered Routing Algorithm) використовує перетворення орієнтованих графів [13]. Основна ідея полягає у створенні (шляхом розсилки запитів-зондів від відправника та збору відповідей-зондів) і підтримці (через обмін коригувальними зондами) коректної маршрутної мережі. Ця мережа представляє собою ваговий орієнтований ациклічний граф (Go-a) з вузлом-відправником як коренем та вузлом-одержувачем як кінцевою вершиною.

$Go-a = (N_i, K_{ij}), N_a > \dots > N_i > N_a$, де $K_{ij} = \downarrow$ ($K_{ij} = \uparrow$) - напрям каналу від вузла i до вузла j "вниз" ("вгору"), який визначається співвідношенням ваги сусідніх вузлів ($j \in N_i$); N_o, N_i, N_a - ваги вузлів відправника, i -го вузла, адресата, відповідно.

Завдяки наявності декількох шляхів доставки повідомлень, вихід з ладу одного з них не вимагає перебудови всієї маршрутної мережі, що суттєво скорочує обсяг службового трафіку. Метод TORA активується вузлом лише за потреби та гарантує відсутність зациклення маршрутів.

Кожен вузол у цьому методі зберігає інформацію про "напрямок" передачі (адресу наступного ретранслятора) для кожного адресата. Відносно конкретного адресата, кожен i -й вузол мережі має вагу $N_i = (t_i, \beta_i, r_i, d_i, i)$, де:

- t_i – час відмови каналу.
- β_i – ідентифікатор вузла, що визначає відносний рівень ієрархії вузлів.
- r_i – біт, який розділяє рівень на два підрівні та використовується для виявлення поділу мережі на окремі підмережі.
- d_i – ціле число, що використовується для впорядкування вузлів на загальному рівні та служить для розповсюдження нового відносного рівня.

- i – унікальний ідентифікатор вузла.

Усі ідентифікатори вузлів упорядковані для встановлення пріоритету та уникнення конфліктів ($a \leq b \leq c \leq \dots \leq z$). Перші три значення (t_i, β_i, r_i) визначають новий відносний рівень вузла.

Від самого початку вага кожного вузла мережі не визначена: $Hi = (-, -, -, -, i)$. В подальшому вага вузлів буде змінюватися. Вага адресата, наприклад F , спочатку рівна нулю - $HF = (0,0,0,0, F)$. Крім того, кожен вузол зберігає вагу своїх сусідніх вузлів $j \in Ni$ ($HNij = (-, -, -, -, j)$ для кожного j) і стану каналів. Кожен канал $Kij \in L$ може знаходитись в одному з трьох станів:

- неспрямований ($Kij = -$), якщо вага вузла j не визначена;
- спрямований від вузла i до вузла j (якщо ($Hi > Hj$) або Hi - визначений, а Hj - не визначений) - канал “вниз” ($Kij = \downarrow$) відносно вузла i .
- спрямований від вузла j до вузла i ($Hi \leq Hj$) - канал “вверх” ($Kij = \uparrow$) відносно вузла i .

Розглядають три основні етапи функціонування TORA: створення маршруту передачі інформації, підтримка (оптимізація) маршруту та знищення.

2.5 Протокол MAODV

Протокол MAODV (Multicast AODV) [10] належить до гібридних протоколів маршрутизації, оскільки в його основі лежать концепції AODV та DSDV. Він розроблений для використання в мережах з великою кількістю мобільних вузлів (висока щільність користувачів), де топологія мережі постійно змінюється.

В основі алгоритму лежить створення двостороннього дерева для кожної мультикастової групи. Це дерево включає мобільні вузли двох типів: вузли, які приєдналися до мультикастового дерева, та вузли, які не є членами мультикастової групи, але пересилають мультикастові повідомлення іншим вузлам у дереві. Для встановлення та підтримки маршрутів протокол використовує чотири типи повідомлень:

1. Route Request (RREQ): Використовується для запиту маршруту до певної цілі. Вузол ініціює RREQ, коли йому потрібно відправити пакет до певного призначення, але він не має активного маршруту до нього.
2. Route Reply (RREP): Повідомлення-відповідь на RREQ. Коли вузол отримує RREQ і має активний маршрут до запитуваного призначення, він надсилає RREP назад до вузла, який ініціював RREQ.
3. Multicast Activation (MACT): Використовується для активації мультикастового маршруту. Коли вузол хоче приєднатися до мультикастової групи, він відправляє MACT лідеру групи або іншому її члену.
4. Group Hello (GRPH): Періодичне повідомлення, яке використовується для підтримки мультикастового дерева. Воно допомагає визначити активність сусідніх вузлів та їхню належність до мультикастового дерева.

Недоліком використання MAODV є значний обсяг службової інформації та висока обчислювальна складність оновлення маршрутної інформації.

2.6 Оцінка ефективності протоколів маршрутизації в мережі MANET

Специфіка функціонування мереж MANET висуває особливі вимоги до задач управління, зокрема до вибору оптимального протоколу маршрутизації потоків даних, що є першочерговим завданням при проектуванні мереж як цивільного, так і військового призначення.

Існуючі методи маршрутизації різняться за багатьма характеристиками, серед яких найважливішими є: розподілене функціонування, мінімальне навантаження мережі службовою інформацією, стійкість до перевантажень, відсутність зациклених маршрутів тощо. Враховуючи це, необхідно проаналізувати наявні протоколи та методи маршрутизації з точки зору їхньої придатності для використання в мобільних мережах типу MANET.

Основна задача методу маршрутизації полягає у створенні, збереженні та підтримці маршрутів із заданою якістю (зазвичай найкоротших для

забезпечення енергоефективності вузлів) між відправником та одержувачем. Найкоротший маршрут визначається як маршрут з мінімальною сумарною вартістю всіх його каналів.

Серед найпоширеніших методів та протоколів маршрутизації різних класифікаційних типів було обрано чотири протоколи: OLSR, AODV, DSDV та MAODV. Два з них (OLSR та AODV) представляють класи проактивних та реактивних протоколів відповідно, які були розглянуті раніше. Тому далі буде проаналізовано їхню ефективність з точки зору можливості застосування та напрямків удосконалення в мобільних комунікаційних мережах класу MANET з урахуванням умов їхньої роботи та ресурсних обмежень.

Проактивний таблично-орієнтований протокол OLSR (Optimized Link-State Routing Protocol) розроблений спеціально для комунікаційних мереж класу MANET. Він використовує алгоритм Дейкстри та обмін hello-повідомленнями для отримання інформації про стан маршрутів і топологію мережі.

Переваги OLSR:

- Відсутність затримки при передачі даних, пов'язаної з виявленням та побудовою маршрутів.
- Витрати ресурсів вузлів та мережі не зростають зі збільшенням кількості маршрутів передачі.

Недоліки OLSR:

- Неможливість побудови маршрутів із заданою якістю обслуговування (QoS).
- Неефективне використання енергетичних і мережевих ресурсів при розсиланні службової інформації.
- У великих мережах потребує значної пропускної здатності радіоканалів та високої продуктивності процесорів вузлів.

Ще одним таблично-орієнтованим протоколом маршрутизації є Destination-Sequenced Distance Vector (DSDV), який базується на класичному алгоритмі Беллмана-Форда. Його особливість полягає в тому, що кожен мобільний комунікаційний вузол підтримує маршрутну таблицю до всіх

можливих адресатів у мережі. Кожен запис у цій таблиці містить порядковий номер, визначений адресатом. Маршрутна інформація поширюється між вузлами шляхом періодичної відправки повної маршрутної таблиці та додаткових оновлень, які передаються частіше [9].

Переваги DSDV: відсутність зациклення маршрутів; у мережах з невеликою кількістю вузлів забезпечує миттєве встановлення маршрутів передачі. Недоліки DSDV: потребує регулярного оновлення маршрутних таблиць, що призводить до витрат ресурсів вузлів і мережі навіть у стані очікування; малоефективний для мереж з високою динамікою зміни топології.

AODV – це реактивний протокол маршрутизації, що поєднує елементи протоколів DSR та DSDV. Побудова та підтримка маршрутів здійснюється за запитом, а зберігання маршрутної інформації – відповідно до таблично-орієнтованих методів. Для відстеження актуальності маршрутів використовується їх порядкова нумерація. Протокол оперує чотирма типами повідомлень: запит маршруту, відповідь на запит маршруту, повідомлення про помилку маршруту та hello-повідомлення [10]. Принцип роботи протоколу був описаний раніше.

Переваги AODV: відсутність зациклення маршрутів; вирішення проблеми "рахунку до нескінченності"; гарантія отримання актуальних маршрутів; підтримка багатоадресної маршрутизації; низька обчислювальна складність та вимоги до пам'яті. Недоліки AODV: тривалий та складний процес встановлення з'єднання; використання hello-повідомлень; недостатня адаптивність до мереж з динамічною топологією [11].

Протокол MAODV (описаний раніше) є доцільним для використання в мережах з великою кількістю мобільних вузлів (висока щільність користувачів) та постійно змінюваною топологією. Його основними недоліками є висока обчислювальна складність оновлення маршрутної інформації та значний обсяг службового трафіку.

Для оцінки ефективності маршрутизації в мобільних комунікаційних мережах класу MANET було застосовано метрики мобільності та радіозв'язку,

використовуючи модель мобільності, запропоновану в [7]. Моделювання протоколів здійснювалося за допомогою мови програмування Python та середовища Google Colab з використанням визначених параметрів та наступних математичних співвідношень.

1. Моделювання затримки в мережах MANET є складним процесом, оскільки залежить від численних факторів, таких як топологія мережі, протокол маршрутизації, розмір пакетів та швидкість руху вузлів. Для визначення функціональних залежностей змінних необхідно описати основні математичні співвідношення, що визначають час затримки передачі. Рівняння затримки передачі пакета в каналі виглядає наступним чином:

$$T_{зпрд} = L_{п}/R, \quad (2.1)$$

де $T_{зпрд}$ – затримка передачі; $L_{п}$ – розмір пакета; R – номінальна швидкість передачі.

Затримка обробки повідомлення вузлом описується рівнянням:

$$T_{зобр} = N_{п}/C_{обр}, \quad (2.2)$$

де $T_{зобр}$ – затримка обробки; $N_{п}$ – кількість оброблюваних пакетів; $C_{обр}$ – швидкість обробки (в пакетах за секунду).

Запишемо рівняння часу вибору маршруту - функцію затримки маршрутизації. Ця функція відображає, як протокол маршрутизації і топологія мережі впливають на затримку маршрутизації

$$T_{зrout} = f_T(P, T), \quad (2.3)$$

де $T_{зrout}$ – затримка маршрутизації; P – протокол маршрутизації; T – топологія мережі.

Загальний час затримки передачі повідомлення від вузла адресанта до вузла адресата

$$T_{total} = T_{зпрд} + T_{зобр} + T_{зrout}. \quad (2.4)$$

Через високу динамічність топології комунікаційної мережі класу MANET, особливо при використанні табличних протоколів маршрутизації, виникає потреба у частішому оновленні метрик (таблиць маршрутизації), що може призвести до збільшення затримки маршрутизації.

Отже, основними обмеженнями при реалізації цільової функції управління часом затримки передачі є:

- Кількість вузлів у мережі: збільшення кількості вузлів призводить до зростання кількості маршрутів, обсягу інформації для обробки та, як наслідок, до збільшення загального часу затримки.
- Характеристики протоколу маршрутизації: визначають порядок обміну інформацією між вузлами та необхідний обсяг службової інформації в мережі.
- Динаміка топології: математична модель, що описує структуру мережі або фізичне розташування вузлів з урахуванням рельєфу місцевості.

2. Джитер у мережах з комутацією пакетів являє собою варіацію часу затримки. Для застосунків реального часу, таких як VoIP або відеоконференції, збільшення джитера може значно погіршити якість зв'язку.

Джитер математично - це стандартне відхилення затримки пакетів з урахуванням формули (9):

$$J = \sigma(T_{total}). \quad (2.5)$$

Варто зазначити, що джитер враховує варіацію затримки, тому при розрахунках його значення додається до загальної затримки.

3. Пропускна здатність в мережах MANET. Застосуємо для моделювання пропускної здатності формулу Шеннона:

$$C_{ab} = B \log_2(1 + SINR), \quad (2.6)$$

де C_{ab} – пропускна здатність каналу між вузлами a і b ; B – ширина смуги пропускання каналу; $SINR$ – відношення сигнал/шум.

Загальна довжина маршруту

$$D_{ij} = \sum_{a=i}^j d_{ab}, i, j, a, b \in N_{KM}, \quad (2.7)$$

де D_{ij} - загальна довжина маршруту між вузлами i та j ; d_{ab} - довжина каналу між вузлами a і b .

При цьому загальна довжина маршруту визначатиметься залежно від динаміки топології мережі та типу вибраного протоколу маршрутизації

$$D_{ij} = f_D(P, T).$$

4. При моделюванні енергоефективності MANET-мереж враховуються витрати потужності за граничний час функціонування $t_{funcmax}$, що визначається зарядом батареї МК e_{MKmax} (e_{MBCmax} для МБС):

$$\begin{aligned} e_{MKmax} &= P_{MKi} \cdot t_{funcmax}, i \in N_{KM}, \\ e_{MBCmax} &= P_{MBCi} \cdot t_{funcmax}, i \in N_{KM}, \end{aligned} \quad (2.8)$$

де P – потужність, яку споживає вузол за одиницю часу.

Що стосується рівняння потужності споживання для мобільних користувачів, то воно визначається витратами на передачу і прийом пакетів визначеного розміру L_n P_{IO} , Дж/біт, за одиницю часу

$$P_{MKi} = N_{\pi} L_{\pi} P_{10}, \quad (2.9)$$

а для мобільної станції необхідно врахувати витрату потужності на процес адаптивного переміщення на одиницю довжини маршруту $P_{\text{пер}}$

$$P_{\text{МБС}i} = N_{\pi} L_{\pi} P_{10} + \frac{\text{ШР}_{\text{пер}}}{K_{\text{ман}}}, \quad (2.10)$$

де Ш – пройдений шлях роботизованою платформою; $K_{\text{ман}}$ – коефіцієнт маневреності.

Таким чином, енергоефективність вузла КМ в деякий момент часу t можна визначити за формулою

$$\eta_e = \frac{O_i t_{\text{func}}}{P_i}, i \in N_{\text{КМ}}, \quad (2.11)$$

де η_e - енергоефективність i -го вузла; O_i – обсяг переданих даних; P_i – витрачена потужність.

Рівняння (2.1-2.11) були використані для оцінки продуктивності протоколів маршрутизації. Результати моделювання показано на рисунку 2.4.

На графіку (зверху праворуч) представлено розподіл середнього часу затримки передачі даних від відправника до отримувача. Ці статистичні дані відображають час затримки в мілісекундах для кожного протоколу маршрутизації в умовах максимального навантаження мережі. Маршрути будувалися зі збільшенням кількості вузлів, що прямо корелює зі зменшенням пропускної здатності в діапазоні від 20 до 5 Мбіт/с. Графік показує, що протокол MAODV демонструє найменший час затримки. При зростанні навантаження в мережі середній час затримки для MAODV коливався в межах 40-120 мс, тоді як для DSDV становив приблизно 40-165 мс, для AODV – 46-179 мс, а для OLSR – 40-160 мс.

На графіку (внизу ліворуч – Jitter (мс)) зображено розподіл часу затримки між послідовно переданими пакетами даних. Графік ілюструє статистичну

залежність між пропускнуою здатністю та стандартним відхиленням часу затримки доставки пакетів. Особливу увагу приділено моменту максимальної пропускнуї здатності в мережі. Найкращі результати в процесі моделювання мобільної мережі показали протоколи MAODV (джитер $\approx 5-25$ мс) та OLSR (джитер $\approx 5-35$ мс).

