

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ
СІКОРСЬКОГО»**

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«__» _____ 2024 р.

Дипломна робота

на здобуття ступеня бакалавра

**за освітньо-професійною програмою «Інженерія та програмування
інфокомунікацій»**

спеціальності 172 Телекомунікації та радіотехніка

**на тему: «Аналіз принципів побудови і функціонування безпроводових
інфокомунікаційних мереж із самоорганізацією»**

Виконав:

студент IV курсу, групи ТЗ-01

Ткачов Богдан Володимирович _____

Керівник:

Доцент кафедри ТК НН ІТС, к.т.н.

Валуйський Станіслав Вікторович _____

Рецензент:

Завідувач кафедри ІТТ НН ІТС, професор, д.т.н., с.н.с.

Скулиш Марія Анатоліївна _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій КРАВЧУК

«___» _____ 2024 р.

ЗАВДАННЯ

на дипломну роботу студенту

Ткачову Богдану Володимировичу

1. Тема роботи «Аналіз принципів побудови і функціонування безпроводових інфокомунікаційних мереж із самоорганізацією», керівник роботи Валуйський Станіслав Вікторович, к.т.н., затверджені наказом по університету від «26» квітня 2024 р. № 1884-с.

2. Термін подання студентом роботи 10 червня 2024 р.

3. Вихідні дані до роботи: інформаційні матеріали про принципи побудови і функціонування безпроводових інфокомунікаційних мереж із самоорганізацією.

4. Зміст роботи:

- Розглянути основні характеристики безпроводових інфокомунікаційних мереж із самоорганізацією.
- Розглянути принципи побудови і функціонування безпроводових мереж із самоорганізацією.
- Розглянути актуальні приклади застосування безпроводових мереж із самоорганізацією .
- Провести їх аналіз, та визначити особливості.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

- Тема.

- Види безпроводових інфокомунікаційних мереж із самоорганізацією .
- Структури бездротових інфокомунікаційних мереж із самоорганізацією.
- Аналіз стандартів протоколів канального рівня.
- Загальні висновки по роботі.

6. Дата видачі завдання видачі завдання « 9» лютого 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз та підбір літературних джерел, проведення патентних досліджень з тематики дипломної роботи.	9.02.2024-07.03.2024	Виконано
2	Обґрунтування актуальності теми роботи, мети та задач дослідження, об'єкту та предмету дослідження, практичної цінності роботи.	08.03.2024-24.04.2024	Виконано
3	Обґрунтування актуальності теми роботи, мети та задач дослідження, об'єкту та предмету дослідження, практичної цінності роботи.	25.04.2024-01.06.2024	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	01.06.2024-10.06.2024	Виконано
5	Підготовка та оформлення презентації для доповіді	10.06.2024-15.06.2024	Виконано

Студент

Богдан ТКАЧОВ

Керівник

Станіслав ВАЛУЙСЬКИЙ

РЕФЕРАТ

Дипломна робота містить 59 сторінок, 14 рисунків, 1 таблицю. Було використано 13 джерел інформації.

Метою роботи є дослідження та аналіз принципів побудови і функціонування безпроводових інфокомунікаційних мереж із самоорганізацією. Основними методами дослідження були аналітичний огляд літератури та моделювання.

У результаті роботи було розглянуто архітектурні принципи SON, ключові протоколи маршрутизації, методи управління ресурсами та інтерфейси і стандарти. Отримані результати включають нові підходи до оптимізації маршрутів і управління ресурсами, що підвищують ефективність та надійність безпроводових мереж.

Рекомендації щодо використання результатів дипломної роботи включають впровадження запропонованих методів у військових та цивільних мережах для підвищення мобільності та гнучкості комунікацій. Результати роботи можуть бути використані для подальшої розробки стандартів і протоколів для безпроводових мереж. Планується публікація результатів у наукових журналах та подання заявок на патенти.

Ключові слова: безпроводові мережі, самоорганізація, протоколи маршрутизації, управління ресурсами, архітектура, інтерфейси, стандарти, мобільність, гнучкість, надійність, оптимізація, ефективність.

ABSTRACT

This work contains 59 pages, 14 figures, 1 table, and 13 references.

The aim of the thesis is to study and analyze the principles of construction and operation of self-organizing wireless infocommunication networks. The main research methods were literature review and modeling.

The thesis examines the architectural principles of self-organizing wireless infocommunication networks, key routing protocols, resource management methods, interfaces, and standards. The obtained results include new approaches to route optimization and resource management, enhancing the efficiency and reliability of wireless networks.

Recommendations for the use of the thesis results include the implementation of the proposed methods in military and civilian networks to improve mobility and communication flexibility. The results can be used for further development of standards and protocols for wireless networks. It is planned to publish the results in scientific journals and submit patent applications.

Keywords: wireless networks, self-organization, routing protocols, resource management, architecture, interfaces, standards, mobility, flexibility, reliability, optimization, efficiency.

ЗМІСТ

ВСТУП.....	11
РОЗДІЛ 1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО БЕЗДРОТОВІ ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ ІЗ САМООРГАНІЗАЦІЄЮ	
1.1 Визначення бездротових інфокомунікаційних мереж із самоорганізацією та їх важливість у сучасному світі.....	13
1.2 Історія SON	15
1.3 Класифікація SON	18
1.3.1 Ad Hoc мережі.....	20
1.3.2 MANET, VANET, FANET мережі.....	22
1.3.3 Mesh мережі	23
1.3.4 WSN, UW-ASN мережі	25
1.3.5 Hybrid мережі.....	26
1.4 Особливості бездротових інфокомунікаційних мереж із самоорганізацією.....	30
1.5 Проблеми бездротових інфокомунікаційних мереж із самоорганізацією	32
Висновки	33
РОЗДІЛ 2. ПРИНЦИПИ ПОБУДОВИ І ФУНКЦІОНУВАННЯ БЕЗПРОВОДОВИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ.....	
2.1 Архітектурні принципи	34
2.2 Протоколи маршрутизації.....	37
2.3 Управління ресурсами в MANET мережі	42
2.4 Інтерфейси та стандарти	43
Висновки	46

РОЗДІЛ 3. СУЧАСНІ ПРИКЛАДИ ВИКОРИСТАННЯ БЕЗПРОВОДОВИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ	47
3.1 Архітектура C4ISR	47
3.2 In-door Mesh мережа на прикладі Omada EAP	51
3.3 БІМС військового призначення на прикладі радіостанції Nimera	53
Висновки	56
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	59

ПЕРЕЛІК СКОРОЧЕНЬ

SON	Self-Organizing Networks
БІМС	Бездротові інфокомунікаційні мережі із самоорганізацією
DSR	Dynamic Source Routing
OLSR	Optimized Link State Routing
AODV	Ad hoc On-Demand Distance Vector
OFDM	Orthogonal Frequency-Division Multiplexing

ВСТУП

У сучасному світі, де бездротові інфокомунікаційні мережі із самоорганізацією стають невід'ємною частиною нашого повсякденного життя, їх розвиток та вдосконалення набувають особливого значення. Ці мережі забезпечують широкий спектр послуг, включаючи передачу даних, голосовий зв'язок, доступ до Інтернету та багато іншого. Вони відіграють критичну роль у забезпеченні зв'язку в умовах динамічних змін та високих вимог до якості обслуговування.

Метою даної роботи є глибокий аналіз принципів побудови і функціонування бездротових інфокомунікаційних мереж із самоорганізацією, а також розробка та вдосконалення методів і технологій їх оптимізації. Основний акцент робиться на підвищенні продуктивності мереж, забезпеченні їх автономності та стійкості до збоїв, а також створенні нових алгоритмів і протоколів, що дозволяють мережам ефективно адаптуватися до змінних умов середовища та вимог користувачів.

Бездротові інфокомунікаційні мережі із самоорганізацією є важливою складовою сучасної інфраструктури, оскільки вони дозволяють швидко та ефективно встановлювати зв'язок у найрізноманітніших умовах. Такі мережі особливо корисні в ситуаціях, коли традиційні методи зв'язку не працюють, наприклад, під час надзвичайних ситуацій або у віддалених регіонах. Завдяки здатності до самоорганізації, ці мережі можуть самостійно налаштовувати свої параметри для забезпечення оптимальної роботи, що робить їх надзвичайно гнучкими та надійними.

У рамках роботи розглянуто сучасні виклики та проблеми, з якими стикаються бездротові інфокомунікаційні мережі із самоорганізацією. Серед таких викликів можна виділити високу динамічність топології мереж, обмеженість ресурсів, зокрема енергетичних та спектральних, необхідність швидкої адаптації до змін у навантаженні та умовах роботи.

Бездротові інфокомунікаційні мережі із самоорганізацією відкривають нові можливості для багатьох галузей, від військової справи до повсякденного життя, роблячи зв'язок більш доступним, надійним та гнучким. Ці мережі

дозволяють ефективно використовувати доступні ресурси, забезпечуючи високу якість зв'язку в будь-яких умовах. Удосконалення методів і технологій оптимізації роботи таких мереж забезпечить стабільний зв'язок, що має велике значення для підтримки різних застосувань, від промислових до побутових.

РОЗДІЛ 1

ЗАГАЛЬНІ ВІДОМОСТІ ПРО БЕЗДРОТОВІ ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ ІЗ САМООРГАНІЗАЦІЄЮ

1.1 Визначення бездротових інфокомунікаційних мереж із самоорганізацією та їх важливість у сучасному світі.

Автоматизовані мережі із самоорганізацією (Self-Organizing Networks, SON) є технологією автоматизації, яка спрямована на спрощення та прискорення планування, конфігурації, управління, оптимізації та відновлення мобільних радіодоступних мереж. Функціональність та поведінка SON були визначені і специфіковані у загальновизнаних рекомендаціях мобільної індустрії, створених такими організаціями, як 3GPP (3rd Generation Partnership Project) та NGMN (Next Generation Mobile Networks)[1].

SON була закодована у 3GPP Release 8 та наступних специфікаціях у серії стандартів, включаючи 36.902, а також у публічних білих книгах, які описують варіанти використання від NGMN. Першою технологією, що використовувала функції SON, стала Long Term Evolution (LTE), але ця технологія також була адаптована для старіших технологій радіодоступу, таких як Universal Mobile Telecommunications System (UMTS). Специфікація LTE від початку підтримує функції SON, такі як автоматичне виявлення сусідніх відносин (ANR), яка є флагманською функцією 3GPP LTE Release 8.

Нові базові станції повинні самоконфігуруватися відповідно до парадигми "plug-and-play", тоді як усі діючі базові станції регулярно самостійно оптимізуватимуть параметри та алгоритмічну поведінку у відповідь на спостережувану продуктивність мережі та радіоумови. Крім того, функція самооздоровлення (self-healing) дозволяє мережі автоматично виявляти та виправляти несправності, забезпечуючи стабільну роботу без необхідності втручання людини.

Основною характеристикою таких мереж є топологія "Ad Hoc", яка визначається як випадкова, спонтанна і спеціально створена для визначених цілей. У таких мережах вузли можуть вільно приєднуватися і залишати мережу, забезпечуючи високу гнучкість і масштабованість. Відсутність

централізованого управління означає, що кожен вузол у мережі має можливість приймати самостійні рішення, що забезпечує децентралізоване управління.

Топологія "Ad Hoc" базується на принципі прямої радіовидимості, де дані передаються від одного вузла до іншого, якщо вони знаходяться в межах досяжності. Якщо два вузли не можуть спілкуватися безпосередньо, використовуються інші вузли як ретранслятори для пересилання пакетів, що дозволяє створити мережу з динамічно змінюваною топологією. Така структура дозволяє мережі автоматично адаптуватися до змін у навколишньому середовищі і забезпечує надійну передачу даних у складних умовах.

Децентралізоване управління в таких мережах здійснюється за рахунок "інтелектуальних" автономних вузлів. Кожен вузол в мережі може виступати як хост (джерело і приймач інформації) і як маршрутизатор, що передає дані від одного вузла до іншого. Це дозволяє мережі функціонувати без необхідності в централізованому контролері, знижуючи ризики відмови вразливих точок і підвищуючи загальну стійкість мережі.

З розвитком технологій самоорганізуючі мережі стали невід'ємною частиною сучасних мобільних мереж, таких як LTE і 5G. Впровадження SON у ці мережі дозволяє автоматично налаштовувати параметри базових станцій, оптимізувати використання спектра і забезпечувати самооздоровлення мережі. Наприклад, функція автоматичного виявлення сусідніх відносин (Automatic Neighbor Relation, ANR) у LTE дозволяє базовим станціям автоматично виявляти та налаштовувати свої зв'язки із сусідніми станціями, забезпечуючи оптимальну конфігурацію мережі.

Одним з ключових напрямків розвитку SON є інтеграція технологій машинного навчання та штучного інтелекту, що дозволяє мережам краще адаптуватися до змін умов та прогнозувати потреби у ресурсах. Наприклад, системи штучного інтелекту можуть аналізувати великі обсяги даних про стан мережі та поведінку користувачів, щоб оптимізувати розподіл ресурсів у реальному часі, знижуючи затримки та підвищуючи пропускну здатність.

Іншим важливим аспектом є розвиток мереж на основі програмно-визначених мереж (SDN) і мережевої функціональної віртуалізації (NFV). Ці технології

дозволяють створювати більш гнучкі і масштабовані мережі, де фізичні ресурси можуть бути динамічно перепризначені для різних задач. Інтеграція SON з SDN і NFV дозволяє автоматизувати багато процесів управління мережею, знижуючи витрати та підвищуючи ефективність.

