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

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз методів управління доступом до середовища в безпроводових сенсорних мережах»

Виконав:
студент IV курсу, групи ТС-11
Терзі Олександр Олександрович _____

Керівник:
Старший викладач кафедри ТН, Кандидат наук,
Новіков В. І.

_____

Рецензент:
Професор кафедри ТК, д.т.н., професор
Лисенко О.І. _____

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

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Терзі Олександр Олександрович

1. Тема роботи «Аналіз методів управління доступом до середовища в безпроводових сенсорних мережах», керівник роботи Новіков В. І старший викладач, кандидат наук, затверджені наказом по університету від «26» квітня 2025 р. № 1755-С

2. Термін подання студентом роботи 12.06.2025

3. Вихідні дані до роботи: Інформаційні матеріали щодо технологій безпроводових сенсорних мереж. План виконання дипломної роботи

4. Зміст роботи

Загально охарактеризувати безпроводові сенсорні мережі зазначивши обмеження з якими стикаються при їх побудові. Описати методи управління доступом в безпроводових сенсорних мережах, та зробити їх порівняльний аналіз. Змоделювати мережу для демонстрації причин виникнення колізій через проблему прихованого вузла. Запропонувати та впровадити в модель вирішення проблеми прихованого вузла.

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

- Тема, мета, актуальність
- Безпроводові сенсорні мережі (БСМ)
- Методи доступу до середовища
- Проблема прихованої станції
- Моделювання в OMNeT++
- Опис сценаріїв
- Результати моделювання
- Висновки

6. Дата видачі завдання 01.10.2024

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи
1	Основи побудови безпроводових сенсорних мереж − Загальна характеристика безпроводових сенсорних мереж − Історія безпроводових сенсорних мереж − Архітектура сенсорного вузла − Особливості безпроводових сенсорних мереж − Енергетичні та функціональні обмеження БСМ − Енергетичні обмеження − Самоорганізація − Безпроводові мережі − Децентралізоване управління − Обмеження − Безпека − Інші проблеми	02.05.2025
2	Методи управління доступом до середовища в БСМ − Роль і функції MAC-рівня	16.05.2025

	− Класифікація протоколів: − Протоколи на основі конкуренції − Протоколи із механізмом резервації − Протоколи із механізмом планування − Протоколи із управлінням маршрутизацією − Протоколи управління спрямованістю та потужністю антени − Порівняльна характеристика методів	
3	Вирішення проблеми прихованої станції − Суть проблеми прихованої станції − Моделювання проблемної ситуації − Опис топології мережі − Поведінка вузла − Налаштування параметрів та подій − Результати моделювання − Шляхи вирішення	30.05.2025
	Вступ, висновки	01.06.2025
	Чистовий варіант	10.06.2025

Студент Олександр ТЕРЗІ

Керівник роботи Валерій НОВІКОВ

РЕФЕРАТ

Текстова частина дипломної роботи: 69 с., 4 рис., 3 табл. 12 джерел.

Мета роботи – Провести аналіз та порівняльну оцінку основних методів управління доступом до середовища у безпроводових сенсорних мережах. А також дослідити та змоделювати проблему прихованих станцій в безпроводових сенсорних мережах

На даний момент не створено єдиного протоколу який буде універсальним рішенням всіх проблем які виникають при розгортанні безпроводових сенсорних мереж (БСМ). Тому під певні потреби треба обирати рішення, які можуть бути не ефективні за інших умов. В дипломній роботі розглянуто основи побудови БСМ та підходи до управління доступом. Описані вимоги до протоколів управління доступом, типові проблеми та класифікація цих протоколів.