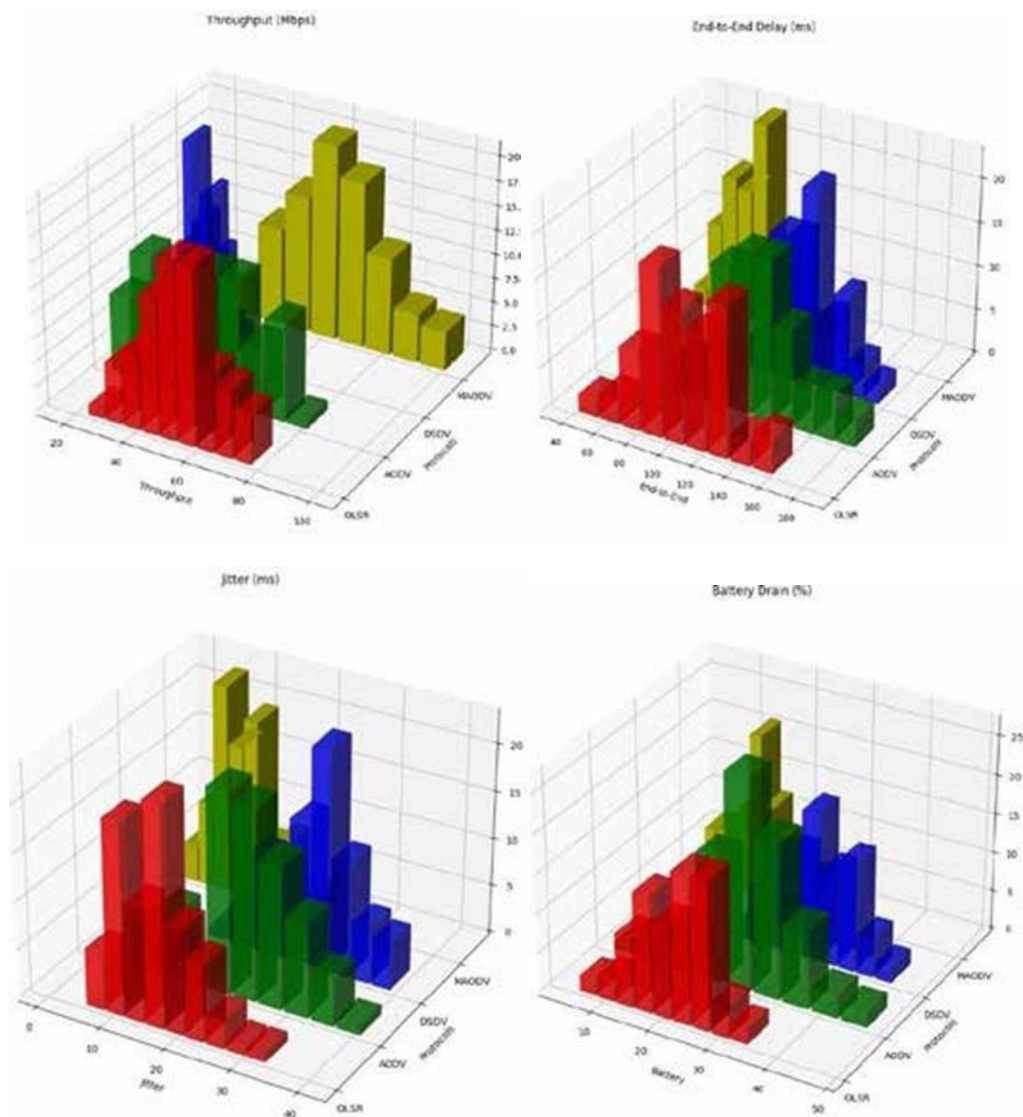


Рисунок 2.4 - Графіки оцінки ефективності OLSR, AODV, DSDV, MAODV

На графіку (внизу праворуч – Battery Drain (%)) представлено розподіл процесу розряду акумуляторів вузлів мережі у відсотках для кожного протоколу. Графіки демонструють, що при зменшенні кількості абонентів рівень розряду акумуляторів зростає. Відповідно, одні з найкращих показників

розподілу розряду акумуляторів забезпечують протоколи MAODV та OLSR (приблизно 10-35%).

Отже, протоколи маршрутизації MAODV та OLSR демонструють кращу адаптивність до умов високої динаміки (зміни швидкості вузлів мережі) порівняно з іншими розглянутими протоколами (AODV, DSDV) з точки зору ключових метрик, таких як пропускна здатність, затримка, джитер та рівень розряду акумуляторів.

Виявлено статистичний взаємозв'язок між пропускною здатністю та стандартним відхиленням часу затримки доставки пакетів даних, що може бути використано для подальшої оптимізації алгоритмів маршрутизації.

Крім того, під час моделювання було отримано оцінку енергоефективності вузлів, яка показала, що протоколи MAODV та OLSR характеризуються меншим відсотком розряду акумуляторів порівняно з іншими протоколами. Це може слугувати основою для прийняття рішення щодо вибору протоколу за критерієм максимального "часу життя" вузлів мережі.

2.7 Висновки до розділу

Для функціонування мереж MANET необхідне спеціалізоване програмне забезпечення, яке забезпечує ефективну маршрутизацію, управління зв'язком, моніторинг стану мережі та забезпечення безпеки. Враховуючи, що в MANET мережа змінюється динамічно, важливо мати протоколи маршрутизації, які адаптуються до змін у топології мережі.

Протокол маршрутизації OLSR базується на оновлених даних про стан ліній зв'язку, що дозволяє знизити кількість передаваної контрольної інформації, що важливо у щільних мережах. Він підтримує стан лінії зв'язку і постійно оновлює інформацію про маршрути в мережі, що дозволяє швидко адаптуватися до змін топології.

Протокол маршрутизації AODV, який працює лише за потребою, тобто маршрути встановлюються лише тоді, коли необхідно передати дані. Це

дозволяє знижувати навантаження на мережу, оскільки не потрібно підтримувати постійні маршрути. Отже, це динамічний алгоритм маршрутизації, цінність якого проявляється особливо у випадку високої щільності користувачів.

DSR – це протокол маршрутизації на основі джерела, який використовує інформацію про маршрути без необхідності підтримки таблиці маршрутизації на кожному вузлі. Це ще один алгоритм маршрутизації на вимогу, який використовує інформацію про маршрут, що передається разом з пакетом. Кожен вузол визначає шлях для передачі даних до кінцевої точки.

Протокол маршрутизації TORA орієнтований на адаптивність до змін у топології, використовуючи тимчасову орієнтацію для формування маршруту.

Протокол MAODV доцільний для використання в мережах, що складаються із великої кількості мобільних вузлів (велика щільність користувачів), тобто в умовах коли топологія мережі постійно змінюється. Його недолік – висока обчислювальна складність оновлення маршрутної інформації та великий обсяг службової інформації.

Виконано порівняльний аналіз ефективності протоколів маршрутизації в мережі MANET. Протоколи маршрутизації MAODV та OLSR мають переваги в умовах високої динаміки та щільності користувачів відносно інших розглянутих протоколів (AODV, DSDV) з точки зору ключових метрик (пропускна здатність, затримка, Jitter та процес розряду батареї).

Виявлено статистичний взаємозв'язок між пропускною здатністю та стандартним відхиленням часу затримки між доставкою пакетів даних, що може бути використано для подальшої оптимізації алгоритмів маршрутизації.

З МНОЖИННИЙ ДОСТУП З ОРТОГОНАЛЬНИМ ЧАСТОТНИМ РОЗДІЛЕННЯМ КАНАЛІВ

Технологія OFDMA (Orthogonal Frequency Division Multiple Access) демонструє високу ефективність у мережах мобільного зв'язку, Wi-Fi та WiMAX. За умов значної щільності користувачів її застосування може бути вигідним і в мережах MANET, забезпечуючи значні переваги завдяки ефективному використанню спектра та зменшенню взаємних завад.

OFDMA дозволяє розподілити доступний частотний діапазон на кілька вузьких каналів, надаючи кожному користувачеві власний субканал. У MANET-мережах з високою щільністю це забезпечує можливість одночасної передачі даних кількома користувачами з мінімізацією інтерференції. Кожен пристрій у мережі може використовувати виділені частотні ресурси, що сприяє підвищенню пропускної здатності та загальної ефективності мережі.

В умовах високої щільності користувачів у MANET зростає ймовірність колізій та перешкод між пристроями. OFDMA допомагає мінімізувати ці завади завдяки ортогональності частотних каналів. Оскільки кожен користувач використовує окремий підканал, це значно знижує можливість перехресних завад.

OFDMA також забезпечує гнучкий розподіл ресурсів залежно від якості каналу та потреб користувачів. В умовах швидко мінливого середовища високощільних мереж така адаптивність є особливо цінною. Користувачі з кращою якістю каналу можуть отримувати більшу кількість ресурсів, тоді як користувачі зі слабким сигналом можуть використовувати меншу кількість частотних ресурсів, що оптимізує загальну пропускну здатність та ефективність мережі.

Оскільки OFDMA є ключовою технологією для сучасних мобільних стандартів, таких як LTE (4G) та 5G, її інтеграція в MANET може сприяти сумісності з існуючими мобільними мережами. Це може бути корисним для

розширення MANET на більші відстані або для використання в гетерогенних мережах.

В умовах високої мобільності, коли пристрої постійно змінюють своє розташування, технологія OFDMA може сприяти підтримці стабільного з'єднання. Це досягається за рахунок динамічного перепризначення підканалів для кожного користувача залежно від їхньої мобільності, що забезпечує ефективну підтримку зв'язку навіть при значних змінах у топології мережі.

У реальних сценаріях експлуатації бездротові мережі часто стикаються з проблемами не стільки через обмеження швидкості передачі, скільки через велику кількість підключених пристроїв, тобто високу щільність користувачів. Саме тому на практиці не завжди вдається досягти теоретичних показників продуктивності через вимушене очікування звільнення середовища передачі, взаємний вплив сусідніх точок доступу та інші фактори, і ця проблема з часом лише загострюється. З огляду на це, застосування технології OFDMA в мережах MANET є логічним кроком. Далі ми детальніше розглянемо сутність цієї технології.

Однією з головних проблем бездротових мереж, що стають дедалі щільнішими, є дефіцит спектру. На сьогоднішній день спостерігається перевантаження діапазону 2,4 ГГц, а також виникають проблеми в діапазоні 5 ГГц. Причини цього різноманітні: від відмінностей в умовах поширення сигналу та вартості кінцевих пристроїв до прагнення використовувати всі доступні частоти під популярний бездротовий стандарт, оскільки кількість клієнтських пристроїв зростає експоненційно. Більше того, теоретично стандарт може бути використаний і в сусідніх частотних діапазонах. Наразі обговорюється пропозиція Федеральної комісії зі зв'язку (FCC) щодо виділення додаткових смуг у діапазоні 6 ГГц для цих цілей.

Частотний ресурс може бути використаний різними способами. Один підхід полягає в його поділі на максимально широкі смуги для забезпечення високої швидкості передачі даних при невеликій кількості пристроїв – і нові стандарти вже підтримують канали шириною до 160 МГц. Інший підхід

передбачає виділення великої кількості вузьких каналів, щоб мінімізувати взаємні завади між пристроями. Універсальність стандарту визначається гнучкістю переходу між цими підходами.

Технологія OFDMA пропонує ефективне використання спектру в умовах високої щільності користувачів. Частотний канал ділиться на піднесійні шириною близько 78 кГц. Передача здійснюється на каналах, сформованих з кількості піднесійних, кратної 26. Фактично, OFDMA є розширеною версією технології OFDM, оптимізованою для мереж з великою кількістю користувачів. OFDMA дозволяє покращити передачу даних у бездротовій мережі з високою щільністю пристроїв, одночасно зменшуючи затримку доставки пакетів для кожного користувача.

Сучасні стандарти Wi-Fi передбачають використання OFDM для однокористувацьких передач на частотах 802.11. OFDMA ж ділить канал на дрібніші частотні підканали, які називаються ресурсними блоками (RU). Завдяки такому поділу стає можливою паралельна передача невеликих кадрів кільком користувачам одночасно. OFDMA – це технологія, яка розділяє канал на менші підканали для забезпечення одночасної, багатокористувацької передачі. Наприклад, традиційний канал шириною 20 МГц може бути поділено на дев'ять вузьких каналів. Використовуючи OFDMA, один з вузлів мережі може одночасно передавати невеликі кадри дев'яти клієнтам. OFDMA забезпечує ефективніше використання середовища передачі для невеликих кадрів, оскільки одночасна передача скорочує надмірні службові витрати на рівні MAC, а також витрати, пов'язані з боротьбою за середовище передачі.

При поділі каналу шириною 20 МГц точка доступу може виділяти ресурсні блоки (RU) розміром 26, 52, 106 та 242 піднесійних, як показано на рисунку 3.1. Це відповідає каналам шириною 2 МГц, 4 МГц, 8 МГц та 20 МГц відповідно. Точка доступу (вузол-відправник) визначає кількість RU, що використовуються в каналі 20 МГц, причому можуть застосовуватися різні комбінації. Наприклад, точка доступу може одночасно обмінюватися даними з одним клієнтом, використовуючи 8 МГц частотного спектра, та з двома іншими

клієнтами, використовуючи підканали по 4 МГц. У цьому полягає принципова відмінність між OFDM та OFDMA.

На практиці існують різні підходи до керування ресурсними блоками. Наприклад, для простих схем зв'язку може бути достатньо смуги 1,9 МГц, 26 піднесійних та двох пілотних сигналів. На противагу цьому, високошвидкісний обмін даними може потребувати смуги 153,2 МГц, 996 піднесійних та 32 пілотних сигналів.

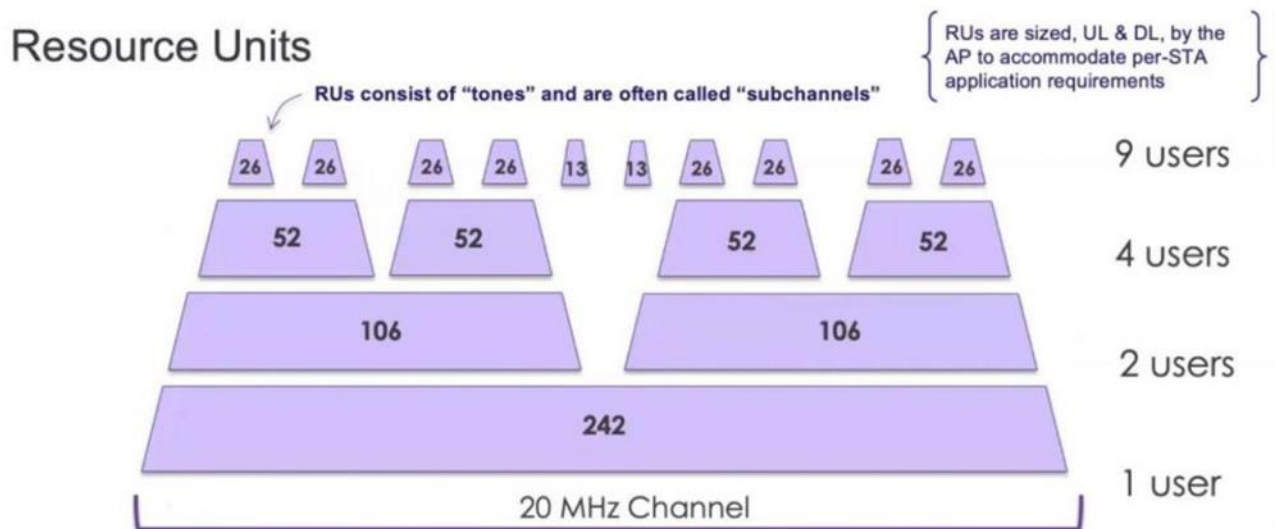


Рисунок 3.1 - Розподіл каналу 20 МГц на ресурсні блоки

Ресурсні блоки (RU) використовуються для призначення піднесійних. Точка доступу (або вузол-джерело в MANET) виділяє RU як фіксовані частотні смуги каналу (наприклад, 20, 40, 80, 80+80 або 160 МГц). Кожен RU може використовувати власну схему модуляції, швидкість кодування та рівень потужності. В інфраструктурних мережах точка доступу контролює зв'язок в обох напрямках для кожного користувача, призначаючи RU часовим інтервалам OFDMA.