Використання SON також є критично важливим для розвитку Інтернету речей (IoT), де велика кількість пристроїв потребує ефективної координації та управління. Автоматизація процесів управління у таких мережах дозволяє забезпечити надійну і стабільну роботу навіть при великій кількості підключених пристроїв.

Загалом, бездротові інфокомунікаційні мережі із самоорганізацією є важливим кроком у напрямку створення більш розумних і ефективних телекомунікаційних систем. Вони дозволяють забезпечити високу гнучкість, надійність та ефективність у різних умовах використання, що робить їх ключовим елементом у сучасному та майбутньому розвитку мобільних і бездротових комунікацій.

1.2 Історія SON.

Автоматизовані мережі із самоорганізацією (SON) з'явилися як відповідь на зростаючу складність та обсяги мобільних мереж, а також на потребу в більш ефективному управлінні цими мережами. Історія SON починається з концепцій автоматизації та самооптимізації, які з'явилися ще в 1990-х роках, але значного розвитку набули на початку 2000-х.

Ранні роботи в цій сфері зосереджувалися на автоматизації окремих завдань, таких як налаштування параметрів базових станцій та управління ресурсами. У цей час мобільні мережі другого покоління (2G) вже були широко поширені, а мобільні оператори стикалися з проблемами управління великим числом базових станцій та зростаючою кількістю користувачів. Концепція самоорганізації отримала підтримку завдяки дослідженням, проведеним у наукових колах та промислових лабораторіях.

З появою мобільних мереж третього покоління (3G) у 2000-х роках проблема управління мережею стала ще більш гострою. Зросла потреба у передачі даних, і мережі стали більш складними. Це сприяло розвитку нових методів автоматизації. Перші кроки у напрямку SON включали автоматичне налаштування параметрів радіомережі (Radio Network Optimization, RNO) та управління трафіком (Traffic Management).

Концепція SON набула офіційного визнання у мобільній індустрії з публікацією стандартів 3GPP Release 8 у 2008 році. Цей реліз включав специфікації для LTE (Long Term Evolution), де були вперше інтегровані функції SON [2]. Основною метою було зменшення витрат на управління мережею та покращення її продуктивності шляхом автоматизації процесів, які раніше вимагали ручного втручання. Це включало такі функції, як автоматичне виявлення сусідніх відносин (Automatic Neighbor Relation, ANR), автоматична оптимізація параметрів мережі та самооздоровлення (self-healing).

З впровадженням LTE та поширенням 4G технології SON стали стандартною практикою для багатьох операторів. LTE від самого початку була розроблена з урахуванням можливостей SON, що дозволило автоматично налаштовувати параметри базових станцій та оптимізувати мережу у реальному часі на основі актуальних даних про продуктивність. Це значно полегшило завдання інженерів з управління мережею та покращило якість обслуговування користувачів.

Однією з ключових функцій SON у LTE стала ANR, яка дозволяє базовим станціям автоматично виявляти та налаштовувати свої зв'язки із сусідніми станціями, забезпечуючи оптимальну конфігурацію мережі. Це значно зменшило час та витрати на налаштування мережі, особливо під час розгортання нових базових станцій. Інші важливі функції включали автоматичну оптимізацію (self-optimization), яка дозволяє мережі адаптуватися до змін умов у реальному часі, та самооздоровлення (self-healing), яке забезпечує автоматичне виявлення та виправлення несправностей.

Сучасні мобільні мережі п'ятого покоління (5G) продовжують розвивати концепцію SON. 5G мережі мають ще більшу складність та вимоги до

продуктивності, що робить функції SON критично важливими для їх успішного функціонування. У 5G SON забезпечує автоматизацію не лише для базових станцій, але й для мережесих функцій на більш високих рівнях архітектури, включаючи управління трафіком, оркестрацію ресурсів та адаптацію до різних сценаріїв використання.

Окрім цього, впровадження SON у 5G сприяє розвитку технологій Інтернету речей (IoT), автономного транспорту та розумних міст, де велика кількість пристроїв та складна мережна інфраструктура потребують високого рівня автоматизації та гнучкості. Завдяки SON, 5G мережі можуть автоматично адаптуватися до змін умов, забезпечуючи стабільну та ефективну роботу в різних сценаріях використання.

Важливу роль у розвитку SON відіграють також галузеві консорціуми та організації, такі як NGMN (Next Generation Mobile Networks), які публікують білі книги та рекомендації щодо використання SON у мобільних мережах. Ці організації працюють над стандартизацією та поширенням найкращих практик для впровадження SON, що сприяє їхньому широкому використанню у галузі.

Історія створення SON також тісно пов'язана з еволюцією радіомереж та технологій бездротового зв'язку: у 1970-х роках Гавайський університет реалізував проєкт ALOHA, який став одним із перших значущих досягнень у галузі бездротових інфокомунікацій. ALOHAnet, розроблений під керівництвом професора Нормана Абрамсона, був першим, хто використав радіокомунікації для з'єднання комп'ютерів. Одним з основних технічних досягнень було впровадження протоколів випадкового доступу, які дозволяли комп'ютерам передавати пакети даних "за бажанням", що призводило до зіткнень, але з можливістю повторної передачі після збою.

Проєкт ALOHA заклав основу для багатьох сучасних технологій, включаючи Wi-Fi та Ethernet. Одним з важливих принципів було простота протоколу: передача, очікування підтвердження та повторна передача у разі відсутності підтвердження. Цей підхід був застосований і вдосконалений в інших мережах, таких як Ethernet, що зробило ALOHA основою для багатьох сучасних систем зв'язку.

На початку 1970-х років також було створено першу в Європі пакетну радіомережу "Дискрет" у Києві під керівництвом С.Г. Буніна та А.П. Войтера. Ця мережа стала важливим етапом у розвитку бездротових інфокомунікацій в Європі.

У 1972 році Міністерство оборони США та DARPA запустили проект PRNET, який став основою для розвитку пакетних радіомереж. У 1980-х роках з'явилися перші зразки PRNET та CNR в США, а в СРСР були розроблені комплекси "Базальт" і "Редут". PRNET став основою для майбутніх мережевих технологій, використовуючи мобільні мережі для військових застосувань.

У 1994 році DARPA розпочала програму GloMo, що сприяла подальшому розвитку мобільних мереж, закладаючи основи для сучасних мобільних комунікаційних систем. У кінці 1990-х з'явилися технології Wi-Fi (стандарт IEEE 802.11) та Bluetooth, які значно розширили можливості бездротових комунікацій, ставши важливими етапами у їх розвитку.

Ці події демонструють еволюцію бездротових інфокомунікаційних мереж від ранніх експериментальних систем до сучасних технологій, які зараз використовуються у повсякденному житті. Впровадження та розвиток цих технологій значно вплинуло на те, як ми сьогодні взаємодіємо з інформаційними системами і забезпечують основи для постійного розвитку галузі бездротових комунікацій.

1.3 Класифікація SON

БІМС класифікуються за кількома ключовими ознаками. Ця класифікація охоплює спосіб управління, мобільність, ширину каналу, спосіб розділення радіоресурсу, обладнання вузлів і площу покриття.

Спосіб управління БІМС може бути однорівневим або ієрархічним. В однорівневих мережах всі вузли мають рівний статус і можуть взаємодіяти безпосередньо один з одним. Такі мережі простіші в реалізації, але можуть страждати від проблем із масштабованістю та ефективністю при великій кількості вузлів. Ієрархічні мережі мають кілька рівнів управління, де вузли

вищого рівня керують вузлами нижчого рівня, що дозволяє краще керувати великими мережами, але вимагає більш складних алгоритмів управління і підтримки.

Мобільність у БІМС може бути стаціонарною, мобільною або гібридною. Стаціонарні мережі складаються з фіксованих вузлів, які не змінюють свого місця розташування, що спрощує управління мережею та стабільність зв'язку. Мобільні мережі, навпаки, складаються з вузлів, які можуть вільно переміщуватися, що вимагає динамічних протоколів маршрутизації і складнішої організації мережових з'єднань. Гібридні мережі поєднують в собі характеристики стаціонарних та мобільних мереж, що дозволяє гнучко адаптуватися до різних сценаріїв використання.

Ширина каналу в БІМС може бути вузькосмуговою, широкосмуговою або надширокосмуговою (I-UWB). Вузькосмугові канали мають обмежену пропускну здатність, але забезпечують високу стабільність і низький рівень інтерференції. Широкосмугові канали дозволяють передавати більші обсяги даних, але можуть бути більш вразливими до інтерференції і потребують складнішого управління. Надширокосмугові канали (I-UWB) використовують широкий діапазон частот, що дозволяє досягати високих швидкостей передачі даних і забезпечувати високу стійкість до інтерференції, але вимагає спеціалізованого обладнання і складних протоколів.

Спосіб розділення радіоресурсу може бути детермінований або випадковий. Детерміновані методи розділення передбачають чітко визначені часові, частотні або кодові інтервали для кожного вузла, що забезпечує високу ефективність і передбачуваність, але вимагає складного планування і управління. Випадкові методи, такі як ALOHA або CSMA/CA, дозволяють вузлам динамічно захоплювати радіоресурси, що спрощує організацію мережі, але може призводити до колізій і зниження ефективності при великій кількості вузлів.

Обладнання вузлів у БІМС включає хости та маршрутизатори. Хости є кінцевими пристроями, які відправляють і приймають дані, тоді як маршрутизатори забезпечують пересилання пакетів між хостами і іншими

маршрутизаторами в мережі. Маршрутизатори можуть виконувати додаткові функції, такі як балансування навантаження, управління потоками і забезпечення безпеки даних.

Площа покриття БІМС може бути різною, залежно від призначення мережі. Персональні мережі (PAN) охоплюють невеликі зони, зазвичай в межах одного користувача або кількох пристроїв, що знаходяться поблизу. Локальні мережі (LAN) охоплюють більші площі, такі як офіси або будинки. Міські мережі (MAN) охоплюють міські території і можуть використовуватися для забезпечення зв'язку в рамках одного або кількох міст. Широкомасштабні мережі (WAN) охоплюють великі географічні області і можуть включати в себе національні або міжнародні мережі. Спеціалізовані мережі, такі як військові, домашні сенсорні або інші мережі, мають специфічні вимоги до безпеки, надійності та швидкості передачі даних, що вимагає використання спеціальних протоколів і технологій.

Таким чином, класифікація БІМС за цими ознаками дозволяє краще зрозуміти їх різноманітність, особливості та можливості, що сприяє ефективнішому проектуванню, впровадженню та експлуатації таких мереж у різних галузях і сценаріях використання.

1.3.1 Ad Hoc мережі

Ad Hoc мережі, відомі також як ad hoc networks, є тимчасовими мережами, які формуються "на ходу" без попередньо визначеної інфраструктури чи централізованого управління. Ці мережі створюються за потреби для конкретних цілей і можуть бути швидко згорнуті після виконання своїх завдань. Основні характеристики Ad Hoc мереж включають автономність, самоорганізацію, динамічну топологію, гнучкість і розподілену природу управління.

У мережах типу Ad Hoc кожен вузол діє як і хост, і маршрутизатор, тобто він може як генерувати, так і ретранслювати пакети даних. Це забезпечує гнучкість і дозволяє вузлам безпосередньо спілкуватися між собою, якщо вони

знаходяться в зоні дії один одного, або через проміжні вузли, якщо прямий зв'язок неможливий.

Однією з основних особливостей Ad Hoc мереж є їх динамічна топологія. Вузли можуть вільно переміщатися, що призводить до постійних змін у структурі мережі. Це створює додаткові виклики для розробки ефективних алгоритмів маршрутизації. У таких мережах широко використовуються протоколи, що здатні адаптуватися до частих змін, наприклад, протоколи AODV та DSR [3].

Ad Hoc мережі можуть застосовуватися в різних ситуаціях, де традиційна інфраструктура недоступна або її використання недоцільне. Приклади таких ситуацій включають військові операції, екстрені рятувальні роботи, організацію тимчасових заходів (конференцій, фестивалів), а також у місцях стихійних лих, де стаціонарна інфраструктура може бути зруйнована.

Основними перевагами Ad Hoc мереж є їх швидке розгортання, відсутність необхідності у фіксованій інфраструктурі та висока гнучкість. Вони можуть забезпечити зв'язок у віддалених та важкодоступних районах, де встановлення традиційних мереж було б надто дорогим або фізично неможливим.

Проте існують також суттєві виклики та недоліки. Динамічна природа топології може призводити до нестабільності зв'язку та зниження продуктивності мережі. Проблеми з масштабованістю виникають при збільшенні кількості вузлів, оскільки це ускладнює маршрутизацію та збільшує кількість колізій. Безпека також є значною проблемою, оскільки відсутність централізованого управління ускладнює аутентифікацію та захист даних від несанкціонованого доступу.

Ad Hoc мережі знаходять своє місце в розвитку майбутніх технологій, таких як Інтернет речей (IoT), де велика кількість пристроїв може динамічно взаємодіяти без централізованої інфраструктури. Такі мережі також мають перспективу в розвитку розумних міст, де вони можуть забезпечувати гнучкий та адаптивний зв'язок між різними елементами міської інфраструктури.

Для створення та підтримки ефективних Ad Hoc мереж необхідні вдосконалені алгоритми маршрутизації, протоколи з низьким енергоспоживанням, а також надійні методи забезпечення безпеки. Дослідження в цій галузі продовжуються, спрямовані на вирішення існуючих проблем та оптимізацію функціонування таких мереж.