УПРАЛІННЯ ДОСТУПОМ , БЕЗПРОВОДОВІ СЕНСОРНІ МЕРЕЖІ, MAC, БСМ, ПРИХОВАНА СТАНЦІЯ

ABSTRACT

The purpose of the work is to conduct an analysis and comparative assessment of the main methods of controlling access to the environment in wireless sensor networks. As well as to investigate and model the problem of hidden stations in wireless sensor networks

At the moment, no single protocol has been created that would be a universal solution to all problems that arise when deploying wireless sensor networks (WSN). Therefore, for certain needs, it is necessary to choose solutions that may not be effective under other conditions. The thesis considers the basics of building WSNs and approaches to access control. The requirements for access control protocols, typical problems and the classification of these protocols are described.

ACCESS CONTROL, WIRELESS SENSOR NETWORKS, MAC, WSN, HIDDEN STATION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ 9
ВСТУП 12
1 ОСНОВИ ПОБУДОВИ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ 13
1.1 Загальна характеристика безпроводових сенсорних мереж 13
1.2 Історія безпроводових сенсорних мереж 16
1.3 Архітектура сенсорного вузла 19
1.4 Особливості безпроводових сенсорних мереж 23
1.5 Енергетичні та функціональні обмеження БСМ 25
1.5.1 Енергетичні обмеження 25
1.5.2 Самоорганізація 27
1.5.3 Безпроводові мережі 29
1.5.4 Децентралізоване управління 30
1.5.5 Обмеження 31
1.5.6 Безпека 32
1.5.7 Інші проблеми 32
1.6 Висновки з розділу 1 33
2 МЕТОДИ УПРАВЛІННЯ ДОСТУПОМ ДО СЕРЕДОВИЩА В БСМ 34
2.1 Роль і функції MAC-рівня 34
2.2 Класифікація протоколів: 35
2.2.1 Протоколи на основі конкуренції 41
2.2.2 Протоколи із механізмом резервації 43
2.2.3 Протоколи із механізмом планування 45
2.2.4 Протоколи із управлінням маршрутизацією 46
2.2.5 Протоколи управління спрямованістю та потужністю антени 47
2.3 Порівняльна характеристика методів 49
2.4 Висновки з розділу 2 51
3 ВИРІШЕННЯ ПРОБЛЕМИ ПРИХОВАНОЇ СТАНЦІЇ 52
3.1 Суть проблеми прихованої станції 52

3.2 Моделювання проблемної ситуації 53
3.2.1 Опис топології мережі 53
3.2.2 Поведінка вузла 54
3.2.3 Налаштування параметрів та подій 57
3.2.4 Результати моделювання 58
3.3 Шляхи вирішення 58
3.4 Моделювання після впровадження RTS/CTS 61
3.5 Висновки з розділу 3 65
ВИСНОВКИ 66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 67
ДОДАТКИ 69
ДОДАТОК А 69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

БСМ (WSN — Wireless Sensor Network) — безпроводова сенсорна мережа: розподілена мережа автономних сенсорних вузлів, що збирають і передають дані через бездротові канали.

MAC (Medium Access Control) — керування доступом до середовища: підрівень канального рівня моделі OSI, що визначає правила доступу до спільного передавального середовища.

OSI (Open Systems Interconnection) — модель взаємодії відкритих систем: семирівнева еталонна модель мережевих протоколів, що стандартизує обмін даними в комп’ютерних мережах.

FAMA (Floor Acquisition Multiple Access) — множинний доступ із захопленням каналу: протокол, який використовує RTS/CTS для уникнення колізій на початку передачі.

S-FAMA (Slotted FAMA) — слотований FAMA: модифікація FAMA з часовими слотами, що підвищує ефективність у середовищах з високим навантаженням.

RC-SFAMA (Receiver-Controlling Slotted FAMA) — слотований FAMA з контролем приймача: варіант S-FAMA, де приймач контролює доступ, знижуючи ймовірність колізій.

Le-WiMARK — Low-energy WiMedia-based MAC for Reliable Communication: енергоефективний MAC-протокол для мультимедійних сенсорних мереж (неформалізований, зустрічається в окремих дослідженнях).

DBTMA (Dual Busy Tone Multiple Access) — множинний доступ із подвійним тоном зайнятості: використовує два тони (передавальний і приймальний), щоб запобігти колізіям і проблемі прихованого вузла.