Принцип роботи OFDM полягає в тому, що лише один користувач може передавати свій сигнал, використовуючи виділені йому часові слоти та всі піднесійні OFDM, призначені для передачі даних. У цій схемі користувачі отримують доступ до системи OFDM за допомогою часового поділу, як це схематично зображено на рисунку 3.2 зверху.

На відміну від цього, в технології OFDMA, показаній на рисунку 3.2 знизу, доступний частотно-часовий ресурс поділяється на базові частотно-часові ресурсні блоки, причому частотні підканали можуть бути розділені. OFDMA передбачається як у низхідному, так і у висхідному потоках, що для MANET означає рівноправність вузла-джерела та вузла-приймача.

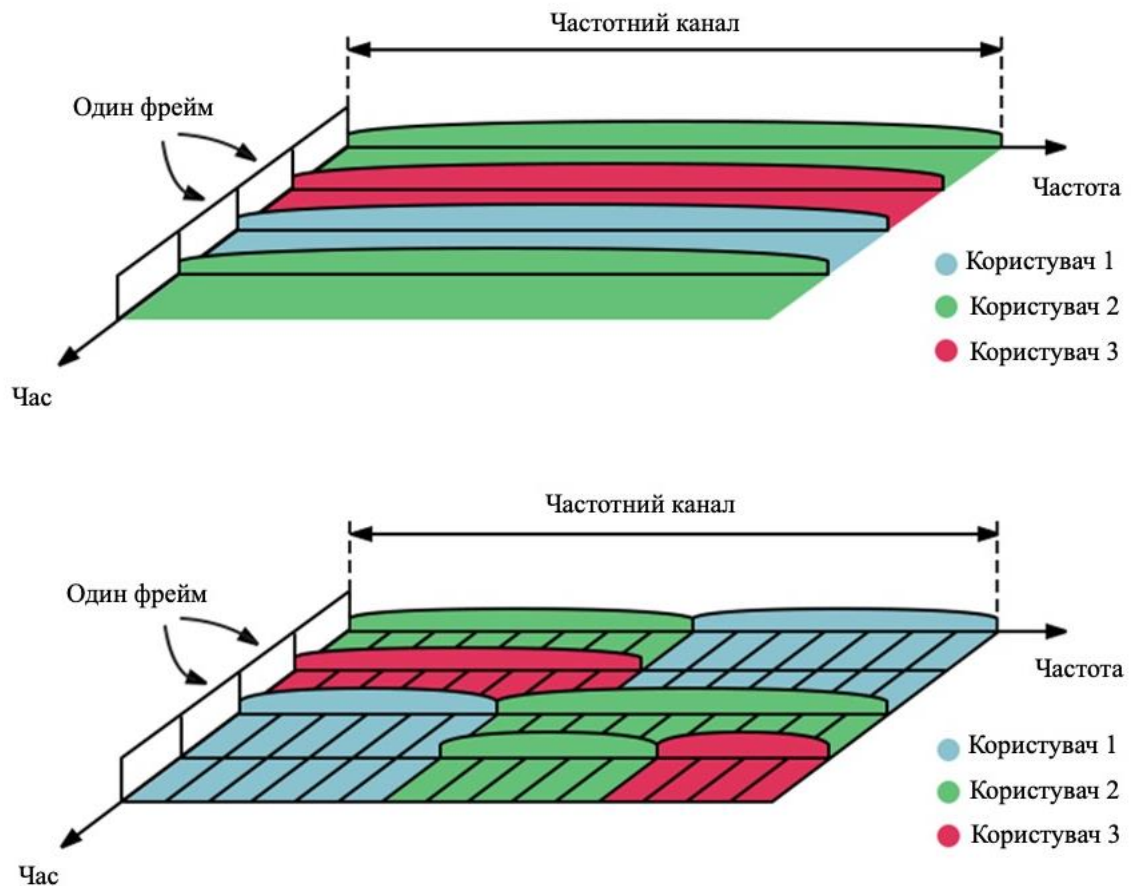


Рисунок 3.2 - Розподіл частотно-часового ресурсу в OFDMA:
зверху – поділ за часом у OFDM, знизу – ресурсні блоки у OFDMA з
локалізованими піднесійними

Завдяки комбінації груп OFDMA та обраних швидкостей модуляції, точка доступу (або будь-який вузол в MANET) може досягати необхідної швидкості передачі даних, частоти помилок та затримки для кожного окремого клієнта або потоку трафіку. Це забезпечує значно складніший рівень якості обслуговування (QoS) порівняно з попередніми технологіями. Важливо, що групи OFDMA не закріплюються за певними потоками трафіку чи клієнтами на постійній основі –

їх конфігурація може змінюватися для кожного пакета. Це дозволяє одній точці доступу підтримувати більшу кількість клієнтів, ніж раніше, що особливо актуально для сценаріїв Інтернету речей з високою щільністю пристроїв, але низькою індивідуальною швидкістю передачі даних. Таким чином, однією з ключових переваг OFDMA є збільшення кількості одночасно обслуговуваних клієнтів.

Функціональність OFDMA як у низхідній, так і у висхідній лініях зв'язку є обов'язковою. Принцип їх роботи дуже схожий: у низхідному каналі точка доступу обробляє трафік, передаючи його кільком клієнтам паралельно, як показано на рисунку 3.3. У висхідному каналі аналогічно відбувається паралельна передача даних від кількох клієнтів до точки доступу. У контексті MANET це означає, що будь-який вузол може одночасно приймати та передавати дані кільком іншим вузлам.

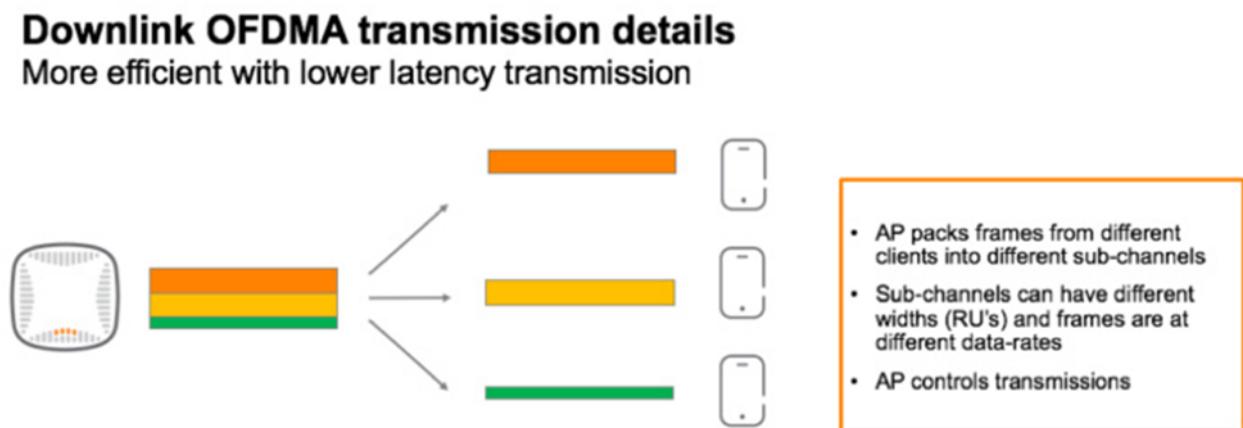


Рисунок 3.3 – OFDMA у низхідному каналі

Доповнення до преамбули повідомляють клієнтам, яку групу OFDMA необхідно прослуховувати та демодулювати. У висхідній лінії зв'язку OFDMA дозволяє кожному клієнту передавати дані у власній виділеній групі OFDMA, тоді як точка доступу одночасно приймає дані від кількох клієнтів. Однак керування висхідною лінією зв'язку OFDMA є складним процесом. Точка доступу координує, які клієнти здійснюватимуть передачу в кожному часовому

інтервалі, а також призначає кожному швидкість передачі та рівень потужності. Для цього спочатку точка доступу має отримати інформацію про бажання клієнтів передавати дані, запитуючи звіти про стан буфера. Потім вона надсилає кадр запуску в низхідній лінії зв'язку, який визначає структуру наступного кадру даних OFDMA у висхідній лінії зв'язку, як показано на рисунку 3.4.

Для забезпечення якісного прийому передачі клієнтів повинні бути точно синхронізовані за часом і досягати точки доступу з подібними рівнями потужності, що вимагає складного керування. Структура багатокористувацьких керуючих кадрів є досить складною. Незважаючи на це, інтеграція OFDMA значно покращує мережу за багатьма параметрами. Ми спостерігаємо зменшення службових витрат, збільшення кількості одночасно обслуговуваних клієнтів, зменшення затримки та джитера, а також покращення загальної якості обслуговування. OFDMA є потужною функцією, яка суттєво змінює функціональність точки доступу та її роль у мережі.

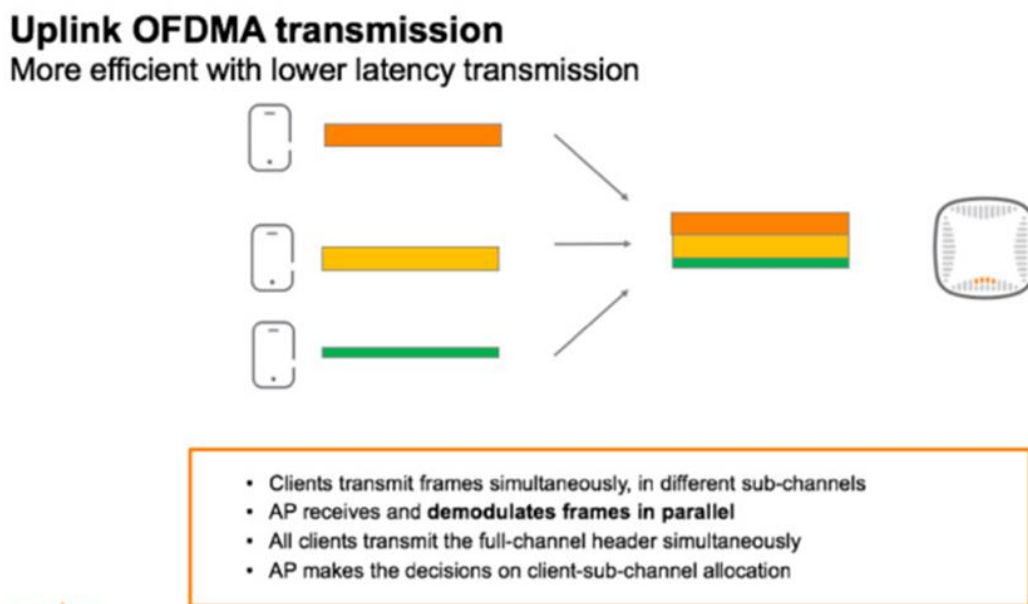


Рисунок 3.4 - Передача OFDMA по висхідній лінії зв'язку

Висновки до розділу

Завдяки своїм перевагам у спектральній ефективності та зменшенні взаємних завад, OFDMA може бути цінною технологією для MANET, особливо в умовах високої щільності користувачів. OFDMA забезпечує можливість паралельної передачі даних шляхом розподілу частотних ресурсів між користувачами. В щільних мережах це значно підвищує пропускну здатність, оскільки багато користувачів можуть одночасно передавати дані на різних частотних каналах, що покращує ефективність використання доступного спектра. Ортогональні частотні канали для кожного користувача сприяють мінімізації інтерференції.

Однак складність синхронізації та керування ресурсами в MANET може становити значну проблему, оскільки ці мережі функціонують без централізованої інфраструктури. Крім того, обробка сигналів OFDMA вимагає значних обчислювальних потужностей, що може бути обтяжливим для мобільних пристроїв з обмеженими ресурсами.

4 МЕХАНІЗМИ ЕНЕРГОЗБЕРЕЖЕННЯ

Зниження енергоспоживання пристроїв є важливим аспектом сучасних мереж Wi-Fi (стандарт 802.11 є одним з ключових для MANET). Для продовження терміну служби акумулятора вузли повинні якомога довше перебувати в режимі сну. Протокол маршрутизації має забезпечувати ефективність при мінімальній активності вузлів – у цьому полягає принцип енергозбереження. Для вирішення цієї проблеми базова функціональність енергозбереження була закладена ще в першій версії стандарту Wi-Fi. Останні доповнення IEEE 802.11ax та IEEE 802.11ba описують сучасні механізми енергозбереження: цільовий час пробудження TWT (Target Wake Time) та радіо пробудження WUR (Wake-Up Radio).

Основна ідея цих механізмів полягає в періодичному вимкненні основного радіоінтерфейсу для зменшення споживання енергії шляхом припинення прослуховування каналу. Однак ефект дрейфу годинника, тобто випадкове відхилення часу станцій, може суттєво знижувати ефективність TWT та WUR, які використовують розклад інтервалів активності. Базовий механізм енергозбереження менш чутливий до дрейфу годинника завдяки періодичній синхронізації при прослуховуванні біконів – керуючих кадрів з інформацією про мережу. Імітаційне моделювання показало, що TWT та WUR забезпечують нижчі показники енергоспоживання та затримки доставки кадрів порівняно з базовим механізмом, навіть з урахуванням ефекту дрейфу годинника.

Модулі Wi-Fi використовуються як у споживчих пристроях (ноутбуки, планшети, смартфони), так і в пристроях Інтернету речей (які можуть бути частиною MANET). Відмінність полягає в різних вимогах до якості обслуговування. Зазвичай споживчі пристрої не мають жорстких вимог до енергозбереження, але можуть періодично генерувати великі обсяги даних (постійно мати кадри для передачі), що потребує високих швидкостей передачі та низьких затримок. З іншого боку, у мережі можуть бути пристрої, які рідко отримують дані від точки доступу, але мають строгі обмеження щодо

енергоспоживання. Таким чином, одночасне задоволення вимог до швидкості передачі даних та обмежень на рівень енергоспоживання для різних типів пристроїв є непростим завданням.

4.1 Базовий механізм енергозбереження

При використанні базового механізму енергозбереження станція може працювати в одному з двох режимів: активному або енергозберігаючому. В енергозберігаючому режимі станція може перебувати у стані сну або в робочому стані. У стані сну станція вимикає свій приймач, повністю припиняючи прослуховування каналу, що забезпечує значну економію енергії. У робочому стані приймач станції залишається увімкненим, що призводить до споживання енергії на прослуховування каналу та прийом передач від інших станцій. В активному режимі станція постійно перебуває в робочому стані. Важливо, що станція повинна повідомляти точку доступу про зміну режиму роботи. Перехід в енергозберігаючий режим можливий лише після отримання підтвердження від точки доступу, а доступ до каналу станція може отримати не раніше оновлення значення NAV (Network Allocation Vector). Точка доступу здійснює буферизацію кадрів, призначених для станцій, що працюють в енергозберігаючому режимі.

Для інформування енергозберігаючих станцій про наявність буферизованих для них даних, точка доступу в кожному біконі (маячковому кадрі) передає таблицю TIM (Traffic Indication Map), яка вказує наявність або відсутність буферизованих кадрів для кожної такої станції. Крім того, з періодичністю, визначеною параметрами мережі, в біконах передається таблиця DTIM (Delivery Traffic Indication Map). Ця таблиця містить інформацію про енергозберігаючі станції, для яких точка доступу має ширококомовні кадри. Такі ширококомовні дані точка доступу надсилає одразу після передачі бікона, що містить таблицю DTIM.

Для економії енергії станції з живленням від акумуляторів (STA)

використовують процедуру узгодження часу пробудження між точкою доступу (AP) та групою STA. З метою забезпечення мобільності та портативності STA зазвичай оснащені акумуляторами з обмеженою ємністю та використовують режим енергозбереження (Power Save Mode, PSM). PSM ефективно працює в стандарті 802.11ah, проте STA, узгоджуючи періоди "неспанья", можуть тривалий час перебувати в PSM, витрачаючи енергію.