1.3.2 MANET, VANET, FANET мережі

MANET (Mobile Ad Hoc Network) – це тип бездротової мережі, де мобільні вузли динамічно організовують мережу без використання попередньо налаштованої інфраструктури чи централізованого управління. У MANET кожен вузол одночасно виступає як маршрутизатор і передавач інформації, забезпечуючи ретрансляцію пакетів до інших вузлів. MANET характеризуються високою динамічністю топології через постійне переміщення вузлів, що може викликати часті зміни в маршрутах передачі даних. Для забезпечення надійної передачі даних у таких мережах використовуються різні алгоритми маршрутизації, зокрема AODV, DSR та OLSR.

Основними перевагами MANET є швидке розгортання, гнучкість і відсутність необхідності в стаціонарній інфраструктурі. Це робить їх ідеальними для застосування у військових умовах, екстрених ситуаціях, при стихійних лихах та у віддалених районах, де немає можливості використовувати традиційні мережі. Проте MANET мають і свої недоліки, такі як обмежена пропускна здатність, високе енергоспоживання і складнощі з забезпеченням безпеки даних через їх відкриту природу.

VANET (Vehicular Ad Hoc Network) – це підвид MANET, що спеціалізується на комунікаціях між транспортними засобами (автомобілями, автобусами) та між транспортними засобами й інфраструктурою (наприклад, дорожніми знаками, світлофорами). Основною метою VANET є підвищення безпеки дорожнього руху та оптимізація транспортних потоків. Вузли в VANET постійно змінюють своє місцезнаходження, що ускладнює процес маршрутизації. Для вирішення цих проблем використовуються спеціалізовані

протоколи маршрутизації, такі як GPSR (Greedy Perimeter Stateless Routing) та GSR (Geographic Source Routing) [4].

Однією з ключових функцій VANET є обмін інформацією про дорожні умови, такі як аварії, затори та погодні умови. Це дозволяє водіям отримувати своєчасні попередження і приймати відповідні заходи для уникнення небезпечних ситуацій. Крім того, VANET підтримують функції розважальних систем і покращення сервісів для пасажирів, таких як доступ до інтернету.

FANET (Flying Ad Hoc Network) – це тип MANET, де вузлами мережі є безпілотні літальні апарати (БПЛА). FANET використовуються для виконання різних завдань, таких як спостереження, розвідка, пошуково-рятувальні операції та доставка вантажів. У FANET кожен БПЛА може виконувати роль ретранслятора сигналу, що дозволяє значно розширити зону покриття мережі і забезпечити надійну передачу даних навіть у складних умовах.

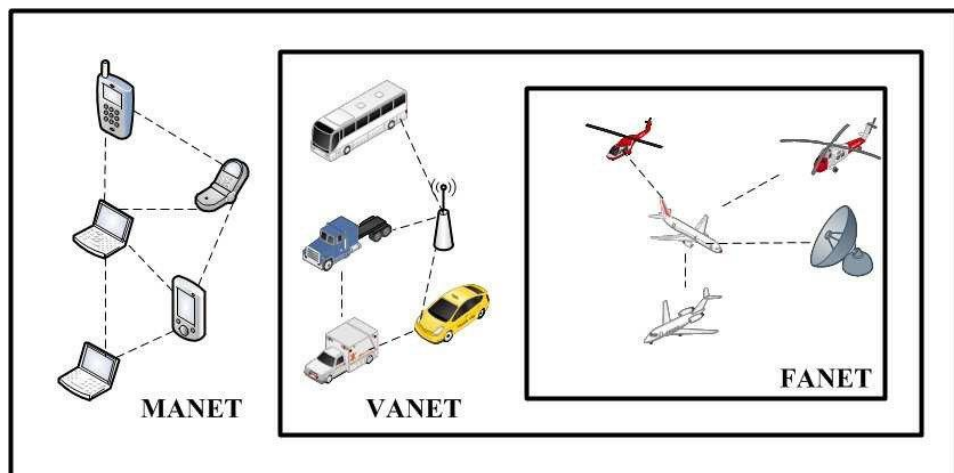


Рис.1.1 Области застосування MANET, VANET, FANET мереж

Особливістю FANET є їх тривимірна мобільність, що створює додаткові виклики для алгоритмів маршрутизації. Протоколи, розроблені для FANET, повинні враховувати швидке переміщення вузлів і зміну їх висоти. Крім того, FANET вимагають високої надійності та низької затримки при передачі даних, що важливо для виконання критично важливих місій. Важливими аспектами FANET є енергоефективність та оптимізація траєкторії руху БПЛА для мінімізації витрат енергії.

1.3.3 Mesh мережі

Mesh мережі – це тип бездротових мереж, в яких вузли організовані таким чином, що кожен вузол може передавати дані до будь-якого іншого вузла без необхідності використовувати централізований маршрутизатор чи інфраструктуру. Вузли в Mesh мережах працюють як маршрутизатори, ретранслюючи дані на інші вузли. Це дозволяє створити надійні та саморегулюючі мережі з високою стійкістю до збоїв, оскільки у разі виходу з ладу одного вузла, дані можуть перенаправлятися через інші вузли.

Основними характеристиками Mesh мереж є їх самоконфігурація та самовідновлення. Самоконфігурація дозволяє вузлам автоматично налаштовувати зв'язки з іншими вузлами при приєднанні до мережі, що спрощує процес розгортання мережі. Самовідновлення забезпечує підтримку зв'язку навіть у випадку зміни топології мережі, наприклад, коли один з вузлів виходить з ладу або змінює своє місцезнаходження. Ці властивості роблять Mesh мережі особливо придатними для використання у динамічних умовах, де мережеві структури часто змінюються.

Для маршрутизації в Mesh мережах використовуються спеціальні протоколи, такі як AODV, DSR та OLSR. Ці протоколи забезпечують ефективну передачу даних, враховуючи динамічні зміни топології мережі та мінімізуючи затримки при передачі. Протоколи можуть адаптуватися до змін у мережі, забезпечуючи таким чином надійну та безперебійну передачу даних.

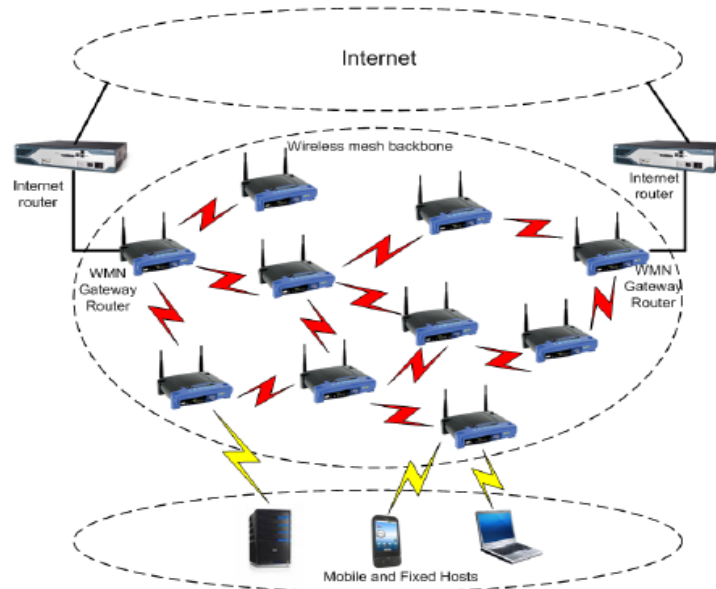


Рис.1.2 Приклад Mesh мережі

Однією з важливих переваг Mesh мереж є їх висока масштабованість. Додавання нових вузлів до мережі не потребує значних змін у конфігурації існуючих вузлів, оскільки нові вузли автоматично інтегруються у мережу. Це робить Mesh мережі ідеальними для великих інфраструктурних проєктів, таких як розумні міста, де необхідно забезпечити зв'язок між великою кількістю датчиків та пристроїв.

Mesh мережі також мають високу стійкість до відмов. Оскільки кожен вузол може зв'язуватися з декількома іншими вузлами, мережа може продовжувати функціонувати навіть у випадку виходу з ладу декількох вузлів. Це робить Mesh мережі привабливими для застосування у військових та рятувальних операціях, де надійність зв'язку є критично важливою.

Ще однією важливою особливістю Mesh мереж є їх здатність до адаптивного розширення. Це означає, що мережа може автоматично адаптуватися до змін у кількості вузлів та їх розташуванні, що забезпечує постійну оптимізацію маршрутизації даних та ефективне використання мережевих ресурсів. Завдяки цьому Mesh мережі можуть використовуватися у різноманітних сценаріях, таких як сільськогосподарські технології, де сенсори та пристрої можуть бути розташовані на великих відстанях один від одного.

Застосування Mesh мереж включає розумні будинки, розумні міста, промислові IoT системи, а також військові та екстрені комунікаційні системи [5]. Вони забезпечують високу гнучкість та надійність зв'язку, дозволяючи користувачам ефективно управляти великими кількістю пристроїв та датчиків.

1.3.4 WSN, UW-ASN мережі

WSN (Wireless Sensor Networks) та UW-ASN (Underwater Acoustic Sensor Networks) є двома типами бездротових інфокомунікаційних мереж, які мають свої особливості та застосування.

WSN – це мережі, які складаються з великої кількості сенсорних вузлів, що мають обмежені обчислювальні ресурси, енергію та здатність до зберігання даних. Основною метою WSN є збір, обробка та передача даних з навколишнього середовища, таких як температура, вологість, тиск, рух тощо. Сенсорні вузли зазвичай розташовуються у віддалених або важкодоступних місцях і передають зібрану інформацію через бездротовий зв'язок до центрального вузла або базової станції для подальшого аналізу.

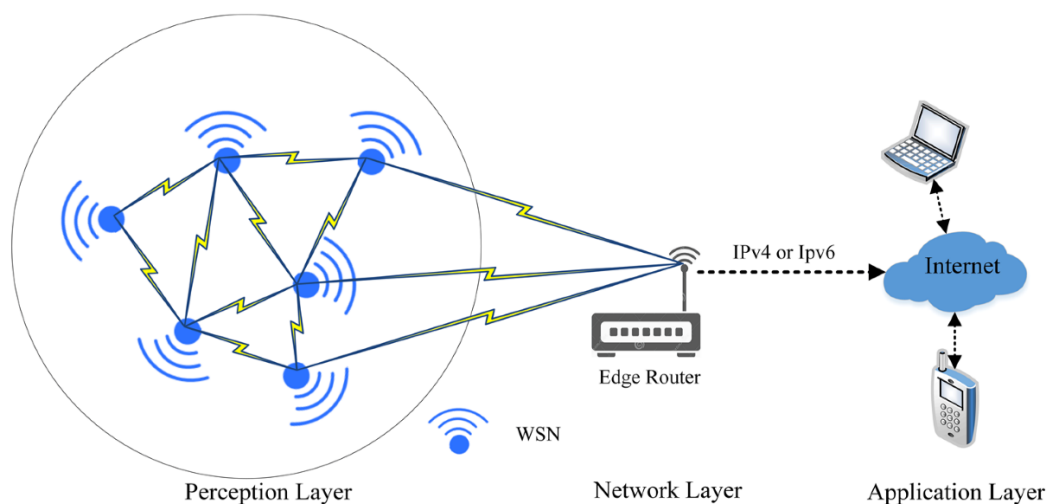


Рис.1.3 Приклад WSN мережі

Ключовими характеристиками WSN є низьке енергоспоживання, висока надійність передачі даних, можливість самоорганізації та самовідновлення. Протоколи передачі даних, такі як Zigbee, Z-Wave та 6LoWPAN, забезпечують ефективну роботу WSN при мінімальному використанні енергії. Сенсорні вузли можуть бути обладнані різноманітними датчиками, що дозволяє використовувати WSN у широкому спектрі застосувань, таких як моніторинг навколишнього середовища, промисловий контроль, охорона здоров'я, військові застосування та розумні міста.

UW-ASN – це тип бездротових мереж, які використовуються для збору та передачі даних у підводному середовищі. Вузли UW-ASN використовують акустичні хвилі для передачі даних, оскільки радіохвилі дуже погано поширюються у воді. Основними завданнями UW-ASN є моніторинг підводного середовища, дослідження океанів, забезпечення безпеки підводних об'єктів та контроль за підводними інфраструктурами, такими як нафтові платформи та підводні кабелі.

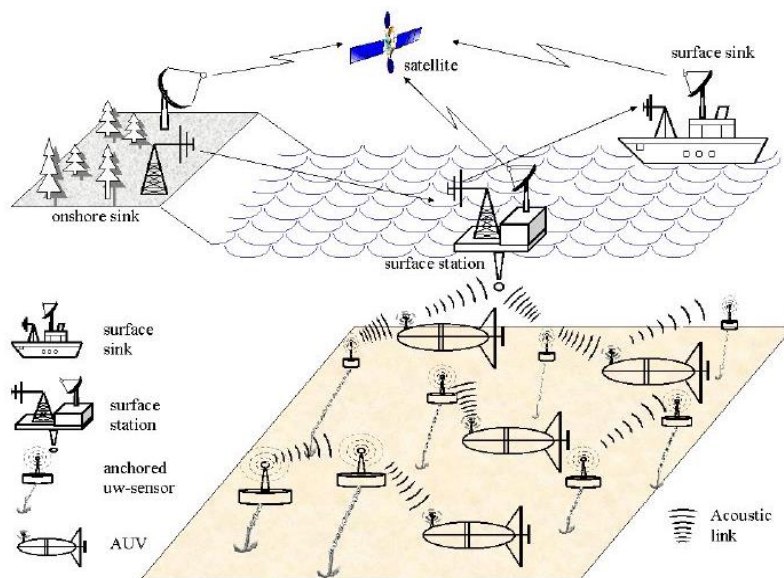


Рис.1.4 Приклад UW-ASN мережі

UW-ASN мають свої особливості та виклики, такі як висока затримка передачі, низька пропускна здатність та високе енергоспоживання порівняно з наземними WSN. Для подолання цих проблем використовуються спеціальні

протоколи, такі як T-Lohi (Tone Lohi) та інших адаптованих для підводного середовища методів передачі даних. UW-ASN вузли часто обладнані акустичними модемами, гідрофонами та іншими сенсорами для збору даних про підводне середовище, такі як солоність, температура, глибина та інші параметри [6].