RI-BTMA (Receiver-Initiated Busy Tone Multiple Access) — BTMA з ініціацією приймачем: приймач подає тон, щоб сигналізувати готовність до прийому і запобігти колізіям.

MACA-BI (MACA By Invitation) — протокол MACA з ініціативою запрошення: приймач ініціює передачу, надсилаючи запрошення передавачу.

MARCH (MAC with Reservation and Channel Hopping) — MAC-протокол з резервуванням і перестрибуванням каналів: дозволяє уникати інтерференції, змінюючи частоту передачі.

NCAC (Noise-aware Contention-based Access Control) — керування доступом з урахуванням шуму: динамічно змінює доступ залежно від рівня перешкод у середовищі.

D-PRMA (Distributed Packet Reservation Multiple Access) — розподілений PRMA: розширення PRMA, де вузли автономно резервують ресурси передачі.

CATA (Collision Avoidance Time Allocation) — розподіл часу з уникненням колізій: призначає часові вікна вузлам для передачі без колізій.

FPRP (Floor acquisition Prioritization and Reservation Protocol) — протокол захоплення каналу з пріоритетом і резервуванням: вузли резервують канал на основі пріоритетів.

SRMA/PA (Self-organizing Resource Management Algorithm with Priority Assignment) — алгоритм самоконфігурації з призначенням пріоритетів: самостійно керує доступом з урахуванням важливості передачі.

HRMA (Hop Reservation Multiple Access) — множинний доступ із резервуванням переходів: резервує весь маршрут перед передачею даних.

DPS (Dynamic Packet Scheduling) — динамічне планування пакетів: адаптивно керує передачею залежно від навантаження й стану мережі.

DWOP (Distributed Wireless Ordering Protocol) — розподілений протокол впорядкування передач у бездротовій мережі: узгоджує порядок доступу без централізованого керування.

DLPS (Dynamic Listening Power Scheduling) — динамічне планування енергоспоживання при прослуховуванні каналу: знижує енергоспоживання за рахунок адаптивного контролю активності.

H-NAME (Hybrid Noise Adaptive MAC for Energy efficiency) — гібридний MAC-протокол з адаптацією до шуму: поєднує кілька стратегій доступу, знижуючи енергоспоживання.

MPR-Tree (Multi-Parent Routing Tree) — дерево маршрутизації з багатьма батьківськими вузлами: розширює класичне дерево для кращої надійності маршрутизації.

DPCF (Distributed Point Coordination Function) — розподілена функція координування вузлів: децентралізований аналог PCF з поліпшенням координації передач.

PCM (Power Controlled MAC) — MAC з контролем потужності: змінює рівень потужності передачі для зменшення інтерференції.

RBAR (Receiver-Based Auto Rate) — автоматичне визначення швидкості на основі приймача: приймач вибирає швидкість передачі залежно від умов каналу.

ERBAR (Extended RBAR) — розширений варіант RBAR з покращенням механізмів вибору швидкості.

DBTMA/DA (Dual Busy Tone Multiple Access with Directional Antennas) — DBTMA з напрямленими антенами: зменшує колізії шляхом просторової ізоляції передач.

MACA-D (MACA with Directional antennas) — варіант MACA, що використовує напрямлені антени для обмеження зони впливу передачі.

OMNeT++ — середовище дискретного моделювання мереж (Open Modular Network Testbed): програмна платформа для симуляцій комп’ютерних мереж і систем, з гнучкою модульною структурою.

ВСТУП

Сучасний розвиток цифрових технологій, а також зростаючі потреби в системах моніторингу та автоматизованого збору даних стимулюють активне впровадження безпровідних сенсорних мереж (БСМ) в різних галузях — від екологічного спостереження до промислової автоматизації. БСМ є особливим класом розподілених мереж, які складаються з великої кількості малопотужних сенсорних вузлів, які взаємодіють між невикористаною фіксованою інфраструктурою. Ефективне функціонування такої системи неможливо без оптимального управління обміном даними на рівнях доступу до середовища, що обумовлює актуальність дослідження методів керування доступом у БСМ.