Як показано на рисунку 4.1, STA в режимі PSM прослуховує певні маячки: стандартні маячки та цільові маячки. Цільовий маячок містить інформаційні елементи TWT (Target Wake Time IE), які визначають загальні періоди обслуговування TWT (Service Period, SP) зі зсувами TWT та інтервалами пробудження. Час прийому цільових маячків визначається на початку, через певний час передачі цільового маячка (Target Beacon Transmission Time, TBTT). Процедура узгодження включає встановлення зсуву (тобто перше TBTT), після чого визначається інтервал між наступними TBTT.

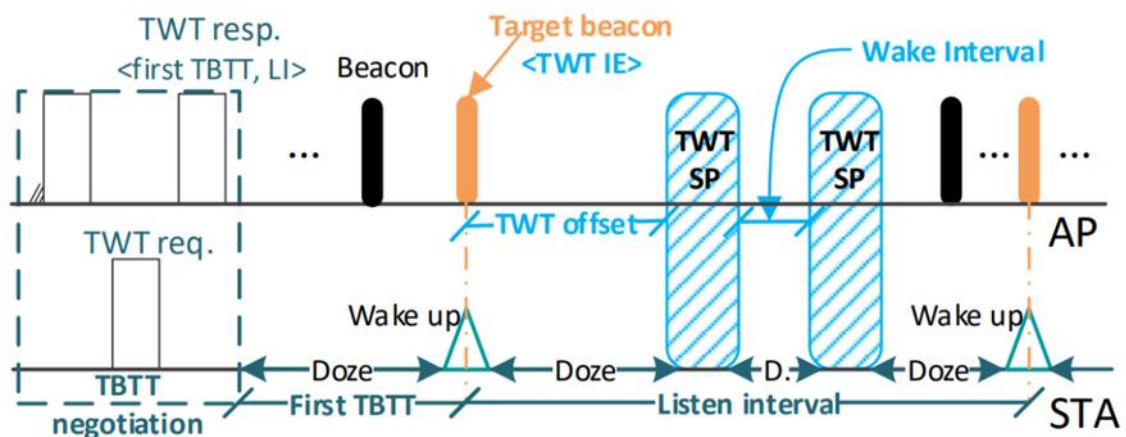


Рисунок 4.1 – Діаграма базового механізму енергозбереження

Оскільки AP може зв'язуватися тільки з однією STA одночасно, інші повинні «не спати», щоб отримувати пакети даних від AP один за одним, незалежно від того, скільки часу займає цей процес. У навантажених сценаріях багато STA можуть одночасно запитувати узгодження TBTT протягом короткого періоду. AP повинен вирішувати ці запити TWT одночасно шляхом "переговорів" з першими TBTT та інтервалами прослуховування (LI). IE TWT у

своїх цільових маяках будуть просити взяти участь або змінити склад трансляції TWT, і одночасно прокидатися для передачі / прийому SP даних. Однакові або невідповідні TBTT STA змушують їх прокидатися одночасно, щоб отримати той же цільовий маяк і запит, претендуючи на безмежний доступ до ресурсів. Це призводить до зниження пропускної здатності та збільшення споживаної потужності.

Точка доступу може також встановлювати інші програми TWT для STA. Зазвичай використовується "широкомовний TWT", тому немає необхідності мати індивідуальний протокол TWT між двома сторонами. Принципова схема «широкомовного TWT» представлена на рис. 4.2.

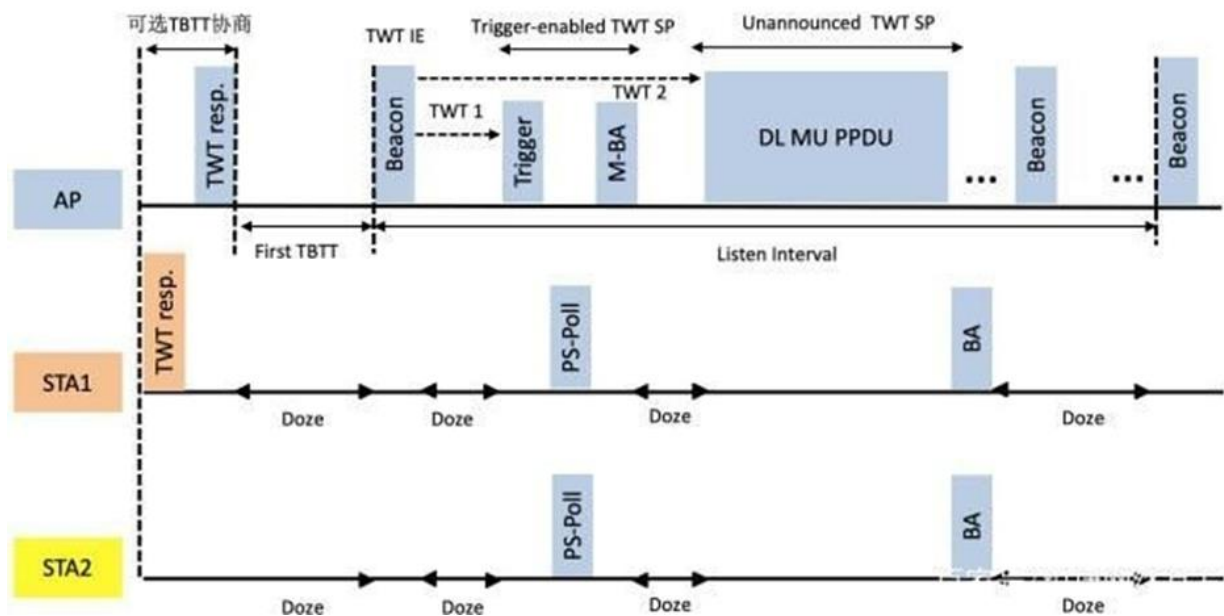


Рисунок 4.2 – Діаграма роботи «широкомовного TWT»

Для отримання інформації про наявність для неї кадрів кожна енергозберігаюча станція має періодично прокидатися та отримувати бікони. Зазначимо, що станції немає необхідності приймати кожен TIM-елемент, тому на практиці енергозберігаючі станції можуть прокидатися лише для прийому деяких біконів із DTIM-елементом. Якщо з прийнятого бікону стало відомо, що для станції немає буферизованих пакетів, станція повертається в стан сну відразу після прийому бікона. В іншому випадку станція відправляє точці доступу спеціальний кадр PS-Poll, а якщо був прийнятий DTIM-бікон, то PS-

Poll відправляється після розсилки точкою доступу широкомовної інформації. У відповідь на PS-Poll точка доступу надсилає станції буферизовані дані.

Незважаючи на те, що використання базової процедури енергозбереження дозволяє значно економити енергію, вона має низку недоліків. Одним із них є те, що енергозберігаючі станції для відправки кадрів PS-Poll використовують метод випадкового доступу до каналу EDCA, що є причиною конкуренції за канал та можливих колізій. Вони можуть виникнути, наприклад, якщо багато енергозберігаючих станцій почнуть одночасно вимагати буферизовані дані від точки доступу. Така конкуренція за канал може призводити до значних втрат в енергоефективності через повторні спроби передачі кадрів PS-Poll та прослуховування енергозберігаючої станцією передач інших станцій до моменту успішного відправлення кадру PS-Poll.

4.2 Target Wake Time

Механізм TWT використовує стани, які визначаються в рамках базової процедури енергозбереження. Відповідно до неї пристрій може працювати в активному або енергозберігаючому режимах. При роботі в режимі енергозбереження пристрій може знаходитися в одному з двох станів: у стані сну або в робочому стані.

Механізм TWT дозволяє парі пристроїв заздалегідь домовлятися про момент часу (а саме про час пробудження TWT), в який обидва пристрої будуть не спати, і про тривалість обслуговування TWT (TWT SP), який відраховується від призначеного TWT. Саме протягом TWT SP станції можуть здійснювати обмін кадрами. Така домовленість дозволяє станціям перейти у стан сну на весь час, окрім TWT SP, не прокидаючись для отримання біконів, що дозволяє значно зменшити енергоспоживання на їх прослуховування. Далі будемо розглядати TWT лише між станцією та точкою доступу. Щоб налаштувати механізм TWT, точка доступу та станція обмінюються спеціальними кадрами налаштування TWT. Ці кадри містять інформацію про запити, згоду або відмову

у встановленні TWT з деякими параметрами, а також значення таких параметрів, як TWT SP або момент пробудження. Крім того, список параметрів включає прапор Тригер, визначальний режим, в якому виконується обмін кадрами, рис. 4.3.

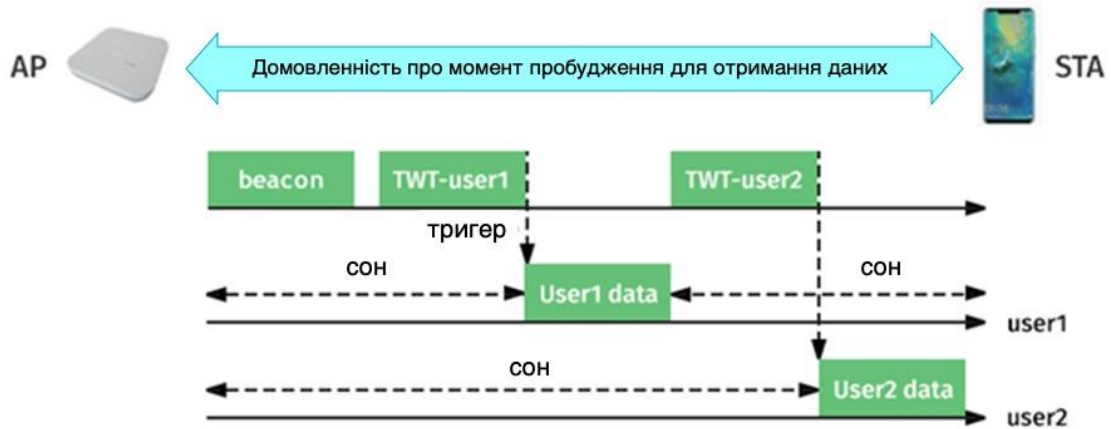


Рисунок 4.3 - Діаграма роботи Target Wake Time

TWT із тригер-кадрами. Якщо прапор Тригер зведений, точка доступу опитує станцію у запланований час, надсилаючи їй спеціальний тригер-кадр. У той же час станція прокидається в призначений момент і чекає на тригер-кадр від точки доступу протягом TWT SP. Через часовий інтервал SIFS після прийому тригер-кадра від точки доступу станція відправляє зворотний кадр даних. Після завершення обміну кадрами станція може перейти в стан сну за відсутності нових кадрів для прийому або передачі.

TWT без тригер-кадрів. Якщо прапор Тригер не зведений, станції прокидаються у запланований час, передають необхідні кадри, використовуючи стандартний метод випадкового доступу до каналу в мережах Wi-Fi, а після завершення обміну даними перемикаються у стан сну.

Незважаючи на те, що тривала відсутність прослуховування каналу при використанні механізму TWT дозволяє значно знизити енергоспоживання сенсора, воно також викликає втрату синхронізації між годинником станції та точкою доступу. Розсинхронізація є наслідком похибки в роботі годинників

будь-яких пристроїв, причому через необхідність максимально знизити вартість сенсорів, похибка їх годинника значно перевершує аналогічну похибку для пристроїв і точки доступу. Зокрема, стандарт Wi-Fi дозволяє абсолютне відхилення годинника, що не перевищує 100 ppm, тобто 100 мкс від 1 с. Таким чином, максимальне відносне відхилення від призначеного часу пробудження може досягати $\delta T = T \cdot 200 \text{ ppm}$, де T - період пробудження датчика. Тому при використанні механізму TWT втрата синхронізації призводить до того, що призначений час пробудження може значно відрізнятись від реального, що призводить до непотрібного прослуховування каналу і, як наслідок, енергії. Для зменшення енергоспоживання, викликаного таким непотрібним прослуховуванням каналу, комітет IEEE 802 LAN/MAN розробляє додаток IEEE 802.11ba [14] до стандарту Wi-Fi.

4.3 Технологія Wake-Up Radio

В даний час для зменшення енергоспоживання пристроїв розробляються не тільки різні механізми на рівні доступу до каналу, але і спеціальні приймачі, що споживають дуже мало енергії, але мають обмежений функціонал. Таким приймачем є WUR (Wake-Up Radio), описаний у додатку IEEE 802.11ba [14] до стандарту Wi-Fi. WUR дозволяє отримувати від точки доступу спеціальні кадри пробудження. Кожна точка доступу та станція мають основний інтерфейс, який використовується в основному каналі шириною 20 МГц для прийому та передачі звичайних (не WUR) кадрів. Також точка доступу, крім основного радіоінтерфейсу, має передавач WUR, а станція — приймач WUR, щоб за допомогою інтерфейсу WUR можна було передавати кадри пробудження від точки доступу для станції. Для зниження енергоспоживання передавача WUR використовується найпростіший вид амплітудної маніпуляції OOK (від on/off keying), а також передача ведеться в смузі шириною 4 МГц.

Для того, щоб проінформувати станцію про необхідність перемикавання основного інтерфейсу в робочий стан (наприклад, якщо точка доступу має

буферизовані кадри для станції), точка доступу відправляє кадр пробудження WUR. Зазначимо, що перемикання основного інтерфейсу станції в робочий стан займає деякий час, про максимальну тривалість якого станція попереджає точку доступу при налаштуванні WUR. Для того, щоб поінформувати точку доступу про пробудження, станція може надіслати їй будь-який кадр, використовуючи для цього основний інтерфейс. Це може бути як кадр даних, так і кадр, що є запитом буферизованих даних, такий як кадр PSpoll.

Завдяки використанню приймача WUR станція може постійно підтримувати свій основний інтерфейс у стані сну, крім безпосередньо моментів обміну кадрами. У той же час, поки основний інтерфейс спить, WUR не спить і споживає енергію, хоча його енергоспоживання в рази менше, ніж у основного інтерфейсу. Для того, щоб вирішити це питання, стандарт пропонує процедуру робочого циклу. При використанні процедури робочого циклу точка доступу WUR та станція заздалегідь домовляються про періодичні часові інтервали, протягом яких інтерфейс WUR не спатиме. В інший час WUR може перебувати в сплячому стані. Процедура робочого циклу для інтерфейсу WUR дозволяє точці доступу зменшити час його неспання, а також рознести в часі періоди активності WUR інтерфейсів різних станцій. Однак використання процедури робочого циклу для зниження енергоспоживання призводить до збільшення затримки на передачу даних.

4.4 Висновки до розділу

Зниження енергоспоживання пристроїв є важливою проблемою для мереж MANET, особливо, якщо вони працюють в умовах значної щільності користувачів. Ефективність механізмів енергозбереження у мережі значною мірою залежить від протоколів маршрутизації, які повинні забезпечувати передачу кадрів за мінімального залучення вузлів. У цьому полягає сутність енергозбереження. Для вирішення цієї проблеми ще в першій версії стандарту Wi-Fi було представлено базовий механізм енергозбереження. У той же час нові

доповнення IEEE 802.11ax та IEEE 802.11ba описують сучасні механізми енергозбереження: механізм цільового часу активності TWT та пробуджуючий інтерфейс WUR.

При використанні базового механізму енергозбереження можливе зниження пропускнуєї здатності та значні втрати енергоефективності через використання методу випадкового доступу до каналу, що є причиною конкуренції за канал та можливі колізії. Вони можуть виникнути, наприклад, якщо багато енергозберігаючих станцій почнуть одночасно вимагати буферизовані дані від точки доступу. Така конкуренція за канал може призводити до значних втрат в енергоефективності через повторні спроби передачі кадрів PS-Poll та прослуховування енергозберігаючої станцією передач інших станцій до моменту успішного відправлення кадру PS-Poll.