Застосування WSN та UW-ASN включають моніторинг навколишнього середовища, промислові системи контролю, військові операції та наукові дослідження. Наприклад, WSN використовуються для моніторингу лісових пожеж, вимірювання забруднення повітря та води, контролю за станом мостів та будівель, а також для збору медичних даних у реальному часі. UW-ASN використовуються для моніторингу морського життя, виявлення підводних течій, забезпечення безпеки портів та берегових ліній, а також для контролю за підводними інфраструктурами.

1.3.5 Hybrid мережі

Гібридні мережі (Hybrid networks) представляють собою комбінацію різних типів мереж, що дозволяє поєднувати переваги кожної з них для забезпечення високої надійності, ефективності та масштабованості. Гібридні мережі об'єднують традиційні інфраструктурні мережі з бездротовими ad-hoc мережами, створюючи гнучку та динамічну систему, яка може адаптуватися до різноманітних умов та вимог користувачів.

Основною перевагою гібридних мереж є їх здатність забезпечувати безперервний та надійний зв'язок навіть у випадку часткових відмов мережі або змін у топології. Це досягається завдяки інтеграції стаціонарних базових станцій із мобільними вузлами, які можуть взаємодіяти між собою безпосередньо або через базові станції. У випадку, коли мобільний вузол втрачає з'єднання з базовою станцією, він може передавати дані через інші вузли мережі ad-hoc, що значно підвищує загальну надійність мережі.

Гібридні мережі можуть використовуватися в різних сферах, включаючи військові операції, де важливо мати надійний та безперервний зв'язок навіть у складних умовах. Також вони застосовуються у сфері громадської безпеки, де

під час надзвичайних ситуацій необхідно швидко розгорнути мережу зв'язку. Крім того, гібридні мережі використовуються в розумних містах (smart cities) для забезпечення зв'язку між різними сенсорами та пристроями Інтернету речей (IoT).

Інтеграція різних типів мереж у гібридних системах дозволяє використовувати різні протоколи та технології зв'язку, що забезпечує високу адаптивність до умов навколишнього середовища. Наприклад, у гібридних мережах можуть застосовуватися як стільникові мережі (наприклад, LTE або 5G), так і бездротові локальні мережі (Wi-Fi), а також мережі ad-hoc, такі як MANET (Mobile Ad Hoc Networks).

Гібридні мережі також дозволяють оптимізувати використання ресурсів мережі завдяки адаптивному маршрутизації та управлінню ресурсами. Наприклад, в умовах високого навантаження на стаціонарні базові станції трафік може бути перенаправлений через мобільні вузли ad-hoc, що допомагає розподілити навантаження і запобігти перевантаженню мережі. Крім того, гібридні мережі можуть використовувати різні частотні діапазони для забезпечення зв'язку, що підвищує їх стійкість до перешкод та інтерференції.

Для управління та оптимізації роботи гібридних мереж застосовуються передові алгоритми маршрутизації, які враховують динамічну природу мобільних вузлів та різні характеристики каналів зв'язку. Наприклад, протоколи, такі як AODV та DSR, можуть бути адаптовані для роботи у гібридних мережах, забезпечуючи ефективну маршрутизацію даних навіть у складних умовах.

Загалом, гібридні мережі представляють собою потужний інструмент для забезпечення надійного та ефективного зв'язку в різноманітних умовах та сценаріях використання. Їх здатність поєднувати переваги різних типів мереж робить їх особливо привабливими для застосування у сфері громадської безпеки, військових операцій, розумних міст та інших критично важливих застосувань.

1.4 Особливості бездротових інфокомунікаційних мереж із самоорганізацією

Бездротові інфокомунікаційні мережі із самоорганізацією (БІМС) мають ряд особливостей, які відрізняють їх від традиційних мереж. Першою особливістю є змінювана кількість вузлів і площа покриття мережею. Вузли можуть динамічно приєднуватися або виходити з мережі, що змінює її топологію та охоплення. Ця змінюваність вимагає гнучких алгоритмів маршрутизації, які можуть адаптуватися до постійних змін у мережі.

Мобільність і стаціонарність вузлів є другою важливою особливістю. У БІМС можуть бути як мобільні вузли, що переміщуються, так і стаціонарні вузли, що залишаються на одному місці. Мобільні вузли додають додаткову складність через постійне змінення топології, в той час як стаціонарні вузли можуть слугувати опорними точками для маршрутизації та стабільних з'єднань. Випадковість топології мережі, її неоднорідність і динамічність зміни є ще однією характерною особливістю. Топологія мережі може змінюватися внаслідок руху вузлів, зміни умов навколишнього середовища або інших факторів. Це робить мережу неоднорідною і вимагає використання алгоритмів маршрутизації, які можуть ефективно працювати в таких умовах, як наприклад, алгоритм OLSR або AODV.

Принцип передачі інформації в БІМС базується на комутації пакетів із багато стрибковою маршрутизацією. Це означає, що дані передаються через мережу шляхом переміщення від одного вузла до іншого, поки не досягнуть кінцевого пункту призначення. Багатострибкова маршрутизація дозволяє покращити охоплення мережі та забезпечити зв'язок між вузлами, які знаходяться на великій відстані один від одного. В цьому контексті важливим є використання протоколів маршрутизації, що підтримують надійність і ефективність передачі даних, наприклад, протоколи на основі вектору відстаней або стану зв'язку.

Децентралізоване управління є ключовою особливістю БІМС. У таких мережах немає централізованого контролера, і всі вузли рівноправно беруть участь в управлінні та обробці даних. Це підвищує стійкість мережі до відмов окремих вузлів, оскільки функції управління розподілені між усіма вузлами. Децентралізовані алгоритми, такі як алгоритми на основі консенсусу або розподілених хеш-таблиць (DHT), є важливими для ефективного функціонування таких мереж.

Багатоканальність мереж є ще однією важливою особливістю. Вона дозволяє одночасно використовувати кілька каналів для передачі даних, що збільшує загальну пропускну здатність мережі та зменшує ймовірність перешкод між каналами. Використання технологій, таких як MIMO (Multiple Input Multiple Output) та OFDMA (Orthogonal Frequency Division Multiple Access), допомагає ефективно управляти багатоканальними ресурсами.

Масштабованість є важливою характеристикою БІМС, яка дозволяє мережі ефективно функціонувати при збільшенні кількості вузлів. Це вимагає розробки алгоритмів та протоколів, які можуть підтримувати продуктивність мережі незалежно від її розміру. Наприклад, протоколи маршрутизації з ієрархічною структурою, такі як HSR (Hierarchical State Routing), можуть забезпечити ефективну маршрутизацію у великих мережах.

Обмеженість ресурсів вузлів мережі є ще однією суттєвою проблемою. Більшість вузлів у БІМС мають обмежені обчислювальні потужності, обсяг пам'яті та енергетичні ресурси. Це вимагає розробки енергоефективних алгоритмів та протоколів, що мінімізують використання ресурсів. Наприклад, використання протоколів, які зменшують кількість обмінів повідомленнями та обчислень, є критичним для продовження часу роботи вузлів від батареї.

Обмежена безпека мережі також є важливою проблемою для БІМС. Відкритий характер бездротових каналів зв'язку робить мережі вразливими до різних атак, таких як перехоплення даних, атаки на відмову в обслуговуванні (DoS) та атаки типу "людина посередині". Для забезпечення безпеки використовуються різні методи шифрування, автентифікації та управління

доступом. Протоколи безпеки, такі як WPA3 та IPSec, допомагають захистити дані та забезпечити конфіденційність і цілісність інформації в мережі.

1.5 Проблеми бездротових інфокомунікаційних мереж із самоорганізацією

Бездротові інфокомунікаційні мережі із самоорганізацією (БІМС) стикаються з низкою технічних проблем, що впливають на їх ефективність і надійність. Однією з головних проблем є організація надійного транспорту даних при змінній топології мережі. У БІМС вузли можуть переміщуватися, виходити з мережі або приєднуватися до неї, що викликає постійні зміни топології. Це ускладнює підтримку стабільних маршрутів для передачі даних. Для вирішення цієї проблеми розробляються алгоритми маршрутизації, такі як AODV і DSR, які динамічно адаптуються до змін у мережі.

Підвищення швидкості передачі інформації обмежується виділенням частотним ресурсом (ЧР) і множинним доступом до спільного ресурсу (МД). Частотний спектр, доступний для бездротових комунікацій, є обмеженим, що викликає проблеми з пропускну здатністю, особливо в умовах високої щільності вузлів. Технології, такі як OFDM та когнітивне радіо, використовуються для оптимізації використання частотного спектра і підвищення ефективності передачі даних.

Створення ефективних методів управління на різних рівнях моделі OSI є ще однією критичною проблемою. Управління ресурсами, такими як пропускну здатність, енергія та пам'ять, вимагає комплексного підходу, що враховує всі рівні моделі OSI. Наприклад, на рівні мережі важливо використовувати енергоефективні протоколи маршрутизації, тоді як на транспортному рівні необхідно забезпечувати надійність передачі даних і мінімальні затримки.

Використання обмежених ресурсів вузлів, таких як обсяг пам'яті, процесорна потужність (CPU), ємність акумуляторних батарей (АкБ) та інші, також становить значну проблему. У мобільних вузлах часто є обмежені ресурси, що потребує розробки енергоефективних алгоритмів і протоколів, які

мінімізують споживання енергії без зниження продуктивності мережі. Технології, такі як енергозберігаюча маршрутизація та адаптивне керування живленням, допомагають продовжити час роботи вузлів.

Забезпечення якості обслуговування (QoS) для різних типів трафіку є критичним завданням, особливо у мережах, що підтримують мультимедійні сервіси, відеоконференції та VoIP (Voice over IP). QoS вимагає пріоритизації трафіку і управління затримками, джитером та втратами пакетів. Механізми, такі як диференційовані послуги (DiffServ) і інтегровані послуги (IntServ), використовуються для забезпечення необхідного рівня обслуговування для різних класів трафіку [7].

Проблема масштабування і адресації в мережах великої розмірності пов'язана з ефективною організацією та управлінням великою кількістю вузлів. Існуючі протоколи IP-адресації не завжди ефективні для динамічних і великих мереж. Використання ієрархічних схем адресації та нових протоколів, таких як IPv6, може допомогти вирішити ці проблеми.

Взаємодія із мережами загального користування і Інтернет є необхідною для інтеграції БІМС з глобальними інформаційними системами. Це вимагає розробки механізмів для безшовного переходу між різними типами мереж та забезпечення сумісності протоколів. Використання шлюзів та проксі-серверів може допомогти у вирішенні цих завдань.

Забезпечення безпеки в умовах широкомовної природи радіоканалу є однією з найбільших проблем БІМС. Широкомовна передача даних робить мережі вразливими до атак, таких як перехоплення даних, атаки типу "людина посередині" та DoS (Denial of Service). Для забезпечення безпеки використовуються методи шифрування, автентифікації та управління доступом. Протоколи, такі як WPA3 (Wi-Fi Protected Access 3) та IPSec (Internet Protocol Security), забезпечують високий рівень захисту даних у бездротових мережах.

Висновки

1. Проведено огляд літератури та аналіз сучасних визначень БІМС. Було підкреслено важливість цих мереж у сучасному світі, зокрема їхню роль у

забезпеченні гнучких, надійних і мобільних рішень для різних галузей, включаючи військові комунікації, системи екстреного реагування, розумні міста та Інтернет речей (IoT).

2. Досліджено історичні аспекти розвитку SON, починаючи з перших ad hoc мереж та їх еволюції в напрямку MANET, VANET та FANET. Було детально розглянуто ключові етапи та проекти, що сприяли розвитку цих технологій, включаючи ALOHA, PRNET, комплекси "Базальт" і "Редут", а також сучасні програми DARPA.
3. Проведено класифікацію різних типів БІМС, включаючи Ad Hoc мережі, MANET, VANET, FANET, Mesh мережі, WSN, UW-ASN та Hybrid мережі. Для кожного типу мережі були проаналізовані їхні особливості, переваги, недоліки та сфери застосування.
4. Проаналізовано ключові особливості БІМС, такі як змінювана кількість вузлів, мобільність та стаціонарність, випадковість та динамічність топології, децентралізоване управління, багатоканальність, масштабованість та обмеженість ресурсів.
5. Ідентифіковано та детально розглянуто основні проблеми, з якими стикаються БІМС, включаючи організацію надійного транспорту даних, підвищення швидкості передачі інформації, ефективне управління на різних рівнях моделі OSI, використання обмежених ресурсів вузлів, забезпечення QoS, масштабування та адресацію в мережах великої розмірності, взаємодію з мережами загального користування та Інтернетом, а також забезпечення безпеки в умовах широкомовної природи радіоканалу.