У першому розділі цієї роботи надано загальну характеристику БСМ, представлено історичні передумови їх виникнення, типи архітектури сенсорного вузла та основні особливості побудови таких мереж. Значну увагу приділено аналізу енергетичних та функціональних обмежень, які ускладнюють проектування протоколів і систем зв’язку в умовах обмежених ресурсів.

Другий розділ присвячено аналізу методів управління доступом до середовища передачі в БСМ. Розглянуто класифікацію MAC-протоколів, їх основні функції та принципи побудови. У роботі наведено порівняльну характеристику конкурентних та планових протоколів, а також протоколів з резервуванням та маршрутизацією.

У третьому розділі акцент зроблено на проблемі досягнутої станції — разом із ключовими причинами виникнення колізій у безпровідних мережах. Проведено моделювання типової конфігурації мережі, в якій проявляється дана проблема, та наведено результати симуляції. Розглянуто можливості способів її вирішення, зокрема через вдосконалення логіки взаємодії вузлів, використання додаткових сигналів, блокування та реалізацію альтернативних MAC-методів.

1 ОСНОВИ ПОБУДОВИ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

1.1 Загальна характеристика безпроводових сенсорних мереж

«Безпровідні сенсорні мережі (БСМ) – це розподілені самоорганізуючі мережі, які складаються з великої кількості сенсорів об'єднаних між собою за допомогою радіоканалу. Область покриття подібної мережі може становити від декількох метрів до декількох кілометрів, за рахунок можливості ретрансляції повідомлень від одного елемента до іншого. Безпровідні сенсорні мережі знаходять використання в різних сферах діяльності, зокрема, в системах технічної безпеки, екологічного моніторингу, в системах контролю та управління технологічними процесами.»[10]

Це твердження каже нам про те, що безпроводові сенсорні мережі – які складаються з багатьох не великих пристроїв, так званих сенсорів. Вони самостійно здатні налагодити зв’язок без участі спеціалізованого керівного центру. Спілкування між об’єктами мережі відбувається за допомогою радіозв’язку, тобто в них не має потреби в кабелі, щоб здійснювати обмін даними між вузлами. Один окремий вузол цілком здатен передати данні, що він зібрав, іншому, той в свою чергу – наступному за ланцюгом, з цього випливає, що мережі даного типу однаково добре підходять для розгортання як на не великій території так і значно більшій. Прикладом розгортання на невеликій території може слугувати дім або навіть одна кімната, але нічого не заважає розгорнути їх і на більшій території до прикладу територія заводу чи цілого сільськогосподарського поля. Ці мережі можуть бути застосовані у великій кількості сфер: на сільськогосподарському полі вони можуть допомагати стежити за вологістю ґрунту, температурою в теплиці, в умовах заводу ці системи допомагають стежити за безпекою це стосується не лише питання не санкціонованого доступу а також пожежної небезпеки чи якщо на заводі працюють з небезпечними речовинами використовуючи БСМ є можливість відслідковувати їх у повітрі. Ці системи мають просто безліч застосувань, бо мають дуже високий показник гнучкості і показують свою

корисність в різних сферах. Це обумовлене їх легкістю розгортання, і можливістю працювати в умовах де просто не можливо розгорнути звичайні традиційні мережі.

Одна з основних функцій будь якої мережі – це передача даних і БСМ не виключення. Ця функція забезпечує узгодженість роботи вузлів безпроводової сенсорної мережі. Специфіка цієї задачі обумовлена особливими вимогами до енергоефективності та здатності мережі пристосовуватися до постійно змінюваної топології. На початкових етапах розвитку БСМ використовувалися стандартні на той час рішення, зокрема IEEE 802.11, впроваджений в 1997 році як один з основних стандартів безпроводового сенсорного зв’язку. Він охоплює різні частотні діапазони наприклад 2,4 ГГц для IEEE 802.11b/g та 5 ГГц для IEEE 802.11a. Попри наявні переваги в вигляді високої пропускної здатності та поширеність в системах з високими вимогами до швидкості передачі даних, через високе енергоспоживання IEEE 802.11 його застосування у БСМ є обмеженим.