TWT дозволяє AP та STA встановити угоду про TWT та активувати STA узгодженим чином у певний час для передачі, при цьому STA залишається у сплячому режимі до TWT. TWT повідомляє пристроїв (клієнтів), коли їм потрібно прокидатися для обміну даними з точкою доступу. Тобто, пристрої не завжди знаходяться в режимі очікування і витрачають енергію, а тільки тоді, коли це необхідно. Але втрата синхронізації призводить до того, що призначений час пробудження може значно відрізнятись від реального, що призводить до непотрібного прослуховування каналу і, як наслідок, витрат енергії.

Відмова від зайвого прослуховування каналу передбачена технологією WUR. Станція може постійно підтримувати свій основний інтерфейс у стані сну, крім безпосередньо моментів обміну кадрами. Поки основний інтерфейс спить, WUR не спить і споживає енергію, хоча його енергоспоживання в рази менше, ніж у основного інтерфейсу. Однак встановлення робочого циклу для енергозаощадження призводить до збільшення затримки на передачу даних.

5 ПІДВИЩЕННЯ СТІЙКОСТІ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ MANET

5.1 Транспортні протоколи в мережах MANET

Призначення транспортного протоколу в мережі MANET полягає в забезпеченні надійної та ефективної передачі даних на основі пакетної комутації в бездротових мобільних мережах.

Надійність передбачає інформування користувача про одну з двох можливих ситуацій, які можуть виникнути під час передачі даних: про те, що дані успішно доставлені адресату, або про те, що виникла непоправна помилка і передача даних не відбулася.

Під ефективністю розуміється мінімізація кількості повторних передач у разі втрати пакетів, порушення зв'язку, зміни маршруту, а також зменшення ймовірності перевантаження мережі.

Забезпечення транспортним протоколом вищезазначених характеристик в умовах змінної топології мережі визначає стійкість передачі даних у мережах MANET [22].

Розглянемо алгоритми роботи «класичного» протоколу керування передачею даних — Transfer Control Protocol (TCP) зі стеку протоколів TCP/IP.

Оскільки для дротових мереж характерна стабільність (розриви з'єднань трапляються дуже рідко), протокол TCP влаштований так, що втрата пакетів зазвичай трактується як наслідок високого навантаження на мережу. Для зменшення так званих «заторів» TCP запускає механізм керування навантаженням, який є неадекватним в умовах змінної фізичної топології і призводить до появи в мережі великої кількості зайвих пакетів.

У MANET, що складається з кількох багатовузлових бездротових з'єднань, втрати пакетів можуть відбуватись через помилки на каналному та фізичному рівнях. У таких умовах TCP демонструє низьку продуктивність, що підтверджено аналізом та моделюванням [19].

Недоліки застосування TCP у MANET можна згрупувати наступним чином:

1. Помилки, пов'язані з конфліктами та колізіями.
2. Проблеми, спричинені мобільністю вузлів у MANET.
3. Неможливість обробки потоку неупорядкованих пакетів.
4. Високе енергоспоживання.

У першій групі найважливішою є проблема прихованого вузла (терміналу). Вона виникає, коли два пристрої (А і В) знаходяться на такій відстані, що не можуть виявити один одного, але обидва перебувають у зоні дії третього пристрою С (рис. 5.1).

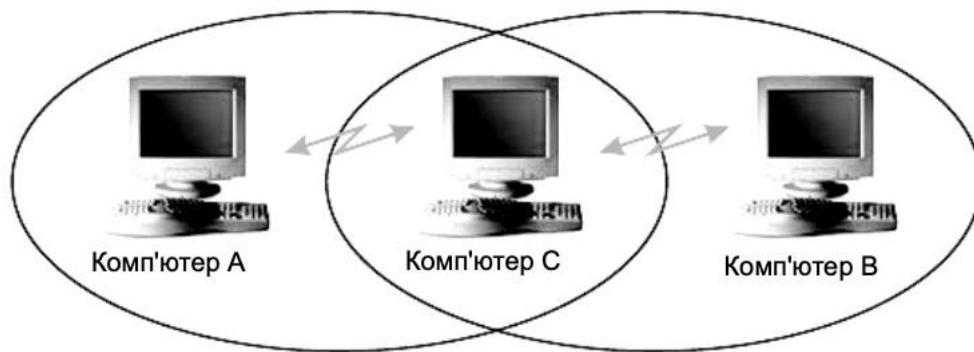


Рисунок 5.1 – Прихований термінал

Якщо А і В починають передачу одночасно, вони не зможуть виявити конфлікт, і пакети не пройдуть через проблеми контролю доступу до середовища. Було прийнято рішення залишити розв'язання цієї проблеми на нижчій рівні протокольного стеку.

Недоліки другої групи зумовлені розривами та відновленням з'єднань, що призводить до втрати пакетів. У такій ситуації TCP помилково вважає, що в мережі виник «затор», і запускає механізми його усунення, хоча насправді це не так. В результаті, після відновлення маршруту швидкість передачі знижується, і з кожним повторенням ситуації стає ще нижчою. Як рішення запропоновано відмовитися від таймерів, застосовувати асинхронну передачу даних і чергу переданих пакетів.

Недоліки третьої групи проявляються при багатомаршрутній (multi-path) маршрутизації. У цьому випадку TCP поводить себе аналогічно попередній ситуації. Як рішення запропоновано сортувати отримані пакети за їхніми номерами, а останній пакет в передачі позначати спеціальним прапорцем.

Недоліки четвертої групи пов'язані з високим енергоспоживанням через надмірну генерацію пакетів, що неефективно для мобільних вузлів з автономним живленням. Тому транспортний протокол у MANET повинен по можливості мінімізувати кількість зайвих повторних передач.

На сьогодні вже існують рішення вказаних проблем — спеціалізовані транспортні протоколи, які були отримані як шляхом модифікації TCP, так і розроблені з нуля. Їх можна поділити на три класи:

- TCP з зворотним зв'язком (TCP-F, TCP-ELFN, ATCP),
- TCP без зворотного зв'язку (TCP-Fixed-RTO, TCP-DOOR, TPA, ATP, ITP),
- протоколи, що використовують спеціальні зміни на інших рівнях протокольного стеку (наприклад, Neighbourhood RED та ін.) [23].

Завдяки зворотному зв'язку, за яким надходить інформація про причини перевантаження мережі, TCP може розрізняти реальне перевантаження і інші проблеми, такі як помилки каналу, розриви маршрутів тощо. Однак механізм зворотного зв'язку у мобільних мережах ускладнює систему і підвищує її вартість.

5.2 Керування передачею та надійність в мережах MANET

Запропонований протокол з одного боку, не використовує зворотний зв'язок, але з іншого — реагує на стан каналу зв'язку та динамічно обирає швидкість передачі даних. Це реалізується за допомогою спостереження за станом буфера протоколу, чергами пакетів і покрокової передачі.

Стан буфера визначається коефіцієнтом заповнення, який відображає напрямок зміни кількості вільного простору.

Протокол використовує три черги:

- черга на відправку,
- черга відправлених пакетів,
- черга на ретрансляцію.

Збираючи статистику по цих чергах, протокол може визначати подальшу стратегію своєї роботи. Покрокова передача означає, що з'єднання встановлюється не одразу з протоколом кінцевого отримувача (якщо немає можливості зв'язатись із ним безпосередньо), а з протоколом вузла, через який проходить маршрут до пункту призначення. Таким чином здійснюється контроль доставки та швидкості передачі між кожною парою сусідніх вузлів маршруту.

Отже, запропонований протокол належить до класу протоколів без зворотного зв'язку. Формат заголовка наведений в таблиці 5.1.

Таблиця 5.1 – Формат заголовка протоколу

Порт відправника (16 біт)									Порт призначення (16 біт)	
Порядковий номер пакета (32 біт)										
Порядковий номер підтвердженого пакета (ACKNOWLEDGMENT) (32 біт)										
Зміщення (4 біта)	Пусто (5 біт)	Прапорці (7 біт)							Коефіцієнт заповнення буфера (16 біт)	
		ACK	PSH	RST	SYN	END	LST	WRG		
IP-адреса джерела										
IP-адреса кінцевого отримувача										
Опції										
Дані										

Розглянемо, за рахунок чого забезпечується надійність у цьому протоколі. Кожному новому вихідному пакету призначається порядковий номер. Після отримання пакету адресат надсилає підтвердження доставки — пакет із

встановленим прапорцем ACK і полем acknowledgment, яке дорівнює номеру прийнятого пакету.

Для перевірки доставки пакетів використовується черга надісланих пакетів. У ній зберігаються елементи, що описують надіслані пакети. Кожен такий елемент має такі поля: номер пакету, вказівник на блок даних і довжина блоку даних (необхідна для відновлення втраченого пакету з буфера), кількість повторних передач (це поле збільшується на 1 під час кожної спроби передати пакет). Щойно кількість повторних передач одного з пакетів перевищує поріг, генерується керуючий сигнал для зміни маршруту. Те саме відбувається, якщо за останній час до черги надісланих пакетів було додано N елементів, але жодного не було вилучено.

Після підтвердження доставки переданого пакету перевіряється відповідність між інформацією, що надійшла з підтвердженням, та інформацією, записаною в елементі, що стоїть на початку черги. Якщо перевірка дає негативний результат, то перший елемент черги переміщується до черги на повторну передачу, а лічильник повторів для цього пакету збільшується на одиницю. Повторно виконується перевірка. Цикл повторюється доти, доки перевірка не дасть позитивний результат. У такому разі елемент, що описує підтверджений пакет, вилучається з черги надісланих пакетів, а блок даних пакету — з буфера.

Цей алгоритм є частиною управління передачею даних, яке ґрунтується на таких принципах:

- Дані передаються по мірі звільнення каналу. Таким чином, передача наступного пакету здійснюється без очікування підтвердження доставки попереднього.
- Під час передачі буфер протоколу підтримується наполовину заповненим. Цей принцип дає змогу вчасно реагувати на зміни.
- Швидкість передачі даних на всіх вузлах маршруту підтримується на одному рівні, який задається вузлом із найнижчою пропускну здатністю. Це дозволяє уникати перевантаження мережі без потреби.

- Першими на відправлення обираються пакети з черги на повторну передачу. Якщо там немає пакетів, формуються нові. Цей принцип дозволяє забезпечити надійність доставки.

- У пакеті АСК разом із підтвердженням передається коефіцієнт заповнення буфера. Він визначається як відношення кількості отриманих даних до загальної кількості оброблених даних з моменту отримання останнього пакету. Обробленими вважаються ті дані, доставка яких підтверджена сусіднім вузлом або процесом-отримувачем [19].

Якщо у пакеті АСК не встановлений прапорець WRG, то перерахунок швидкості здійснюється за формулою 5.1. Якщо встановлений — за формулою 5.2:

$$V_H = \frac{1}{K} + \frac{3}{4} \cdot \left(1 - \frac{1}{K}\right) \cdot V_T \quad (5.1)$$

$$V_H = \frac{1}{K} \cdot V_T \quad (5.2)$$

де V_H — нова швидкість передачі;

V_T — поточна швидкість передачі;

K — коефіцієнт заповнення буфера.

5.3 Моделювання роботи протоколу передачі даних у мережі MANET

Для перевірки алгоритмів і методів була розроблена модель у середовищі MatLab. Схематично вона зображена на рис. 5.2. Кола позначають вузли, які формують мережу та здатні приймати/передавати дані. На ділянці мережі між першим і другим вузлами присутні завади, що погіршують пропускну здатність середовища, що, своєю чергою, призводить до втрат при передачі.

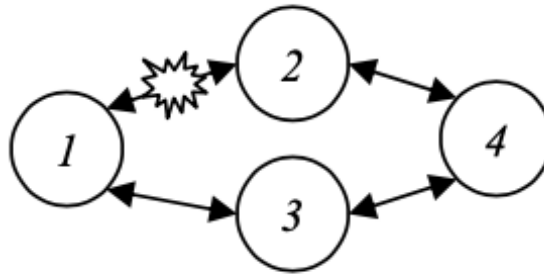


Рисунок 5.2 - Ілюстрація тестового прикладу

Характеристики вузлів:

- Вузол 1: швидкість передачі — 2097 байт/мс; кількість з'єднань — 1; допустима кількість повторних передач пакету — 5.
- Вузол 3: швидкість передачі — 1048 байт/мс; кількість з'єднань — 1; допустима кількість повторних передач пакету — 5.
- Вузли 2 і 4: аналогічно вузлу 1.

Модель вузла зображено на рис. 5.3. Блоки додатків, вхідних з'єднань, каналного і фізичного рівнів — це спрощена реалізація середовища, в якому працює запропонований протокол. У блоці транспортного протоколу реалізовані описані вище механізми та алгоритми. Цей блок здатен приймати дані як від додатків у межах вузла, так і від вхідних з'єднань. Дані з вхідних з'єднань не піднімаються вище рівня транспортного протоколу.

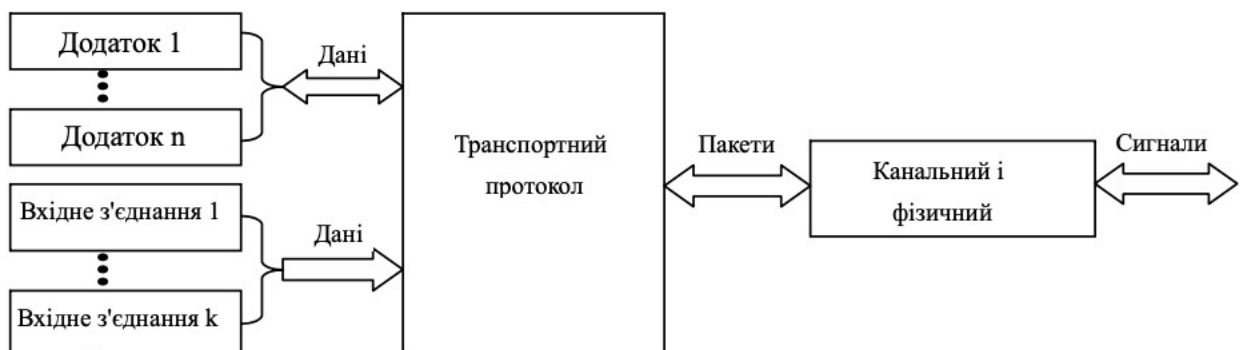


Рисунок 5.3 - Модель вузла

Мережа складається з 4 вузлів. Перший ініціює передачу даних через другий вузол, причому між першим і другим вузлом спостерігаються завади, через які пакети з номерами, кратними трьом, втрачаються. Модель працювала протягом 5 секунд — цього вистачає, враховуючи швидкість передавання, для перевірки працездатності алгоритмів. Затримки, пов'язані з встановленням з'єднання, роботою протоколів чи обладнання, не враховувалися. У розрахунку враховувалася тільки затримка на передачу одного пакету. Розмір пакету: 20970 байт.

Передача починається з пакету 1. За 5 секунд було передано 149 пакетів (рис. 5.4а). У перші 0,9 с спостерігалось порушення порядку пакетів через нестабільний зв'язок між першим і другим вузлами (рис. 5.4б).

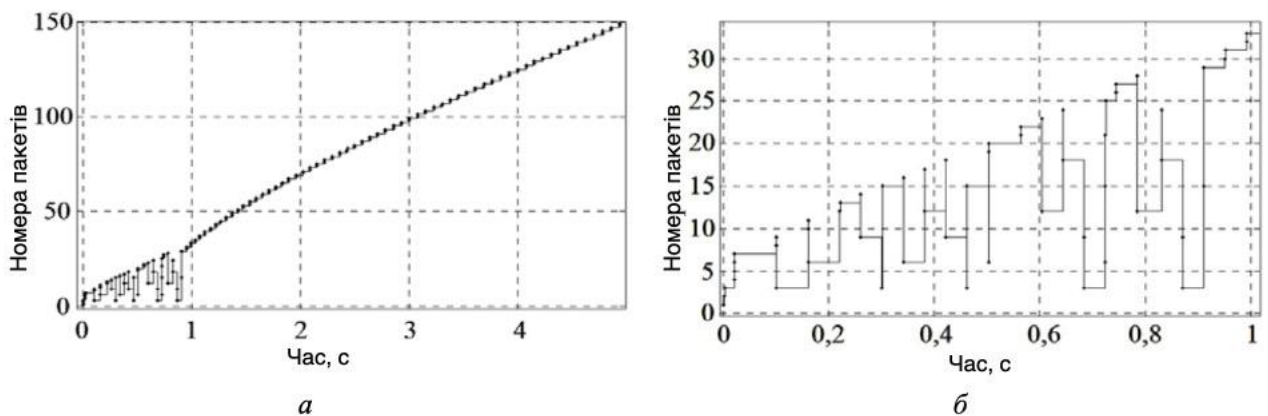


Рисунок 5.4 - Порядок переданих пакетів на першому вузлі

На графіку видно, що, передаючи пакети через другий вузол, третій пакет передавався 5 разів протягом 0,7 с. Після цього, згідно з описаним алгоритмом, здійснено зміну маршруту, і всі втрачені пакети були успішно доставлені за 0,2 с.