РОЗДІЛ 2

ПРИНЦИПИ ПОБУДУВИ І ФУНКЦІОНУВАННЯ БЕЗПРОВОДОВИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ

2.1 Архітектурні принципи БІМС

Основні компоненти архітектури БІМС включають вузли, які можуть бути стаціонарними або мобільними. Вузли виконують функції хостів (джерел і приймачів інформації), маршрутизаторів, або обох одночасно. Кожен вузол обладнаний необхідними апаратними та програмними засобами для виконання цих функцій. Вузли комунікують через бездротові канали, використовуючи радіочастоти, інфрачервоне світло або інші технології передачі даних.

Важливими компонентами є також алгоритми маршрутизації та управління ресурсами, які дозволяють ефективно передавати дані і забезпечувати надійну роботу мережі. Наприклад, енергоспоживання є критичним фактором для мобільних вузлів, тому часто використовуються енергоефективні протоколи.

Архітектури рівнів моделі OSI у БІМС БІМС можуть бути організовані за моделлю OSI, яка включає сім рівнів: фізичний, канальний, мережевий, транспортний, сеансовий, представницький та прикладний. На фізичному рівні визначаються технології передачі даних, такі як радіочастоти або оптичне випромінювання. Канальний рівень відповідає за доступ до середовища передачі та контроль помилок. Мережевий рівень забезпечує маршрутизацію даних між вузлами. Транспортний рівень відповідає за надійність передачі даних, включаючи контроль потоку і корекцію помилок. Сеансовий, представницький та прикладний рівні відповідають за управління сеансами зв'язку, форматування даних та виконання прикладних програм відповідно.

Архітектура стільникових мереж базується на фіксованій стільниковій структурі з фіксованими зонами обслуговування та стаціонарними базовими станціями. Це дозволяє забезпечити високу якість обслуговування і стабільність зв'язку, проте потребує значного часу та ресурсів для розгортання мережі. Управління в таких мережах централізоване, з окремою виділеною

мережею управління, що забезпечує ефективну координацію і контроль, але знижує гнучкість та адаптивність до змін.

Транкінгові мережі, навпаки, не мають фіксованої інфраструктури, кожен вузол в них виконує функцію ретранслятора (маршрутизатора) повідомлень. Це дозволяє швидко розгортати мережі і легко їх масштабувати, оскільки немає необхідності у складному плануванні мережі. Управління в таких мережах децентралізоване, що підвищує живучість і стійкість мережі до збоїв окремих вузлів, а також забезпечує високу мобільність всіх елементів мережі.

Мобільні радіомережі використовують стаціонарну мережу загального користування та фіксовану мережу для з'єднання базових станцій. Це дозволяє забезпечити високу швидкість передачі даних до Гб/с, проте такі мережі мають обмежену живучість і низьку розвідзахищеність. Вони зазвичай використовуються для тилових підрозділів та антитерористичних операцій, де важлива швидкість розгортання і мобільність абонентів в межах зон покриття стаціонарними базовими станціями.

Змінювана кількість вузлів і площа покриття мережею є характерною особливістю БІМС, що дозволяє адаптуватися до різних умов експлуатації та потреб користувачів. Мобільність вузлів забезпечує гнучкість і можливість створення мережі в будь-якому місці та в будь-який час. Випадковість топології мережі, її неоднорідність і динамічність зміни потребують використання адаптивних алгоритмів маршрутизації і управління ресурсами для забезпечення надійної передачі даних.

Принцип передачі інформації в БІМС базується на комутації пакетів із багато стрибковою маршрутизацією, що дозволяє ефективно використовувати доступні ресурси мережі і забезпечити високу швидкість передачі даних. Децентралізоване управління дозволяє підвищити стійкість мережі до збоїв і забезпечити високу живучість системи.

Багатоканальність мереж дозволяє підвищити пропускну здатність і забезпечити якість обслуговування для різних типів трафіку. Масштабованість мереж дозволяє легко нарощувати кількість вузлів і площу покриття, що є

важливим для використання в різних сферах, таких як поле бою, надзвичайні ситуації, розумні міста та інші [8].

Обмеженість ресурсів вузлів мережі, таких як об'єм пам'яті, CPU, ємність акумулятора та інші, потребує використання ефективних методів управління ресурсами для забезпечення надійної роботи мережі. Обмежена безпека мережі в умовах широкомовної природи радіоканалу вимагає використання передових методів шифрування та захисту даних для забезпечення конфіденційності та цілісності інформації.

2.2 Протоколи маршрутизації у БІМС

Протоколи маршрутизації у безпроводових інфокомунікаційних мережах із самоорганізацією (БІМС) є критичним компонентом, що забезпечує ефективну передачу даних в умовах динамічної топології та обмежених ресурсів. Ці протоколи визначають, як пакети даних переміщуються через мережу, забезпечуючи їх доставку від джерела до призначення.

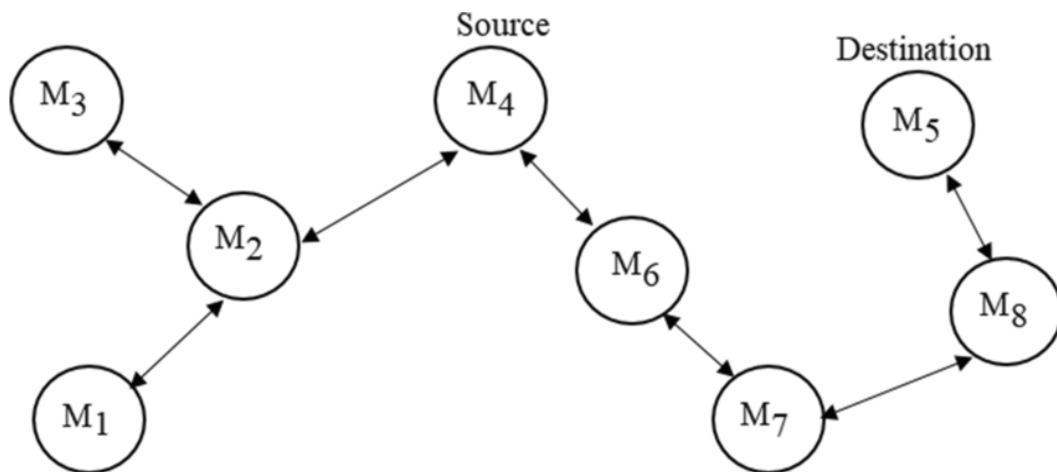


Рис.2.1 Діаграма DSDV протоколу маршрутизації

Протокол Destination-Sequenced Distance-Vector (DSDV) є одним із проактивних протоколів маршрутизації, який широко використовується в динамічних мережах Ad-hoc. У таких мережах кожен мобільний вузол підтримує свою власну таблицю маршрутизації, яка містить всю необхідну інформацію для передачі пакетів до інших вузлів. Основна мета DSDV –

забезпечити стабільність і достовірність маршрутів, використовуючи періодичні оновлення маршрутних таблиць.

Таблиця маршрутизації в DSDV включає наступні поля для кожного доступного пункту призначення:

Пункт призначення (Dest): Ідентифікатор вузла, до якого призначено пакет.

Наступний стрибок (Next Hop): Ідентифікатор сусіднього вузла, який є наступним пунктом на шляху до пункту призначення.

Метрика (Metric): Кількість переходів (hop count) від поточного вузла до пункту призначення.

Номер послідовності (Seq.No.): Унікальний номер, що використовується для відстеження найновішої маршрутної інформації.

Час встановлення (Install): Час, коли запис для цього пункту призначення був вперше додано до таблиці маршрутизації або оновлено.

Кожен вузол періодично або після виявлення змін у топології мережі розсилає пакет оновлення таблиці маршрутизації своїм сусідам. Цей пакет містить інформацію про всі відомі маршрути, включаючи метрику та номер послідовності для кожного пункту призначення. Такі оновлення допомагають іншим вузлам оновлювати свої таблиці маршрутизації, щоб відображати найновіші зміни в топології мережі.

Коли сусідній вузол отримує пакет оновлення, він перевіряє номери послідовності для кожного пункту призначення. Якщо номер послідовності в отриманому пакеті більший, ніж наявний у власній таблиці маршрутизації, це означає, що інформація є більш актуальною. У такому випадку вузол оновлює свою таблицю маршрутизації новими даними, включаючи наступний стрибок та метрику.

У випадку отримання декількох пакетів оновлення для одного пункту призначення з однаковими номерами послідовності, вузол обирає маршрут із найменшою метрикою. Це гарантує, що пакети надсилаються найефективнішим шляхом до пункту призначення.

Номери послідовності відіграють ключову роль у запобіганні розповсюдженню застарілої інформації. Кожен раз, коли вузол оновлює свою таблицю маршрутизації, він збільшує номер послідовності для відповідного пункту призначення. Таким чином, інші вузли можуть легко визначити, чи є отримана інформація про маршрут більш актуальною, ніж та, що вже зберігається в їхніх таблицях маршрутизації.

Вузли також стежать за часом встановлення записів у таблиці маршрутизації. Якщо запис не оновлювався протягом певного періоду, він вважається застарілим і видаляється з таблиці. Це допомагає запобігти тому, щоб вузли використовували недійсні маршрути для надсилання пакетів.

DSDV використовує методику, засновану на класичному протоколі Bellman-Ford, але з додаванням номерів послідовності для запобігання проблемам, таким як маршрутизаційні петлі та інші аномалії, пов'язані з оновленням маршрутів. Ця техніка дозволяє вузлам визначати свіжість інформації про маршрути та забезпечує стабільність у мережі.

Математично, процес оновлення маршрутизації можна описати через періодичне розповсюдження пакетів оновлення з інформацією про маршрути до всіх відомих вузлів. Оновлення, що мають більший номер послідовності, ніж поточні записи, автоматично вважаються більш актуальними:

$$S_i^{new} * S_i^{old} = UpdateRoutingTable$$

Рис.2.2 Формула процесу оновлення маршрутизації

де S_i^{new} і S_i^{old} – це новий і старий номери послідовності для вузла i .

Кількість переходів (метрика) у таблицях маршрутизації дозволяє визначити найкоротші маршрути до пунктів призначення, що мінімізує затримку передачі даних. Алгоритм оновлення таблиць також враховує оптимізацію енергоспоживання, оскільки періодичні оновлення таблиць є енергоефективнішими порівняно з частими запитами маршрутизації в реактивних протоколах.

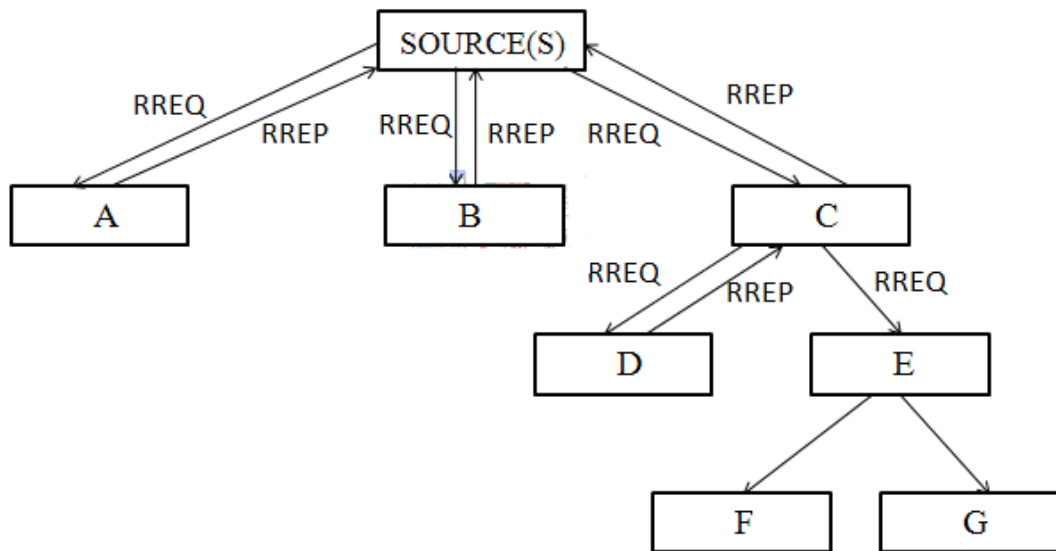


Рис.2.3 Діаграма AODV протоколу маршрутизації

Реактивні протоколи маршрутизації, такі як AODV, відіграють ключову роль в БІМС, особливо в умовах динамічних топологій. AODV є реактивним протоколом, що означає, що маршрути створюються лише за необхідності, коли вузлу потрібно передати дані.

AODV використовує кілька типів повідомлень для підтримки маршрутизації: Route Request (RREQ), Route Reply (RREP), Route Error (RERR) та Hello. Повідомлення вітання (Hello) можуть використовуватися для виявлення та моніторингу зв'язків із сусідами. Вузли, які періодично надсилають ці повідомлення, допомагають забезпечити актуальність інформації про доступність сусідніх вузлів. Якщо вузол не отримує кілька повідомлень Hello від свого сусіда, це сигналізує про можливий розрив зв'язку [9].

Процес маршрутизації починається, коли джерело має дані для передачі до невідомого пункту призначення. Джерело транслює запит маршруту (RREQ), який поширюється через мережу. Кожен вузол, отримуючи RREQ, створює маршрут до джерела. Якщо вузол не є призначенням і не має актуального маршруту до нього, він ретранслює RREQ далі. Коли RREQ досягає вузла призначення або вузла з актуальним маршрутом до призначення, генерується відповідь маршруту (RREP). RREP направляється назад до джерела по зворотньому маршруту, створюючи маршрут до призначення на кожному проміжному вузлі.