Оскільки сенсорні вузли мають працювати в режимі енергетичної автономії, пріоритетом стає мінімізація енергетичних втрат,а не максимальна швидкість передачі даних. Зазвичай інформація яку збирає та передає сенсорний вузол має невеликий об’єм, тому відпадає потреба високої пропускної здатності в каналі зв’язку. Тому в процесі розвитку безпроводових сенсорних мереж були створені нові протоколи передачі даних які не могли похизуватися високою пропускною здатністю, проте мали значно більші показники енергоефективності. Як приклад можна навести стандарт IEEE 802.15.4, розроблений спеціально для малопотужних безпроводових пристроїв. Він здатен забезпечувати надійний зв'язок на коротких відстанях, окрім цього має широку підтримку у більшості сенсорних вузлів.

За умов що діапазон передачі дозволяє кожному з вузлів безпосередньо передавати данні до базової станції утворюється топологія зірка ілюстрацію якої можна побачити ліворуч на рис.1.1. В такій топології спрощена

маршрутизація за рахунок того, що дані передаються до станції минаючи проміжні вузли. Це знижує затримки, зменшує витрати на обчислення на рівні вузлів, але при цьому значно зростає навантаження на передавач і призводить до швидкого розряду елементів живлення.

У більш практичних ситуаціях використовується багатострибкова топологія, її можна побачити на рис.1.1 праворуч. За такої топології використовуються проміжні вузли який може бути один або декілька. Використання такого підходу дозволяє зменшувати радіус дії окремих вузлів, відповідно зменшуючи енергоспоживання. В багатострибкових мережах окремі вузли виступають в ролі ретрансляторів, вони приймають повідомлення від сусідніх вузлів та передають їх до базової станції. Це вимагає реалізовувати ефективні механізми маршрутизації, які мають здійснювати пошук шляхів передачі з урахуванням поточного стану мережі, заряду який мають вузли та можливих збоїв.

Базова ретрансляція не єдине що виконують вузли в багатострибкових мережах не рідко вони беруть на себе попередню обробку та агрегацію даних. Така обробка дає можливість зменшити обсяг інформації, яку потрібно передати, за рахунок вилучення надлишкових або дубльованих даних, окрім цього інформацію стискають. Це зменшує навантаження на мережу та знижує витрати енергії яку використовують для передачі. Сенсорний вузол за таких умов є не лише приймач або передавач, а окремий обчислювальний елемент,який виконує задачу локальної фільтрації,агрегування та навіть може приймати прості рішення.

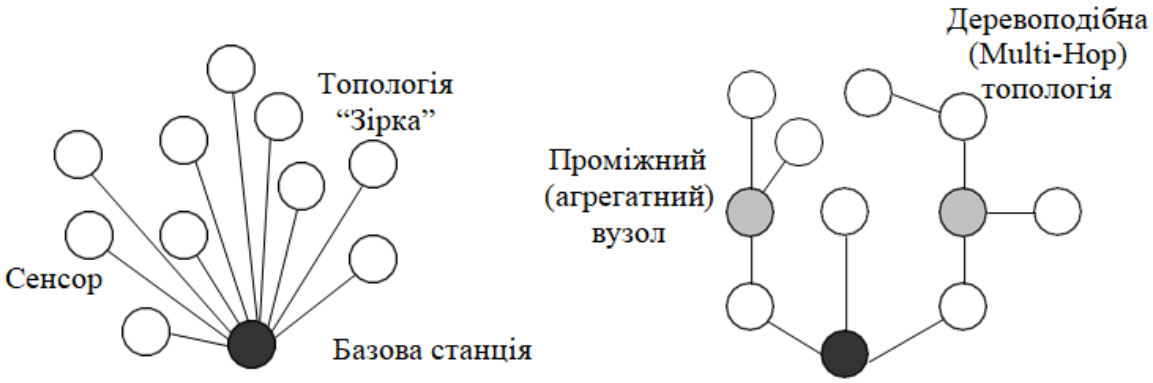


Рисунок 1.1 – “Однострибкова” і “багатострибкова” топологія в сенсорних мережах [12]