Після зміни маршруту швидкість передачі на першому вузлі знизилася, оскільки швидкість передачі на третьому вузлі вдвічі менша (рис. 5.5). В результаті швидкість першого вузла зрівнялася зі швидкістю другого, що дозволило уникнути переповнення на стороні приймача.

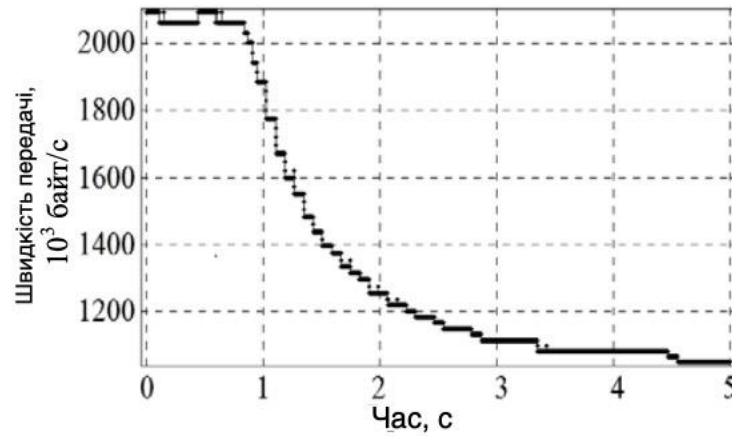


Рисунок 5.5 – Динаміка швидкості передачі на першому вузлі

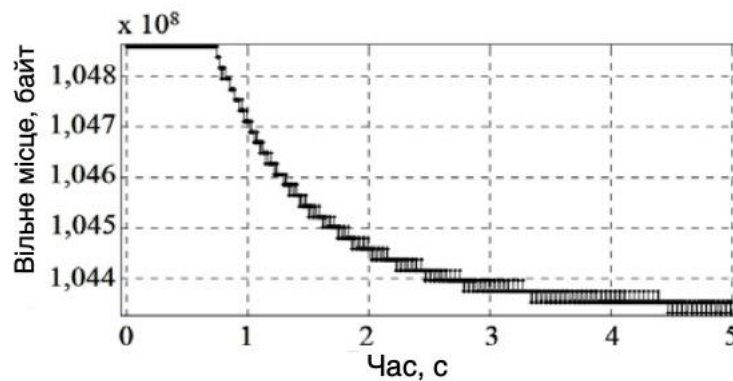


Рисунок 5.6 – Вільний простір в буфері третього вузла

На рис. 5.6 показано, як буфер третього вузла почав заповнюватися після зміни маршруту. Із зменшенням швидкості на першому вузлі, буфер стабілізувався — заповнення припинило зростати.

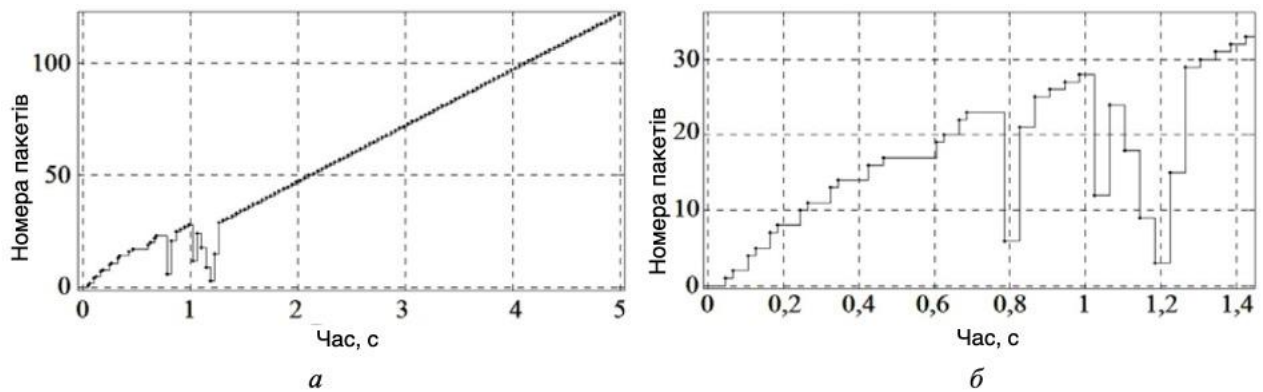


Рисунок 5.7 – Номера пакетів, отриманих на четвертому вузлі

На рис. 5.7а видно, що четвертий вузол отримав усі пакети, які йому були надіслані. У перші 0,7 с порядок прийому був порушений через нестабільний зв'язок. У період з 0,8 до 1,3 с були отримані втрачені раніше пакети (рис. 5.7б). В результаті передано всі пакети без повторної передачі тих, які вже були підтверджені, до моменту зміни маршруту через втрати частини даних.

5.4 Висновки до розділу

Досліджено проблему забезпечення стійкості передачі даних у мережах MANET, які характеризуються динамічною топологією, високим рівнем завад та обмеженими ресурсами. Розгляд класичного транспортного протоколу TCP показав його низьку ефективність у таких умовах через неправильну інтерпретацію втрат пакетів, надмірне навантаження на мережу та неузгодженість із особливостями мобільного середовища.

Для підвищення надійності та ефективності передачі даних було розроблено новий транспортний протокол, який:

- працює без використання зворотного зв'язку;
- враховує стан буфера та адаптує швидкість передачі відповідно до поточних умов;
- застосовує покрокову (hop-by-hop) передачу з контролем на кожному проміжному вузлі;
- ефективно керує чергами пакетів, віддаючи пріоритет повторній передачі.

Моделювання в середовищі MatLab підтвердило працездатність і доцільність запропонованих рішень. Протокол продемонстрував здатність адаптувати швидкість передачі до умов середовища, уникати перевантаження буферів.

Таким чином, розроблений протокол підвищує стійкість передачі даних у MANET, знижує втрати, оптимізує використання ресурсів мережі та зменшує енергоспоживання, що є критично важливим для мобільних пристроїв з автономним живленням.

6 ОХОРОНА ПРАЦІ

Реорганізація економіки та впровадження нових моделей господарювання в Україні призвели до значних змін у структурі підприємств, що, своєю чергою, зумовило необхідність впровадження більш дієвих підходів до покращення умов праці. Якість організації робочого місця стала одним із ключових факторів, що впливає на продуктивність працівників і загальну ефективність виробничої діяльності. Від того, наскільки раціонально організоване робоче середовище, залежить не лише успішність окремого підприємства чи його структурних одиниць, але й розвиток економіки на регіональному та національному рівнях.

У приміщенні, де відбувалися дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів присутні такі шкідливі та небезпечні фактори [25]:

- підвищена чи понижена температура повітря робочої зони;
- недостатнє освітлення робочої зони;
- недостатність природного освітлення;
- підвищений рівень шуму на робочому місці;
- відсутність чи нестача природного світла;
- фізичні перевантаження (статичні);
- нервово - психічні перевантаження (перенапруга аналізаторів, емоційні навантаження).

Відповідно до визначених факторів формуємо рекомендації щодо безпечних умов праці під час виконання роботи.

6.1 Технічні рішення щодо безпечного виконання роботи

Широке промислове та побутове використання ПК актуалізувало питання охорони праці його користувачів. Дотримання вимог цих правил може значно знизити наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відеодисплейними матеріалами, зокрема можливість зорових, нервово-емоційних переживань, серцево-судинних захворювань.

Виходячи з цього, роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації ПК, робочого середовища, робочих місць з ПК, режиму праці і відпочинку при роботі з ПК тощо, які викладені у Правилах.

Основні вимоги до виробничого приміщення для експлуатації ПК:

- приміщення не може бути розміщено у підвалах та цокольних поверхах;
- площа на одне робоче місце в такому приміщенні повинна становити не менше $6,0\text{ м}^2$, а об'єм не менше $20,0\text{ м}^3$;
- приміщення повинно мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2018 [26];
- необхідно щоденно проводити вологе прибирання;
- поруч з приміщенням для роботи з ПК мають бути обладнані: побутова кімната для відпочинку під час роботи; кімната психологічного розвантаження.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам. Виконуючи практичні завдання щодо використання робочої пози, потрібно:

- зменшувати величину статичних напружень;
- розподіляти статичні напруження;
- передбачати можливість змін пози під час роботи.

Для роботи операторів ПК у положенні сидячи рекомендовані такі параметри робочого простору: ширина - не менше 700 мм, глибина - не менше 400 мм, висота робочої поверхні над підлогою – 700 ...750 мм. Під робочою поверхнею необхідно передбачити простір для ніг: висота - менше 600 мм, ширина - не менше 500 мм, глибина - не менше 400 мм. За необхідності огляду робочого місця його висота не повинна перевищувати 1200 мм

Під час роботи сидячи нижня частина корпуса розслаблена, а основне статичне навантаження припадає на м'язи ший, спини, таза, стегон. Неправильна сидяча поза може викликати застій крові в ногах, а якщо виконується великий обсяг роботи для пальців рук – запалення суглобів.

При проектуванні письмового столу варто враховувати наступне:

- висота столу повинна бути обрана з урахуванням можливості сидіти вільно, у зручній позі, при необхідності спираючись на підлокітники;
- нижня частина столу повинна бути сконструйована так, щоб оператор міг зручно сидіти, не був змушений підбирати ноги;
- поверхня столу повинна мати властивості, що виключають появу відблисків у поле зору оператора;
- конструкція столу повинна передбачати наявність висувних шухляд (не менш 3-х для збереження документації, канцелярського приладдя, особистих речей).

На робочому місці дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів існує небезпека поразки електричним струмом. Електричний струм, впливаючи на [тіло](#) людини, може заподіяти йому явні чи приховані пошкодження, в тому числі [опіки](#) всього тіла або окремих його ділянок; [електричні](#) удари характерні внутрішніми ушкодженнями тощо.

Приміщення, де виконується робота, згідно ПУЕ «Правила влаштування електроустановок» класифікується як приміщення без підвищеної небезпеки [27].

Безпечна експлуатація електроустановок здійснюється у відповідності з вимогами ПУЕ [27] та «Правила безпечної експлуатації електроустановок» [28] і передбачає такі заходи та засоби:

- недоступність струмоведучих частин, прокладання електрокабелів під підлогою, в спеціальних каналах, скрите виконання освітлювальної проводки, ізоляцію струмо-провідних елементів ($R_{iz} \geq 0.5 \text{ МОм}$);
- захисне заземлення всіх металевих струмопровідних частин електроустановок та ПК ($R_{з \text{ доп}} \leq 4 \text{ Ом}$);
- використання пониженої напруги 36 В (для аварійного освітлення щита) в операторському пункті та виробничому приміщенні;
- застосування попереджувальної сигналізації, написів, плакатів при проведенні планово-попереджувальних ремонтів і профілактичних випробувань електрообладнання;
- проведення організаційних заходів (спеціальне навчання, атестація та переатестація осіб електротехнічного персоналу, інструктажі тощо).

6.2 Технічні рішення з гігієни праці та виробничої санітарії

6.2.1 Мікроклімат

Температура, відносна вологість, швидкість руху повітря біля тіла людини, а також температура стін і навколишніх предметів утворюють мікроклімат на робочому місці. Температуру, відносну вологість і швидкість руху повітря вимірюють на висоті 1,0 м від підлоги або робочої площадки при роботах, що виконуються сидячи, і на висоті 1,5 м – при роботах, що виконуються стоячи, і не ближче 1 м від нагрівальних приладів і зовнішніх стін.

Робота, яка виконується під час дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів згідно за енерговитратами відноситься до категорії I а (енерговитрати до 139Дж/с) [29]. Допустимі параметри мікроклімату для цієї категорії наведені в табл. 6.1.

Таблиця 6.1 – Параметри мікроклімату

Період року	Допустимі		
	t, °C	W, %	V, м/с
Теплий	22-28	55	0,1-0,2
Холодний	21-25	75	0,1

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціонування повітря, опалювальна система).

6.2.2 Склад повітря робочої зони

Забруднення повітря робочої зони регламентується граничнодопустимими концентраціями (ГДК) в мг/м³ згідно ДСН 3.3.6.042-99 [3]. Джерелами запиленості повітря в приміщенні є одяг людей і пил, що проникає з вулиці. У приміщенні немає значного виділення шкідливих газів. ГДК шкідливих речовин, які знаходяться в досліджуваному приміщенні, наведені в таблиці 6.2.

Таблиця 6.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м ³	Середньо добова	Клас небезпечності
	Максимально разова		
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	4

Параметри іонного складу повітря на робочому місці, що обладнане ПК, повинні відповідати допустимим нормам (табл. 6.3).

Таблиця 6.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 см ³	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Забезпечення складу повітря робочої зони здійснюється за допомогою системи припливно-витяжної вентиляції, регулярного провітрювання, та вологого прибирання.

6.2.3 Виробниче освітлення

Правильно спроектоване освітлення, яке відповідає вимогам санітарних норм здійснює позитивний психологічний вплив на працівника, знижує втому, створює оптимальні умови для роботи органів зору, і тим самим підвищує безпеку праці і знижує травматизм.

Освітлення створюється природним сонячним світлом (природне) і світлом від електричних ламп (штучне). Природне освітлення є найсприятливішим для людини, так як сонячне світло має оптимальний спектр, в ньому наявна достатня кількість ультрафіолетових променів. Штучне освітлення передбачається у приміщеннях, де недостатньо природного світла, і для освітлення у вечірні та нічні години.

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні, які необхідно забезпечити під час виконання роботи зазначені у таблиці 6.4 (за ДБН В.2.5-28-2018 Природне і штучне освітлення [33]):

Таблиця 6.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнення	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, e_n , %			
						Штучне освітлення		Природне освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Високої точності	0,3 – 0,5	III	г	великий	світлий	700	300	5	2	3	1,2

Для забезпечення достатнього освітлення передбачені такі заходи:

- 1) Максимальне використання бічного природного освітлення.
- 2) Систематичне очищення скла від бруду.
- 3) Використання жалюзі на вікнах для регулювання кількості природного світла у приміщенні.
- 4) Загальне штучне освітлення створюється за допомогою люмінесцентних ламп.

6.2.4 Виробничий шум

Шум визначають як сукупність аперіодических звуків різної інтенсивності та частоти. Шум заважає роботі, знижує працездатність і продуктивність праці, при тривалій і інтенсивній дії викликає захворювання організму.

У закритих приміщеннях шум, багаторазово відбиваючись від стін та стелі, посилюється. Тому рекомендується проводити їх акустичну обробку за допомогою звукопоглинальних облицювань з пористих матеріалів, які мають великий коефіцієнт звукопоглинання.

Нормативним документом, який регламентує рівні шуму для різних категорій робочих місць службових приміщень, є ДСН 3.3.6.037-99 [34].

Таблиця 6.5 - Рівень звукового тиску

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньгеометричними частинами (Гц)									Допустимий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Для зменшення шуму здійснюють своєчасний ремонт та профілактику обладнання.

6.2.5 Виробничі випромінювання

На робочій місці розробника у зв'язку із експлуатацією електричної апаратури, існує ризик виникнення підвищеного рівня електромагнітного випромінювання.