При отриманні кількох RREP, джерело обирає маршрут з найменшою кількістю переходів (hops). Під час передачі даних кожен вузол на маршруті оновлює свої таймери, пов'язані з маршрутом до джерела та призначення, що допомагає підтримувати актуальність маршруту в таблиці маршрутизації. Якщо маршрут не використовується протягом певного часу, вузол видаляє його зі своєї таблиці.

У разі розриву зв'язку під час передачі даних, генерується повідомлення про помилку маршруту (RERR), яке направляється назад до джерела. Кожен проміжний вузол, що отримує RERR, видаляє маршрути до недоступних пунктів призначення. Джерело, отримавши RERR, скасовує маршрут і за необхідності повторно ініціює пошук маршруту.

Технічно, AODV забезпечує ефективне використання мережевих ресурсів за рахунок мінімізації накладних витрат на підтримку таблиць маршрутизації та сигналізацію. Однак, у динамічних середовищах можуть виникати затримки під час встановлення маршруту, оскільки RREQ має поширюватися через мережу до призначення. Крім того, широкомовлення RREQ може створювати додаткове навантаження на мережу в умовах високої мобільності.

Для математичного моделювання ефективності AODV можна використовувати формули, що враховують кількість переходів, час поширення сигналів та ймовірність розриву зв'язку. Наприклад, середній час затримки D можна виразити як функцію від середнього часу на кожен перехід t та кількості переходів n :

$$D = n * t$$

Рис.2.4 Формула моделювання ефективності AODV

Багато стрибкова маршрутизація є важливою характеристикою БІМС, що дозволяє пакетам даних переміщуватися через декілька проміжних вузлів на шляху до призначення. Це забезпечує гнучкість та надійність мережі, оскільки дозволяє обходити пошкоджені або перевантажені вузли. Одним з відомих алгоритмів багато стрибкової маршрутизації є алгоритм вектору відстаней, де

кожен вузол підтримує таблицю з відстанями до інших вузлів мережі та використовує її для визначення найкоротшого шляху.

Мережі з високою мобільністю, такі як MANET потребують спеціалізованих протоколів маршрутизації, здатних швидко адаптуватися до змін топології. Одним з таких протоколів є Temporally-Ordered Routing Algorithm (TORA), який забезпечує ефективне маршрутизування в умовах частих змін топології. TORA використовує принцип розподіленої обробки для створення маршруту та підтримки його актуальності, зменшуючи тим самим накладні витрати на сигналізацію.

В умовах обмежених ресурсів, таких як обмежена ємність акумуляторів, оптимізація енергоспоживання є критично важливою для забезпечення тривалої роботи вузлів БІМС. Протоколи маршрутизації можуть бути оптимізовані для мінімізації енергоспоживання за рахунок вибору енергоефективних маршрутів, зниження частоти обміну керуючими пакетами та використання методів агрегації даних. Одним з підходів до оптимізації енергоспоживання є використання енергоефективних алгоритмів, таких як Minimum Energy Routing (MER), який вибирає маршрути з мінімальним споживанням енергії.

2.3 Управління ресурсами в MANET мережі

Управління ресурсами у безпроводних інфокомунікаційних мережах з самоорганізацією є критичним аспектом для забезпечення ефективного функціонування таких мереж, особливо в умовах динамічної топології та обмежених ресурсів.

Одним з ключових компонентів управління ресурсами у мобільних ад-хок мережах (MANET) є мережевий менеджер ресурсів (Network Resource Manager, RM). Забезпечення затримки та пропускну здатності в MANET ускладнено нестабільністю мережі, яка виникає через мобільність вузлів, зміни якості зв'язку та обмеженість ресурсів.

Розглянемо модель розподілу ресурсів, запропоновану системою DYNAMIQUE, яка підтримує періодичні розподілені додатки з топологією

"конвеєра", що складається з ланцюжка комунікаційних завдань. Ця модель застосовується також до розподілених додатків з довільними графовими топологіями.

Розподіл ресурсів для однієї розподіленої програми формулюється як задача оптимізації. Ціль полягає у максимізації якості обслуговування (Quality of Service, QoS) нової програми. Рішення визначає, на якому вузлі буде виконуватися кожне завдання (mapping задач) та скільки ресурсів виділяється. Розглянемо два класи ресурсів: ресурси вузла (навантаження CPU, пам'ять, енергія) та мережеві ресурси (пропускна здатність мережі) [10].

Для вузлових ресурсів використовується модель "обмежених відер" (limited buckets) з умовою допуску:

$$\sum r_i \leq r_{max}$$

Рис.2.5 Умова допуску моделі limited buckets

де r_i — кількість ресурсів, виділених на завдання i , а r_{max} — максимальна доступна кількість ресурсів. Мережеві ресурси також моделюються як обмежені відра, асоційовані з парою вузлів (наприклад, пропускна здатність). Мережеві з'єднання є двонаправленими, і з'єднання в обох напрямках використовують ті ж самі мережеві ресурси.

Розглянемо розподілене середовище з n обчислювальними вузлами, m типами ресурсів вузла та одним мережевим ресурсом. Розподілена програма складається з s комунікаційних завдань $T = \{T_1, T_2, \dots, T_s\}$. Ресурси вузлів задаються вектором:

$$R_i = \{r_{i1}, r_{i2}, \dots, r_{ij}\},$$

Рис.2.6 Формула для обчислення ресурсу вузлів

де r_{ij} — доступна кількість ресурсу типу i на вузлі j . Всі вузли в мережі мають однакову архітектуру управління ресурсами, яка складається з менеджера сервісів додатків, менеджерів ресурсів та клієнтів.

Менеджери ресурсів керують основними ресурсами, такими як навантаження CPU, пам'ять або енергія. Мережевий менеджер ресурсів контролює мережеві ресурси, такі як пропускна здатність та затримка. Всі менеджери ресурсів надають інтерфейс для допуску, адаптації та зворотного зв'язку, що дозволяє легко підключати менеджери ресурсів з різними політиками.

Ресурсний менеджер CPU керує локальним ресурсом CPU. На основі поточного розподілу ресурсів CPU він будує розклад процесів та контролює використання CPU додатками. CPU RM є проміжним програмним шаром, який накладається на локальний планувальник ОС або реалізує політику реального часу, таку як RMA (Rate-Monotonic Analysis)

2.4 Інтерфейси та стандарти

Інтерфейси та стандарти у бездротових інфокомунікаційних мережах самоорганізації (БІМС) є критичним елементом для забезпечення ефективного функціонування таких мереж, особливо у контексті їхньої інтеграції у сучасні телекомунікаційні системи. Одним з основних напрямків розвитку безпроводних технологій є введення мереж MANET як складової мереж зв'язку четвертого покоління, що включає стільникові та мобільні (гібридні) мережі.

Стандарти IEEE для бездротових мереж є основою для побудови сучасних безпроводних локальних та міських мереж цивільного призначення. Найбільш відомі з них включають протоколи IEEE 802.11 та Bluetooth. Таблиця 3 надає детальний огляд основних характеристик існуючих протоколів канального рівня бездротових мереж. Зокрема, протоколи IEEE 802.11 та IEEE 802.16 мають значні переваги завдяки високій пропускній здатності, широкому діапазону частот та підтримці різних типів управління мережею.

Таблиця 2.1

Основні характеристики	Протокол канального рівня			
	IEEE 802.11	IEEE 802.16	HiperLAN 2	Bluetooth
Частота (ГГц)	2.4 / 5.1	2 – 66	5.1	2.4

Відстань (м)	До 500 / до 100	100 – 20000	До 250	10...100
Швидкість передачі в каналі Мб/с	1 / 2 / 11 / 54	120	54	0.7...1
Метод доступу до каналу	DFWMAC (CSMA/CA)	OFDMA/TDMA / TDD		Polling / TDD
Тип управління, Організація мережі	Децентралізоване, Всі вузли одного рівня	Зонове (кластеризація мережі), централізоване управління ресурсами в кожній зоні (пікомережі)		
Мобільність вузлів	Легко реалізується на мережевому рівні	Ускладнена, викликає необхідність перебудови зон мережі		
Пропускна спроможність мережі	Обмежена взаємними завданнями	Визначається конфігурацією мережі, час реконфігурації мережі – значний		

IEEE 802.11, відомий як Wi-Fi, працює на частотах 2.4 ГГц та 5.1 ГГц, забезпечуючи швидкість передачі даних від 1 до 54 Мбіт/с. Використовуючи метод доступу до каналу DFW-MAC (CSMA/CA), Wi-Fi забезпечує децентралізоване управління, де всі вузли мережі мають однаковий рівень. Це дозволяє легко реалізовувати мобільність вузлів на мережевому рівні, обмежуючи пропускну здатність взаємними завданнями.

Протокол IEEE 802.16, відомий як WiMAX, працює на частотах від 2 до 66 ГГц та підтримує відстань до 20 км. Зі швидкістю передачі даних до 70 Мбіт/с та методом доступу до каналу OFDMA/TDMA/TDD, WiMAX забезпечує зональне (кластеризоване) управління мережею, де централізоване управління ресурсами здійснюється в кожній зоні. Однак, мобільність вузлів у WiMAX ускладнена, що викликає необхідність перебудови зон мережі [11].

HiperLAN 2 працює на частоті 5 ГГц і забезпечує швидкість передачі даних до 54 Мбіт/с. Цей протокол також використовує метод доступу до каналу OFDMA/TDMA/TDD і відомий своїм зональним управлінням. Bluetooth, з іншого боку, працює на частоті 2.4 ГГц з відстанню до 100 м та швидкістю передачі даних від 0.7 до 1 Мбіт/с, використовуючи методи Polling/TDD для доступу до каналу. Bluetooth забезпечує низьковитратну та енергоефективну передачу даних з невеликою пропускну здатністю мережі, яка визначається конфігурацією мережі.

Основна мета взаємодії між стандартами – забезпечення безшовного з'єднання та передачі даних між пристроями, що підтримують різні протоколи, такі як IEEE 802.11, IEEE 802.16, Bluetooth та HiperLAN 2.

Для досягнення цієї мети можуть використовуватися декілька ключових підходів, таких як: відкриті інтерфейси, що дозволяють різним системам та пристроям взаємодіяти між собою, використовуючи загальні стандарти. Це забезпечує можливість інтеграції різних мережевих технологій в єдину інфраструктуру. А також міжнародні організації, такі як IEEE, ITU та ETSI, що розробляють стандарти, котрі визначають протоколи взаємодії між різними мережевими технологіями, що дозволяє уникати несумісностей та забезпечувати безшовну комунікацію. Сучасні пристрої підтримують кілька стандартів одночасно. Наприклад, багато смартфонів оснащені модулями Wi-Fi (IEEE 802.11), Bluetooth та LTE (4G), що дозволяє їм автоматично переключатися між різними мережами залежно від доступності та вимог до пропускної здатності. Ці пристрої використовують алгоритми адаптивного вибору мережі, що дозволяє динамічно обирати оптимальну мережу для передачі даних, враховуючи такі параметри, як швидкість передачі, затримка, енергоспоживання та надійність з'єднання.

Проміжне програмне забезпечення (middleware) та мережеві шлюзи забезпечують взаємодію між пристроями, що працюють на різних стандартах. Вони здійснюють перетворення протоколів, управління з'єднаннями та маршрутизацію даних між різними мережами.

Наприклад, мережеві шлюзи можуть об'єднувати мережі Wi-Fi та LTE, забезпечуючи безперервний доступ до Інтернету для мобільних користувачів, незалежно від їхнього місцезнаходження та поточного стандарту з'єднання. Розвиток безпроводних мереж четвертого покоління (4G) та п'ятого покоління (5G) передбачає інтеграцію існуючих технологій, таких як Wi-Fi, WiMAX та Bluetooth, з новими стандартами мобільного зв'язку. Це дозволяє забезпечити високу пропускну здатність, низькі затримки та глобальний роумінг для користувачів.

Одним з ключових аспектів інтеграції є використання IPv6, який забезпечує уніфікований адресний простір та підтримку величезної кількості підключених пристроїв, що є критичним для Інтернету речей (IoT).

Для оптимізації протоколів використовують:

- a) Використання алгоритмів, що динамічно розподіляють мережеві ресурси залежно від поточних умов, таких як навантаження на мережу, кількість активних користувачів та тип трафіку. Наприклад, у Wi-Fi використовується алгоритм динамічного розподілу частотних каналів для уникнення інтерференції.
- b) Впровадження механізмів QoS, що дозволяють пріоритезувати трафік та забезпечувати високу якість обслуговування для критичних додатків, таких як VoIP, відеоконференції та стрімінг мультимедіа. У WiMAX використовуються класи обслуговування, які забезпечують різні рівні пріоритету для різних типів трафіку.
- c) Оптимізація протоколів для зниження енергоспоживання, особливо для мобільних та IoT пристроїв. У Bluetooth використовується механізм низької потужності (Low Energy), який значно знижує споживання енергії під час передачі даних.

Одним із механізмів перетворення протоколів є використання шлюзів та ретрансляторів для перетворення протоколів між різними мережами. Це дозволяє забезпечити безперервне з'єднання та передачу даних між пристроями, що використовують різні стандарти.