Ступінь біологічного впливу електромагнітних полів на організм людини залежить від частоти коливань, напруженості та інтенсивності поля, тривалості його впливу.

Підвищений рівень електромагнітних випромінювань шкодить здоров'ю людини. Від цього страждає передусім нервова і серцево-судинна системи, виникають головний біль і перевтома, знижується точність робочих рухів, порушується сон. Електромагнітне випромінювання викликає зміни тиску крові, гіпотонію або гіпертонію.

Рівні електромагнітних випромінювань моніторів, які вважаються безпечними для здоров'я користувачів, регламентуються нормами MPR II 1990:10 Шведського національного комітету з вимірювань та досліджень (табл.6.6) [11, с.348].

Таблиця 6.6 - Допустимі рівні випромінювань моніторів ПК

Вид поля	ТСО	MPR II
Змінне електричне поле 5 Гц – 2 кГц 2 кГц – 400 кГц	10 В/м 1 В/м на відстані 0,3 м від центра екрана і 0,5 м навколо монітора	2,5 В/м 2,5 В/м на відстані 0,5 м навколо монітора
Змінне магнітне поле 5 Гц – 2 кГц 2 кГц – 400 кГц	250 нТл 200 мА/м 25 нТл 20 мА/м на відстані 0,3 м від центра екрана і 0,5 м навколо монітора	250 нТл 200 мА/м 25 нТл 20 мА/м на відстані 0,5 м навколо монітора

Для захисту людини від дії електромагнітних випромінювань використовують обмеження часу перебування персоналу в робочій зоні та встановлюють раціональні режими експлуатації ПК і роботи працюючого персоналу.

6.3 Пожежна безпека

Неконтрольоване горіння поза спеціальним вогнищем, що завдає матеріальних збитків, називають пожежею.

Запобігання пожеж здійснюється головним чином шляхом виключення можливості утворення горючих або вибухонебезпечних середовищ і джерел запалювання. На випадок пожежі на підприємстві повинна бути пожежний захист для запобігання впливу на людей небезпечних факторів пожежі та обмеження матеріальних збитків від нього.

Пожежна безпека об'єкта повинна забезпечуватися системою запобігання пожежі, системою протипожежного захисту і системою організаційно-технічних заходів.

Метою пожежної безпеки об'єкта є попередження виникнення пожежі на визначеному чинними нормативами рівні, а у випадку виникнення пожежі – обмеження її розповсюдження, своєчасне виявлення, гасіння пожежі, захист людей і матеріальних цінностей.

6.3.1 Технічні рішення системи запобігання пожежі

До причин, що можуть спричинити пожежу в приміщенні, відносяться:

– перевантаження електромережі і перегріву струму несучих частин та з'єднань;

– порушення правил експлуатації техніки.

Система запобігання пожежі передбачає:

- періодичний контроль цілісності ізоляції;
- наявність спеціальних місць для куріння;
- періодичне проведення інструктажів з протипожежної безпеки;
- незахаращення приміщення горючими матеріалами;
- наявність системи захисту від атмосферної електрики.

6.3.2 Технічні рішення системи протипожежного захисту

Приміщення оснащене вуглекислотними вогнегасниками – на території 300 м² 4 вогнегасника (в кожному відділі і на сходовому марші). Також у коридорі встановлений пожежний гідрант з рукавом, який підключений до системи водопостачання.

Вогнегасники слід встановлювати у легкодоступних та помітних місцях (коридорах, біля входів або виходів з приміщень тощо), а також у пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі. При цьому необхідно забезпечити їх захист від попадання прямих сонячних променів і безпосередньої (без загороджувальних щитків) дії опалювальних та нагрівальних приладів [37].

Використані вогнегасники, а також вогнегасники із зірваними пломбами необхідно негайно направляти на перезарядження або перевірку. Вогнегасники, відправлені з об'єкта на перезарядження, повинні бути замінені відповідною кількістю заряджених вогнегасників.

Пожежні щити (стенди) повинні забезпечувати:

- захист вогнегасників від потрапляння прямих сонячних променів, а також захист знімних комплектуючих виробів від використання сторонніми особами не за призначенням (для щитів та стендів, установлюваних поза приміщеннями);

- зручність та оперативність зняття закріплених на щиті (стенді) комплектуючих виробів.

Для зазначення місця розміщення первинних засобів пожежогасіння слід встановлювати вказівні знаки згідно з чинними державними стандартами. Знаки повинні бути розміщені на видних місцях на висоті стандартами. Знаки повинні бути розміщені на видних місцях на висоті 2–2,5 м від рівня підлоги як всередині, так і поза приміщеннями (за потреби).

Власники підприємств, установ та організацій або уповноважені ними органи, а також орендарі зобов'язані:

- розробляти комплексні заходи щодо забезпечення пожежної безпеки, впроваджувати передові досягнення науки;
- забезпечувати дотримання протипожежних вимог стандартів, норм, правил, а також виконання вимог приписів і постанов органів державного пожежного нагляду;
- організовувати навчання працівників правилам пожежної безпеки та пропаганду заходів щодо їх забезпечення;
- у разі відсутності нормативних актів вимог, необхідних для забезпечення пожежної безпеки, вживати відповідні заходи, погоджуючи їх з органами державного нагляду;
- утримувати в справному стані засоби протипожежного захисту і зв'язку, пожежну техніку, обладнання та інвентар, не допускати їх використання не за призначенням;
- створювати, у разі потреби, відповідно до встановленого порядку, підрозділи пожежної охорони та необхідну для їх функціонування матеріально-технічну базу;
- подавати на вимогу державної пожежної охорони відомості та документи про стан пожежної безпеки об'єктів і продукції, що ними виробляється;
- здійснювати заходи щодо впровадження автоматичних засобів виявлення та гасіння пожеж і використання з цією метою виробничої автоматики;
- своєчасно інформувати пожежну охорону про несправність пожежної техніки, систем протипожежного захисту, водопостачання, а також про закриття доріг і проїздів на своїй території;
- проводити службове розслідування випадків пожеж.

6.4 Висновки до розділу

В результаті виконання цього розділу було опрацьовано такі питання охорони праці, як технічні рішення стосовно: гігієни праці та виробничої санітарії, мікроклімат приміщень, виробниче освітлення, виробничий шум та випромінювання. Також розглянуто пожежна безпека у виробничих приміщеннях та технічні рішення системи запобігання пожежі та систем протипожежного захисту

ВИСНОВКИ

В самоорганізованій мережі відсутня фіксована інфраструктура, вузли мережі є одночасно і мобільними терміналами і маршрутизаторами. Маршрутизація у такій мережі є складним завданням. Вона суттєво відрізняється від традиційної маршрутизації у провідних мережах. Зв'язок між вузлами по радіоканалу часто є переривчастим, епізодичним і не може бути гарантованим. Через рухливість вузлів і мимовільної організації з'єднань топологія мережі зазнає частих, непередбачуваних і значних змін. Дальність радіозв'язку в мережі обмежена, безпосередній зв'язок між багатьма парами вузлів неможливий. У зв'язку з цим необхідне використання маршрутизації з численними переходами, стрибками.

З урахуванням заданих умов роботи доцільними та ефективними для використання в мережах MANET прийнято проактивний протокол OLSR та реактивні протоколи DSR, AODV, TORA. Для функціонування мереж MANET необхідне спеціалізоване програмне забезпечення, яке забезпечує ефективну маршрутизацію, управління зв'язком, моніторинг стану мережі та забезпечення безпеки. Розглянуті зазначені протоколи маршрутизації та визначені їх переваги та недоліки. Виконано порівняльний аналіз ефективності протоколів. Протоколи маршрутизації MAODV та OLSR мають переваги в умовах високої динаміки та щільності користувачів відносно інших розглянутих протоколів (AODV, DSDV) з точки зору ключових метрик (пропускна здатність, затримка, Jitter та процес розряду батареї). Виявлено статистичний взаємозв'язок між пропускною здатністю та стандартним відхиленням часу затримки між доставкою пакетів даних, що може бути використано для подальшої оптимізації алгоритмів маршрутизації.

Крім ефективних алгоритмів маршрутизації у мережі MANET для роботи в умовах значної щільності користувачів використовуються також алгоритми та технології, щоб забезпечити стабільне з'єднання, зниження затримок, підвищення пропускної здатності і забезпечення надійності. Особливо

ефективною є мережа MANET, яка поєднує у собі зазначені вище протоколи маршрутизації, технологію множинного доступу з ортогональним частотним розділенням каналів (OFDMA) та алгоритми енергозощадження.

OFDMA дозволяє одночасно обробляти запити кількох різних користувачів або пристроїв в одному каналі, розподіляючи спектр на піднесійних. Таким чином, кілька користувачів можуть передавати дані одночасно, кожен використовує різні частоти в межах одного каналу. Це особливо корисно для зменшення часу затримки і підвищення ефективності в середовищах з великим навантаженням. В умовах щільної мережі це значно покращує пропускну здатність, оскільки багато користувачів можуть одночасно передавати дані на різних частотних каналах, що підвищує ефективність використання доступного спектра. Ортогональні канали для кожного користувача допомагають мінімізувати завади між користувачами.

Для економії енергоспоживання необхідно оптимізувати використання енергії: пристрої можуть автоматично переходити в сплячий режим або знижувати рівень активності, коли вони не використовуються. Це дозволяє зменшити енергоспоживання без шкоди для ефективності мережі. В умовах високої щільності користувачів економія енергії допомагає уникнути перевантаження на окремі вузли та зменшує ймовірність втрати з'єднань. Для вирішення проблеми енергозощадження ще в першій версії стандарту Wi-Fi було представлено базовий механізм енергозбереження. У той же час нові доповнення описують сучасні механізми енергозбереження: механізм цільового часу активності TWT та пробуджуючий інтерфейс WUR.

Було досліджено проблему забезпечення стійкості передачі даних у мережах MANET, які характеризуються динамічною топологією, високим рівнем перешкод та обмеженими ресурсами. Розроблений протокол підвищує стійкість передачі даних у MANET, знижує втрати, оптимізує використання ресурсів мережі та зменшує енергоспоживання.

Виконано розрахунки з питань охорони праці та безпеки життєдіяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бортник Г. Г. Системи передавання в електрозв'язку. Навчальний посібник. – Вінниця: ВНТУ, 2006. – 138 с.
2. Бойко Ю.М. Концептуальні особливості реалізації безпроводних сенсорних мереж / Ю.М. Бойко, В.В. Мішан // Вісник Хмельницького національного університету. – Технічні науки. – Хмельницький . – 2010. – №2. – С. 94 -98.
3. Hoebeke J., Moerman I., Demeester P. Adaptive routing for mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking. 2012. Vol. 2012, no. 1. URL: <https://doi.org/10.1186/1687-1499-2012-126> (date of access: 17.09.2023).
4. MIKARIĆ B. Routing protocols in Mobile Ad-hoc Networks. PRZEGLĄD ELEKTROTECHNICZNY. 2020. Vol. 1, no. 8. P. 108–113. URL: <https://doi.org/10.15199/48.2020.08.21> (date of access: 17.09.2023).
5. Міночкін А.І., Романюк В. А. Маршрутизація в мобільних радіомережах – проблема і шляхи її вирішення. Зв'язок. 2006. № 7. С. 49–55.
6. Teršić D. M., Veinović M. Đ. Classification of MANET routing protocols. Vojnotehnicki glasnik. 2015. Vol. 63, no. 1. P. 84–101. URL: <https://doi.org/10.5937/vojtehg63-5706> (date of access: 17.09.2023).
7. Mummadisetty B. C., Puri A., Latifi S. Performance Assessment of MANET Routing Protocols. International Journal of Communications, Network and System Sciences. 2015. Vol. 08, no. 11. P. 456–470. URL: <https://doi.org/10.4236/ijcns.2015.811041> (date of access: 17.09.2023).
8. PERFORMANCE ANALYSIS OF MANET ROUTING PROTOCOLS / I. A. Rasooly et al. International Journal of Engineering Applied Sciences and Technology. 2019. Vol. 04, no. 08. P. 356–361. URL: <https://doi.org/10.33564/ijeast.2019.v04i08.060> (date of access: 17.09.2023).
9. Беляков Р. О., Фесенко О. Д. Модель мобільності наземної комунікаційної мережі спеціального при- значення. COMPUTER-

INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION.
2023. № 51. С. 130–138. DOI: 10.36910/6775-2524-0560-2023-51-17.

10. Солодовник В.І. Метод адаптивної об'єднаної прийомо–передавальної просторової модуляції для високошвидкісних систем безпроводового зв'язку / Солодовник В.І. // Збірник наукових праць ВІТІ, 2018. – № 1 – С. 126 – 140.

11. Солодовник В.І. Алгоритм адаптивної модуляції та просторового мультиплексування у багатоантенних системах безпроводового зв'язку / Солодовник В.І. // Збірник наукових праць ВІТІ, 2018. – № 3 – С. 103 – 111.

12. Бабак В.П. Обробка сигналів у радіоканалах цифрових систем передавання інформації: Навч. посібник [Текст] / В.П. Бабак, Т.М. Наритник, Ю.В. Куц, В.Я. Казимиренко. – К.: Книжкове вид-во НАУ, 2005. – 476 с.

13. Головін Ю.О. Основи радіозв'язку з рухомими об'єктами: навч. посіб. Київ : ІСЗЗІ НТУУ КПІ, 2016. 322 с.

14. Михалевський Д. В. Оцінка параметрів безпроводного каналу передачі інформації стандарту 802.11Wi-Fi / Д. В. Михалевський // Східно - Європейський журнал передових технологій. – 2014. – № 6/9 (72). – С. 22-25. DOI: 10.15587/1729-4061.2014.31666.

15. Стандарт локальних мереж іеєе 802.11 wi-fi URL: <https://beloshop.ru/uk/ethernet-standard-ieee-80211-wi-fi/> – Дата доступу 18.11.2020.

16. Михалевський Д. В. Передача трафіку у мережах Wi-Fi при дії інтерференційних завад / Д. В. Михалевський, М. Д. Гузь, Р. О.Красота. – Сборник научных трудов Sword. – 2014. – №4(37) Том 5. – С. 12-17.

17. Технологія іеєе 802.11. Підтримка потокових даних. Сумісність з іншими стандартами бездротового зв'язку [Електронний ресурс]. URL: <https://teploskat.ru/the-technology-ieee-80211/> – Дата доступу 02.12.2020.

18.Протокол802.11 URL:http://www.irbisnbnv.gov.ua/cgi-bin/irbis_nbnv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzundiz_2015_6_3.pdf – Дата доступу 06.12.2020.

19. Дослідження показників якості обслуговування в локальних бездротових мережах [Електронний ресурс]. URL:<http://masters.donntu.org/2019/fkita/kolenikov/diss/indexu.htm> – Дата доступу 11.12.2020.

20. Михалевський Д. В. Дослідження передачі інформації в умовах суміщеного та сусіднього інтерференційного каналів для стандарту 802.11n / Д. В. Михалевський, В.В. Номировська, О.М. Постернак // Вимірювальна та обчислювальна техніка в технологічних процесах.– 2015. – №2. – С. 155 – 159.

21. Ткаченко О.М. Особливості створення мережевої інфраструктури великого підприємства / О.М. Ткаченко, А.В. Лемешко, Д.В. Кращенко, Р.С. Кадюк, Т.М. Стельмах // Наукові записки УНДІЗ. – 2019. – №3(55). – С.12-18.

22. IEEE 802.11 «Wireless LAN Medium Access Control and Physical Layer Specifications» [Електронний ресурс] IEEE // Режим доступу: DOI:10.1109/ieeestd.2016.7786995 (дата звернення 11.04.2025).

23. Wi-Fi global economic value to reach \$5 trillion in 2025 [Електронний ресурс] Wi-Fi Alliance // Режим доступу: <https://www.wi-fi.org/news-events/newsroom/wi-fi-global-economic-value-to-reach-5-trillion-in-2025> (дата звернення 01.03.2025).