Також варто зазначити проміжне програмне забезпечення (middleware), яке використовується для абстрагування специфічних деталей протоколів та забезпечення уніфікованого інтерфейсу для додатків. Це дозволяє розробникам створювати додатки, що можуть працювати з різними мережевими технологіями без необхідності враховувати специфіку кожного протоколу.

Висновки

1. Основні компоненти архітектури БІМС включають вузли, які можуть бути стаціонарними або мобільними. Вузли виконують функції хостів (джерел і приймачів інформації), маршрутизаторів або обох одночасно. Кожен вузол оснащений необхідними апаратними та програмними засобами для виконання цих функцій. Вузли комунікують через бездротові канали, використовуючи радіочастоти, інфрачервоне світло або інші технології передачі даних. Важливими компонентами є також

алгоритми маршрутизації та управління ресурсами, які дозволяють ефективно передавати дані і забезпечувати надійну роботу мережі.

2. У цьому розділі ми розглянули протоколи маршрутизації що ключовими для ефективного функціонування безпроводових мереж із самоорганізацією. Основні протоколи, такі як AODV, DSR та OLSR, забезпечують динамічний вибір маршрутів для передачі даних. Ці протоколи оптимізують мережевий трафік, зменшуючи затримки та підвищуючи надійність зв'язку, що є критичним для військових застосувань.
3. Ефективне управління ресурсами є важливим аспектом для підтримки стабільності та продуктивності MANET мереж. Використання методів динамічного розподілу частотного спектра, енергозберігаючих алгоритмів та адаптивних протоколів дозволяє оптимізувати використання доступних ресурсів. Військові застосування вимагають високої надійності та безперервного зв'язку, що досягається за рахунок удосконалених алгоритмів управління ресурсами.
4. У цьому підрозділі розглянуто інтерфейси та стандарти, які визначають взаємодію між різними компонентами безпроводових мереж. Важливими стандартами є IEEE 802.11 для Wi-Fi мереж, IEEE 802.15 для персональних мереж (Bluetooth) та IEEE 802.16 для мереж широкосмугового доступу (WiMAX). Ці стандарти забезпечують сумісність та інтероперабельність різних пристроїв та систем, що є критичним для інтеграції мобільних сенсорів та дронів у єдине інформаційне середовище.

РОЗДІЛ 3

СУЧАСНІ ПРИКЛАДИ ВИКОРИСТАННЯ БЕЗПРОВОДОВИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ

3.1 Архітектура C4ISR

Архітектура C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) представляє комплексну інтеграцію засобів оперативно-стратегічної розвідки, спостереження та військової розвідки із системами управління, контролю, зв'язку та обчислювальними засобами в єдиному інформаційному середовищі. Це середовище забезпечує інтеграцію навігаційної, загальногеографічної та тактичної інформації в єдиній географічній системі координат. Такі інтеграційні процеси дозволяють реалізувати мережецентричну архітектуру управління військами, яка змінює підходи до ведення бойових дій, використовуючи принципи мережецентричності.

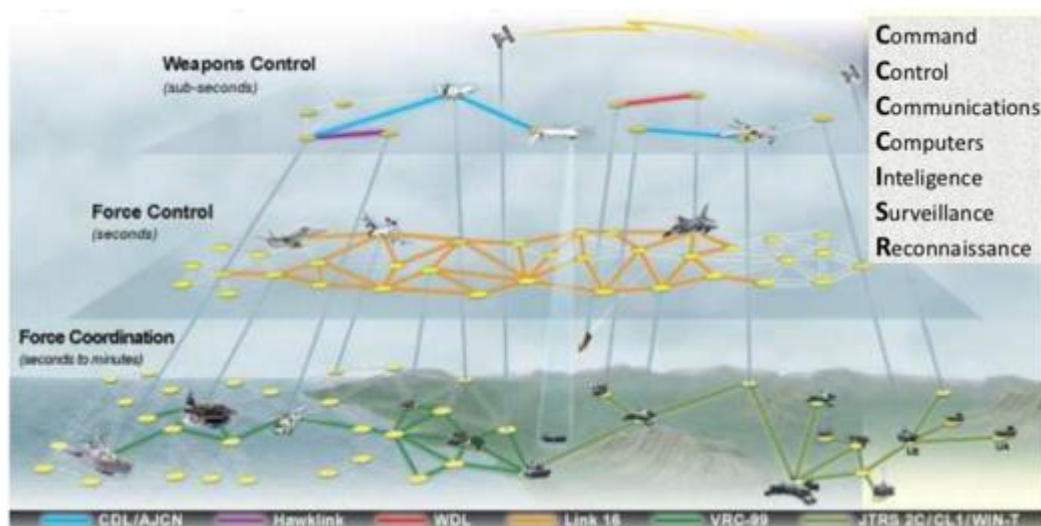


Рис.3.1 Приклад C4ISR архітектури

C4ISR також можна розглядати як єдиний масштабний програмно-технічний комплекс. У назві C4ISR (командування, контроль, зв'язок, комп'ютери, розвідка, спостереження, рекогносцировка) перераховані функції,

які мають бути автоматизовані. Тому системи, побудовані за подібною концепцією, називаються інтегрованими системами розвідки та управління.

Відмінність C4ISR від C2+ або C2SR (Command, Control, Surveillance, Reconnaissance) полягає у тому, що в концепціях тактичного рівня самостійною одиницею є окремий солдат або військова техніка. У C4ISR ці одиниці стають членами тактичної мережі або бойового інтернету [12]. Архітектури та концепції C4ISR і C2+ передбачають створення інформаційного середовища, яке дозволяє:

- a) автоматично визначати положення і переміщення своїх підрозділів (відображається на електронних картах);
- b) автоматично визначати положення противника і його переміщення (також відображається на електронних картах);
- c) автоматично обирати маршрути руху;
- d) автоматично давати цілевказівки засобам вогневого ураження;
- e) автоматично інформувати свої підрозділи про дії і місцезнаходження сусідів та противника.

Ці можливості доступні на оперативному і тактичному рівнях. Для C4ISR на оперативному рівні додаються такі функції як: повна автоматизація збору інформації та її обробка, автоматизоване надання варіантів рішень командира, заснованих на автоматично отриманих розвідданих і інформації про наявні сили і засоби, моделювання бою і його можливих результатів, пропозиції часткових рішень для командира під час бою, засновані на поточній ситуації.

Різниця між тактичним і оперативним рівнями систем полягає в можливості автоматизації прийняття рішень, моделюванні бою і прогнозуванні результатів. Крім того, C4ISR включає розширену автоматизацію для логістики, що дозволяє постійно вести облік витрат необхідних засобів. Дані про потреби підрозділів у поповненні боєкомплекту, логістичному забезпеченні, необхідних запчастин та іншому обробляються безперервно, що забезпечує своєчасне постачання всього необхідного для успішного ведення бойових дій.

Прикладом реалізації C4ISR на тактичному рівні є програмне забезпечення DAP (Digital Army Program), розроблене американськими

компаніями Northrop Grumman та Lockheed Martin. Метою DAP є створення єдиного інформаційного поля, що забезпечує ситуаційну обізнаність, автоматизацію управління, вдосконалення оперативних можливостей і найбільш ефективного використання сил, засобів і ресурсів.

Програмне забезпечення DAP включає комплекс інтегрованих модулів, які забезпечують різні аспекти управління та координації військових операцій. Основні модулі DAP охоплюють такі функціональні області, як управління бойовими діями, логістика, розвідка та зв'язок.

Один з ключових компонентів DAP - це система управління бойовими діями, яка забезпечує автоматизоване планування та виконання бойових операцій. Ця система дозволяє командирам в реальному часі отримувати інформацію про стан військ, розташування противника та хід бойових дій, що значно підвищує ефективність прийняття рішень. Інформація збирається з різних джерел, включаючи мобільні сенсори, дрони, супутники та наземні станції спостереження, і обробляється за допомогою потужних алгоритмів обробки даних.

Система логістики в рамках DAP автоматизує процеси постачання, транспортування та управління ресурсами. Це включає відстеження запасів, планування маршрутів постачання та моніторинг стану техніки. За рахунок інтеграції з іншими модулями, система логістики забезпечує своєчасне та ефективне постачання необхідних ресурсів на поле бою, мінімізуючи затримки та підвищуючи оперативну готовність військ.

Розвідувальний модуль DAP забезпечує збирання, обробку та аналіз розвідувальної інформації. Це включає використання методів аналізу великих даних для виявлення потенційних загроз та прогнозування дій противника. Розвідувальна інформація передається командирам в реальному часі, що дозволяє швидко реагувати на зміни в оперативній обстановці та приймати обґрунтовані рішення.

Зв'язок є критичним компонентом DAP, що забезпечує надійну та захищену передачу даних між різними підрозділами та командними пунктами. Система зв'язку використовує сучасні технології, такі як захищені радіоканали,

супутниковий зв'язок та мобільні мережі, для забезпечення безперервної комунікації навіть у складних умовах бойових дій.

DAR також включає модулі для моделювання та тренувань, які дозволяють проводити симуляції бойових дій та тренування персоналу. Це допомагає військовим підрозділам готуватися до різних сценаріїв та вдосконалювати свої навички в умовах, максимально наближених до реальних бойових дій.

У підсумку, DAR представляє собою потужний інструмент для інтеграції різних аспектів військового управління, забезпечуючи єдине інформаційне поле, що підвищує ефективність та оперативність військових операцій. Завдяки використанню передових технологій та інтегрованого підходу, DAR сприяє покращенню ситуаційної обізнаності, автоматизації управління та ефективному використанню ресурсів на тактичному рівні.

3.2 In-door Mesh мережа на прикладі Omada EAP

Mesh мережа, побудована з використанням продуктів Omada EAP, включає наступні компоненти: точки доступу (EAP225, EAP245, EAP225-Outdoor) і керуючий пристрій (OC200). EAP225 виконує роль Root AP (базової точки доступу) і підключається до мережі через PoE комутатор. EAP245 та EAP225-Outdoor виконують роль Mesh AP (точок доступу Mesh) і підключаються до Root AP через бездротове з'єднання в діапазоні 5GHz. OC200 забезпечує централізоване управління всіма точками доступу в мережі і підключається до мережі через PoE адаптер або PoE комутатор.

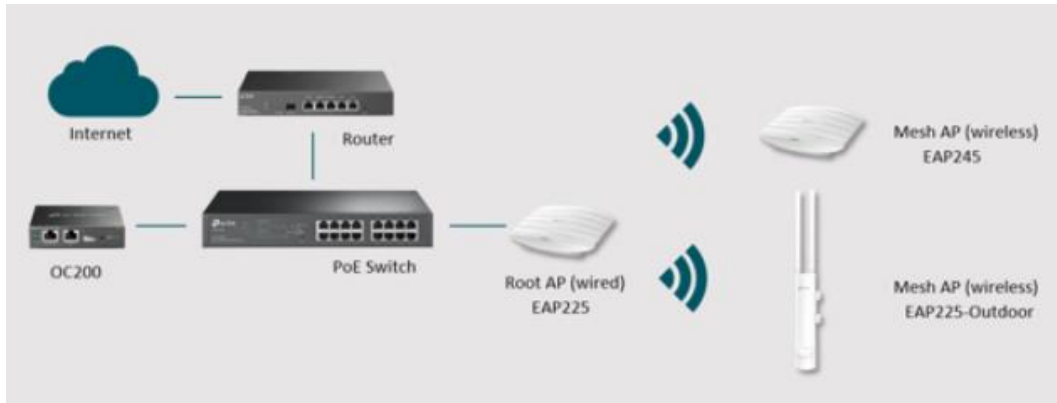


Рис.3.2 Приклад будови Omada EAP мережі

Мережа Omada EAP має низку важливих можливостей. По-перше, використання Mesh технології дозволяє значно розширити зону покриття мережі без необхідності прокладки додаткових кабелів. Це досягається шляхом бездротового з'єднання точок доступу, що особливо корисно на великих відкритих просторах або у важкодоступних місцях. По-друге, точки доступу автоматично вибирають оптимальні маршрути передачі даних, що забезпечує стабільність та надійність з'єднання. Мережа автоматично адаптується до змін у середовищі, таких як поява нових перешкод або зміна розташування точок доступу. По-третє, керуючий пристрій OC200 забезпечує зручне централізоване управління мережею. Користувачі можуть легко додавати нові точки доступу, контролювати стан мережі та виконувати необхідні налаштування з єдиної панелі управління.

Налаштування Mesh мережі Omada EAP включає кілька кроків. Підключення та живлення пристроїв: всі точки доступу (EAP225, EAP245, EAP225-Outdoor) підключаються та увімкнені через PoE адаптер або PoE комутатор. Це забезпечує одночасне живлення та передачу даних через один кабель Ethernet, що спрощує інсталяцію та зменшує кількість необхідних кабелів. Доступ до керуючого пристрою OC200 здійснюється за допомогою IP-адреси OC200. Це дозволяє здійснювати централізоване управління всіма точками доступу в мережі. Увімкнення функції Mesh: на сторінці управління OC200 необхідно перейти до налаштувань сайту та увімкнути функцію Mesh. Ця функція за замовчуванням вже активована, що спрощує процес налаштування. Вона дозволяє точкам доступу бездротово з'єднуватися одна з

одною, створюючи мережу з широким покриттям. Прийняття Root AP: на сторінці пристроїв необхідно знайти EAP225 (Root AP) у списку очікування. Наступним кроком потрібно натиснути кнопку "adopt" для прийняття цієї точки доступу в управління контролером. Це інтегрує точку доступу в централізовану систему управління. Після прийняття EAP225, контролер автоматично виявить інші бездротові точки доступу EAP. Кнопка "adopt" використовується для прийняття EAP245 та EAP225-Outdoor. Важливо перевірити, що канал 5GHz на Root AP працює на Band4, особливо для EAP225-Outdoor (Канада), щоб забезпечити оптимальну роботу мережі. Автоматичне налаштування IP-адрес: через 3-5 хвилин EAP245 та EAP225-Outdoor отримають IP-адреси від DHCP-сервера та автоматично підключаються до контролера Omada, завершуючи процес налаштування Mesh мережі. Це забезпечує безперебійне функціонування мережі та мінімізує необхідність ручного втручання.

Mesh мережі Omada EAP мають низку переваг, які роблять їх ідеальними для широкого спектра застосувань:

- a) Мережі Omada EAP дозволяють легко додавати нові точки доступу без необхідності складних налаштувань або прокладки додаткових кабелів. Це робить їх ідеальними для середовищ, де потрібно швидко розширювати або змінювати конфігурацію мережі.
- b) Автоматичний вибір оптимальних маршрутів передачі даних забезпечує високу надійність з'єднання та стійкість мережі до збоїв.
- c) Використання контролера ОС200 забезпечує централізоване управління всіма точками доступу, що значно спрощує процес моніторингу та налаштування мережі.
- d) Використання PoE технології забезпечує одночасне живлення та передачу даних через один кабель Ethernet, що зменшує витрати на інсталяцію та спрощує обслуговування мережі.

Технічна будова Mesh мережі на базі продуктів Omada EAP показує високу ефективність та зручність використання цієї технології для створення бездротових мереж з широким покриттям. Детально описані кроки конфігурації та технічні аспекти дозволяють створювати надійні та стабільні мережі як для

внутрішнього, так і для зовнішнього застосування. Це робить технологію Mesh від Omada EAP ідеальним вибором для широкого спектра застосувань, від домашніх мереж до великих корпоративних інфраструктур.

3.3 БІМС військового призначення на прикладі радіостанції Nimera

Радіостанції Nimera забезпечують надійний зв'язок за рахунок своїх можливостей функціонування в режимі Mesh. Кожна радіостанція Nimera G1 з актуальною прошивкою підтримує ретрансляцію виклику в мережі і може використовуватися в якості ретранслятора. Всі станції в мережі працюють з ППРЧ (стрибки по частотах) і з шифруванням, аналогічно як у прямому режимі. Оновлення прошивки відбувається за допомогою мобільного додатку через смартфон, який має бути підключеним до мережі інтернет. Система підтримує до 8 ретрансляцій. Радіосигнал на частоті роботи радіостанції чутливий до фізичних перешкод, тому наявність цегляних або бетонних стін, густих насаджень, земляних валів суттєво знижує дальність зв'язку. В реальних умовах дальність зв'язку обмежена лише умовами прямої видимості. Експериментально підтверджено роботу радіостанції в якості ретранслятора на дальності 23 кілометри при підйомі станції-ретранслятора на 400м за допомогою аеростата. Для організації стабільного покриття важливо забезпечити хоча би одну станцію достатньою висотою для покриття потрібної території. Це може бути щогла, високе дерево або дах будівлі. При вазі радіостанції 0.11 кг доцільною є тактика підняття радіостанції на аеростаті, БПЛА або повітряному змії. Час роботи від вбудованого акумулятора становить 3-5 діб в залежності від інтенсивності радіообміну, а від посиленого зовнішнього акумулятора ємністю 10000 мАг - 14-21 діб, вага станції з посиленням акумулятором складає 280г. Посилений акумулятор під'єднується до радіостанції через USB-C коннектор і працює як Powerbank з функцією always on. Функція віддаленого контролю рівню заряду батареї знаходиться в розробці і буде доступна в найближчих оновленнях прошивки, що дозволить віддалено передбачити необхідність заміни або зарядки батареї.

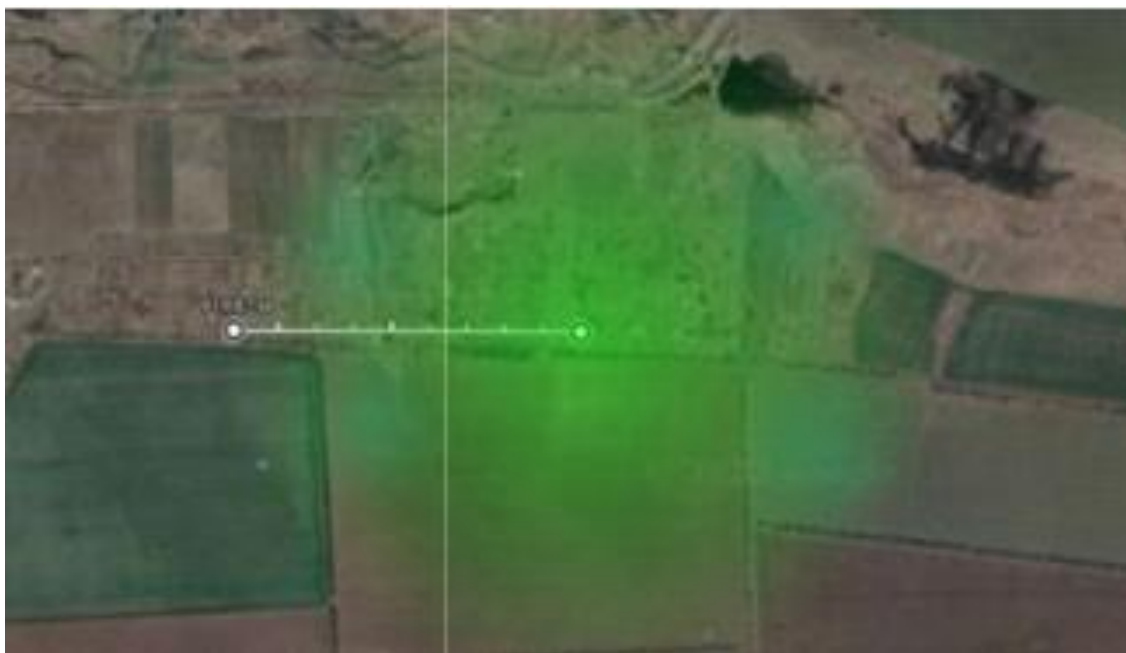


Рис.3.3 Розрахункова зона покриття для опорного пункту взводу

Для створення мережі що буде покривати територію для забезпечення зв'язку опорному пункту взводу необхідна комплектація включає телескопічну щоглу висотою 6-8 метрів, радіостанцію Himera G1 у якості ретранслятора, посилений зовнішній акумулятор на 8000-10000 мАг, пластиковий тримач на щоглу для станції і акумулятора, радіостанції для особового складу. Розрахункова зона покриття в полі складає в радіусі 1 км, в лісі в радіусі 500 м, в густому лісі (стовбури $\varnothing > 0.4\text{м}$) 250 м.



Рис.3.3 Розрахункова зона покриття для опорного пункту роти

Для створення мережі що буде покривати територію для забезпечення зв'язку опорному пункту роти необхідна телескопічна щогла висотою 8 метрів, одна радіостанція у якості ретранслятора, посилений зовнішній акумулятор на 8000-10000 мАг, пластиковий тримач на щоглу для станції і акумулятора та 10 радіостанцій для особового складу. Розрахункова зона покриття для роти складає в полі площу 0,8*1,5км, в лісі площу 400м*800м, в густому лісі 250м*400 м.

Налаштування станцій Himera G1 включає прописування паролю мережі і паролів для груп 1-3 в налаштуваннях персональних рацій. В налаштуваннях станції-ретранслятора прописується пароль мережі і пароль групи 4, ретранслятор працює в беззвучному режимі. Станцію-ретранслятор із зовнішнім акумулятором, бажано закрити в герметичному пакеті, розміщують якомога вище на щоглі для стабільного зв'язку. Термін роботи ретранслятора з акумулятором Li-Pol 10.000 мАг залежно від активності перемовин досягає 21 дня.

Висновки

1. В даному розділі розглянуто сучасні приклади використання безпроводових інфокомунікаційних мереж із самоорганізацією. Зокрема, було проаналізовано архітектуру C4ISR, що є основою для інтеграції різних компонентів у єдину інформаційну систему, що забезпечує командування, контроль, зв'язок, комп'ютерну обробку та розвідку. Ця система дозволяє підвищити ефективність військових операцій завдяки покращенню ситуаційної обізнаності, автоматизації управління, вдосконаленню оперативних можливостей і найбільш ефективному використанню сил, засобів і ресурсів.
2. Розглянуто приклад побудови In-door Mesh мережі на базі Omada EAP. Детально описано процес конфігурації мережі з використанням точок доступу EAP225, EAP245 і EAP225-Outdoor. Було встановлено, що використання Mesh технології значно спрощує розгортання та управління

безпроводовими мережами в умовах обмеженого доступу до кабельної інфраструктури. Mesh мережі забезпечують високу надійність зв'язку та масштабованість, що дозволяє ефективно розширювати мережеве покриття в залежності від потреб користувачів.

3. Також було розглянуто можливості та функціональні особливості тактичних радіостанцій Nimera, що використовуються для побудови безпроводових інфокомунікаційних мереж військового призначення. Завдяки підтримці ретрансляції викликів, шифрування та частотних стрибків, ці радіостанції забезпечують високий рівень захисту та стійкості до перешкод. Було продемонстровано, як з допомогою таких радіостанцій можна створювати стабільні мережі зв'язку в різних умовах, включаючи міські та лісові території.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1. У даній дипломній роботі розглянуто теоретичні основи, принципи побудови та сучасні приклади використання бездротових інфокомунікаційних мереж із самоорганізацією. Робота складається з трьох основних розділів, кожен з яких детально аналізує окремі аспекти теми.
2. У першому розділі надано загальні відомості про бездротові інфокомунікаційні мережі із самоорганізацією, визначено їх важливість у сучасному світі та проаналізовано історію розвитку БІМС. Наведена класифікація БІМС, яка включає Ad Hoc мережі, MANET, VANET, FANET мережі, Mesh мережі, WSN та UW-ASN мережі, а також гібридні мережі. Особлива увага приділена особливостям та проблемам функціонування таких мереж, що дозволяє краще зрозуміти їх складність та важливість у різних галузях застосування.
3. Другий розділ присвячений принципам побудови та функціонування бездротових інфокомунікаційних мереж із самоорганізацією. Розглянуто архітектурні принципи, протоколи маршрутизації, управління ресурсами в MANET мережах, а також інтерфейси та стандарти. Цей розділ надає глибокий технічний аналіз, який допомагає зрозуміти основні технологічні рішення, що забезпечують ефективну роботу SON.
4. Третій розділ містить сучасні приклади використання бездротових інфокомунікаційних мереж із самоорганізацією. На прикладі архітектури C4ISR розглянуто інтеграцію різних компонентів у єдину інформаційну систему, що забезпечує командування, контроль, зв'язок, комп'ютерну обробку та розвідку. Було детально описано побудову In-door Mesh мережі з використанням Omada EAP та можливості і функціональні особливості тактичних радіостанцій Nimera, що використовуються для створення бездротових мереж військового призначення.
5. Загалом, результати дослідження свідчать про високу ефективність та гнучкість бездротових інфокомунікаційних мереж із самоорганізацією. Вони забезпечують надійний зв'язок у різних умовах, сприяють покращенню ситуаційної обізнаності та координації дій, що є критично важливим як у

цивільних, так і у військових застосуваннях. Подальший розвиток та впровадження БІМС сприятиме підвищенню ефективності управління ресурсами та забезпеченню безпеки інформаційних систем у сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Брунер К. Флор Д. Generation of Pathloss and Interference Maps as SON Enabler in Deployed UMTS Networks, 2009 – 2 с.
2. Марчетті Н. Рашмі Прасад Н. Self-Organizing Networks: State-of-the-Art, Challenges and Perspectives, 2010 – 503 с.
3. Насіпурі А. Mobile Ad Hoc Networks, 2003 – 9 с.
4. Йогараван С. Wireless Ad Hoc Network of MANET, VANET, FANET and SANET: A Review, 2021 – 14 с.
5. Ліу Ю. Др. Тонг К. Wireless Mesh Networks in IoT Networks, 2017 – 3 с.
6. Ядав С. Кумар В. Optimal Clustering in Underwater Wireless Sensor Networks Acoustic, EM and FSO Communication Compliant Technique, 2017 – 12764 с.
7. Премнатан К. Challenges in self organizing networks for wireless telecommunications, 2011 – 21 с.
8. Наоки В. Self-Organization Based Network Architecture for New Generation Networks, 2010 – 458 с.
9. Routing protocols in ad hoc networks: A survey [Електронний ресурс]: Боукерч А., 2011, URL: <https://www.sciencedirect.com/science/article/abs/pii/S1389128611001654>
10. Романюк В. Мобільні радіомережі (MANET) - основа побудови тактичних мереж зв'язку, 2007 – 6 с.
11. Боркар П. Comparative Study of IEEE 802.11, 802.15, 802.16, 802.20 Standards for Distributed VANET, 2012 – 114 с.
12. Кірпічніков Ю., Федорієнко В., Головченко О., Андрощук О., Аналіз рамкових архітектур побудови інформаційних систем НАТО та визначення особливостей архітектури C4ISR, 2017 – 79 с.
13. How to Build a Mesh Network via Omada EAP in Controller Mode [Електронний ресурс]: 2024, URL: <https://www.tp-link.com/uk-ua/support/faq/2949/>