24. Європейський інститут телекомунікаційних стандартів [Електронний ресурс] ETSI // Режим доступу: <https://www.etsi.org> (дата звернення 05.03.2025).

25. ДСТУ ОHSAS 18002:2015. Системи управління гігієною та безпекою праці. Основні принципи виконання вимог ОHSAS 18001:2007 (ОHSAS 18002:2008, IDT). К. : ГП «УкрНИУЦ», 2016. 21 с

26. ДСТУ ISO 45001:2019 Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування (ISO 45001:2018, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88004.

27. НПАОП 0.00-4.12-05. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці. URL: <http://zakon.rada.gov.ua/laws/show/z0231-05>

28. ДСТУ 8829:2019 Пожежовибухонебезпечність речовин і матеріалів.

Номенклатура показників і методи їхнього визначення. Класифікація. URL: <https://www.alutal.com.ua/wp-content/uploads/2021/02/dstu-8829-2019-1.pdf>

29. ДСТУ 8828:2019 Пожежна безпека. Загальні положення. URL: <https://dwg.ru/dnl/15125>

30. ДБН В.2.5-28-2018 Природне і штучне освітлення - [Електронний ресурс] - Режим доступу: <http://document.ua/prirodne-i-shtuchne-osvitlennja-nor8425.html>

31. НАПБА.01.001-14. Правила пожежної безпеки в Україні. К. : МВС України, 2014. 47 с

32. ДБНВ.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд. К. : Мінбуд України, 2006. 154 с

33. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: <http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html>

34. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: <http://mozdocs.kiev.ua/view.php?id=1972>

35. Охорона праці та промислова безпека: навч. посіб. [К.Н.Ткачук, В.В.Зацарний, Р.Н.Сабарно та ін.]; за ред. К.Н.Ткачука, В.В.Зацарного. – К.: Основа. – 2009. – 454 с.

36. Правила улаштування електроустановок. URL: <http://www.energiy.com.ua/PUE.html>

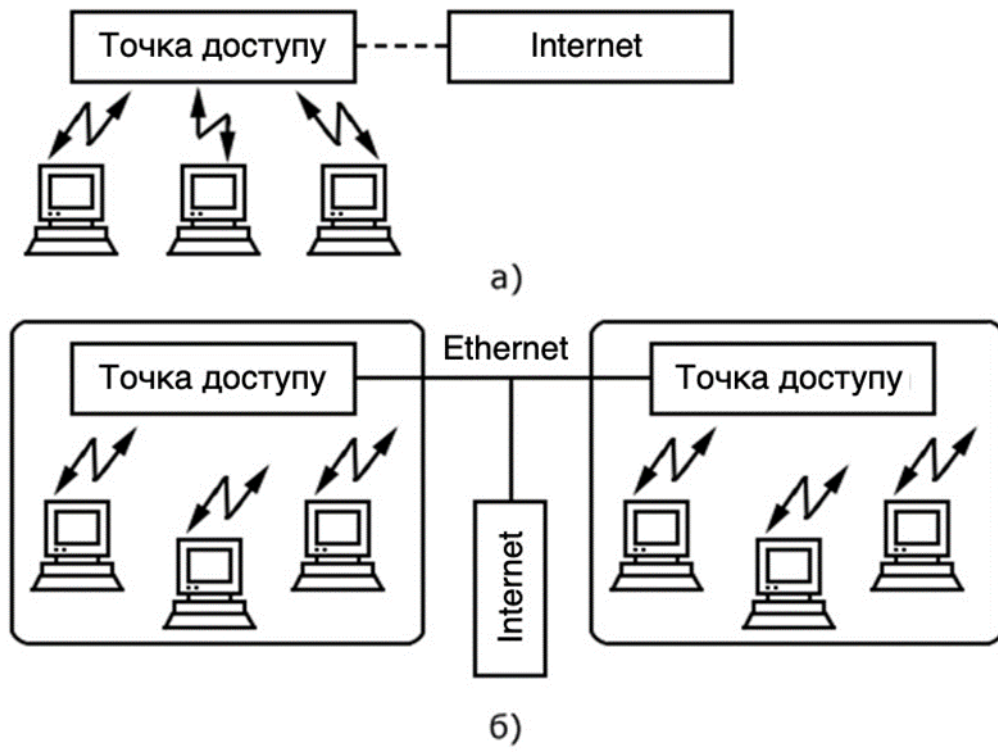
37. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop_0_00-7_15-18_01_ua.php

Додаток А
(обов'язковий)

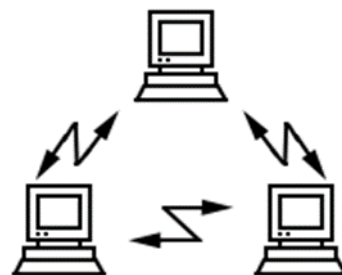
ІЛЮСТРАТИВНА ЧАСТИНА

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ФУНКЦІОНУВАННЯ СПЕЦІАЛЬНИХ
МЕРЕЖ MANET В УМОВАХ ВИСОКОЇ ЩІЛЬНОСТІ КОРИСТУВАЧІВ

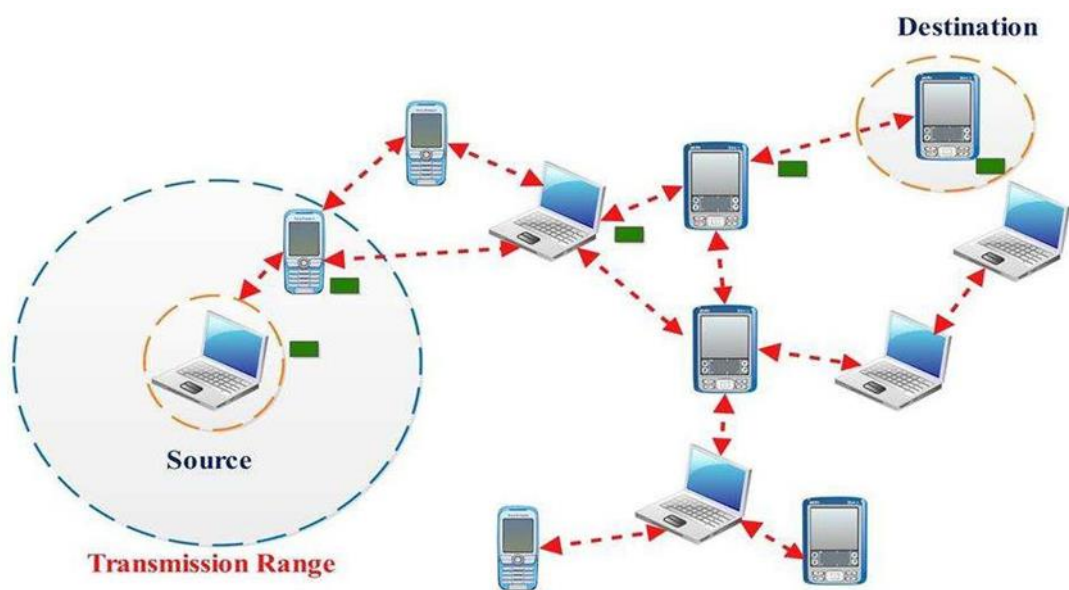
назва бакалаврської кваліфікаційної роботи



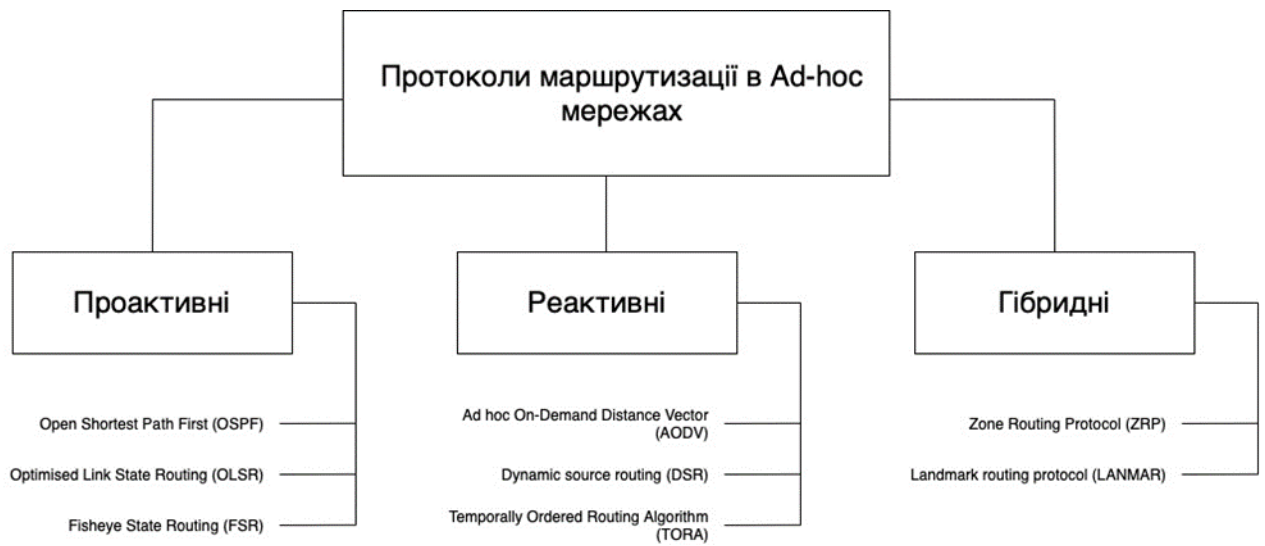
Архітектура - режим з точкою доступу



Архітектура - режим без точки доступу (мережа Ad Hoc)



Топологія мережі MANET



Протоколи маршрутизації MANET

Downlink OFDMA transmission details

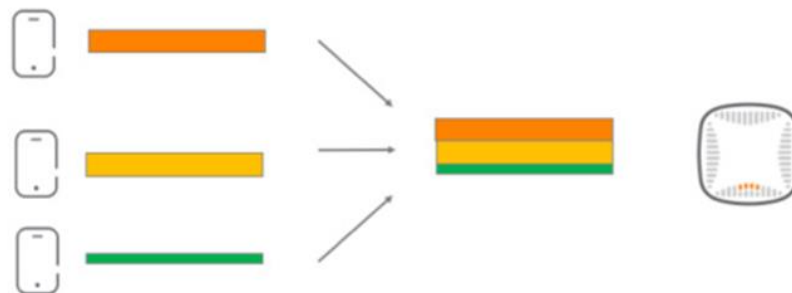
More efficient with lower latency transmission



OFDMA у низхідному каналі

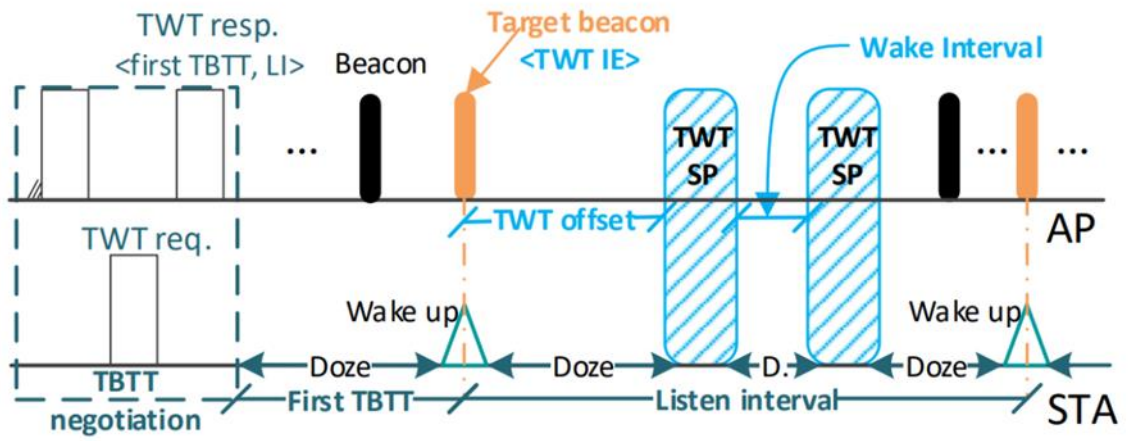
Uplink OFDMA transmission

More efficient with lower latency transmission

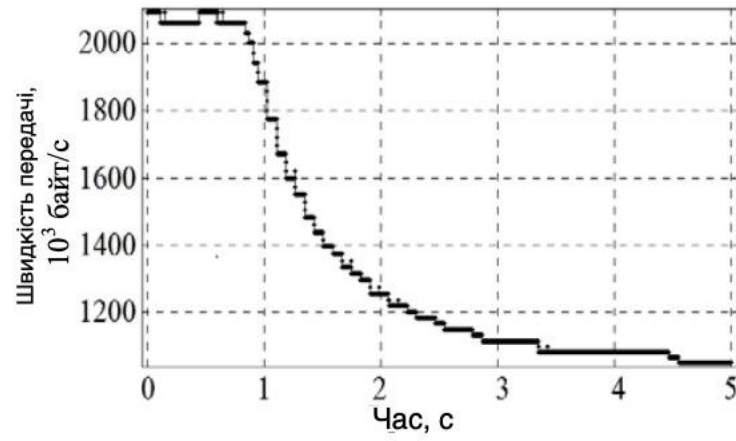


- Clients transmit frames simultaneously, in different sub-channels
- AP receives and **demodulates frames in parallel**
- All clients transmit the full-channel header simultaneously
- AP makes the decisions on client-sub-channel allocation

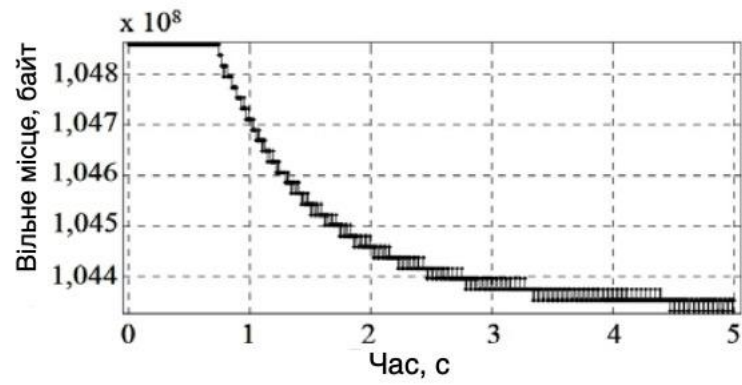
Передача OFDMA по висхідній лінії зв'язку



Діаграма базового механізму енергозбереження



Результати моделювання:
Динаміка швидкості передачі на першому вузлі



Результати моделювання:
Вільний простір у буфері третього вузла

Додаток Б

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Дослідження алгоритмів функціонування спеціальних мереж MANET в умовах високої щільності користувачів

Тип роботи: бакалаврська кваліфікаційна робота
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ кафедра ІКСТ, факультет ІЕС, група ПЗТ-216
(кафедра, факультет, навчальна група)

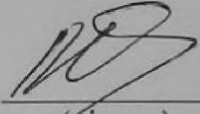
Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism 13,83 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

- ☒ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту
- ☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.
- ☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

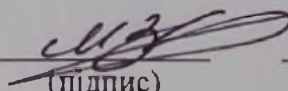
Експертна комісія:

Кичак В.М., завідувач кафедри ІКСТ
(прізвище, ініціали, посада)

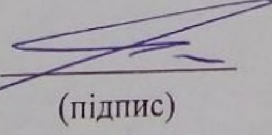

(підпис)

Васильківський М.В., гарант ОПП
(прізвище, ініціали, посада)

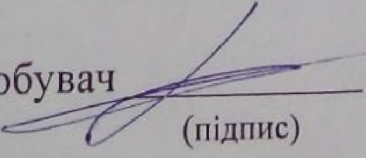

(підпис)

Особа, відповідальна за перевірку  Васильківський М.В.
(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник 
(підпис)

Барась С.Т., професор кафедри ІКСТ
(прізвище, ініціали, посада)

Здобувач 
(підпис)

Гамалєєв Д.Д.
(прізвище, ініціали)