1.2 Історія безпроводових сенсорних мереж

Як і багато технологій, особливо в сфері зв’язку, історія безпроводових сенсорних мереж починається з військових досліджень, які й стали каталізатором до подальшого розвитку цієї галузі. Вперше концепція з’явилась у 1978 під час семінару «Distributed Sensor Networks», який було зібрано з ініціативи агентства передових оборонних дослідницьких проектів США (DARPA). «Семінар приділяв особливу увагу науково-дослідним завданням в галузі сенсорних мереж, таких, як мережні технології, методи обробки сигналів і технології розподілених обчислень»[12]

На початку 1980-х років DARPA ініціювало програму DSN(Distributed Sensor Networks), яка стала основою для побудови розподілених інтелектуальних систем збору даних. Логічним продовженням програма SensIT(Sensors in Information Technology), «Основною метою програми SensIT є створення нового класу програмного забезпечення для розподілених мікросенсорів. Програма має два ключові напрямки: а) розробка нових мережевих методів для розгортання спеціальних мікросенсорів, та б) використання парадигми розподілених обчислень для вилучення правильної та своєчасної інформації з поля датчика, включаючи виявлення, класифікацію та відстеження цілей. Програма має п'ять завдань: фіксовані

мережі, фіксовано-мобільні мережі, спільна обробка сигналів та інформації, запити/завдання та інтеграція.»[3]

Одним з перших масштабних проєктів, що поєднував ці напрямки, став WINS (Wireless Integrated Network Sensors) «Бездротові інтегровані мережеві датчики (WINS) забезпечують розподілений доступ до мережі та Інтернету до датчиків, елементів керування та процесорів, вбудованих в обладнання, приміщення та навколишнє середовище. WINS поєднують сенсорну технологію, обробку сигналів, обчислення та можливості бездротової мережі в інтегрованій системі. Технологія інтегральних схем тепер дозволяє створювати датчики, радіоприймачі та процесори за низькою ціною та низьким енергоспоживанням, що дозволяє масове виробництво складних, але компактних систем, які зв'яжуть фізичний світ з мережами. Масштаби варіюватимуться від локальних до глобальних, із застосуваннями, включаючи медицину, безпеку, автоматизацію виробництва, моніторинг навколишнього середовища та обслуговування на основі стану. Компактна геометрія та низька вартість дозволяють вбудовувати та розповсюджувати WINS за невелику частку вартості звичайних дротових систем датчиків та виконавчих механізмів. Це може забезпечити роботу сотень або тисяч датчиків на користувача, що призводить до багатьох нових проблем проектування мереж.»[7] Результатом проекту WINS стала реалізація концепції малопотужних інтегрованих сенсорів LWIM (Low-power Wireless Integrated Microsensors), яку було побудовано на основі CMOS-чіпу з інтегрованими датчиками, мікроконтролером, цифровими схемами обробки та безпроводових зв’язком.

Наступним знаковим кроком у розвитку БСМ став проєкт Smart Dust («Розумний пил»), ініційований університетом Каліфорнії у Берклі. Метою проєкту було довести, що повнофункціональний сенсорний вузол може бути мініатюризований до розміру піщинки або навіть частки пилу. Ці мініатюрні пристрої, відомі як motes, поєднували сенсори, обчислювальні компоненти та радіозв’язок на єдиній платформі. Як зазначено у публікації К. С. Потті та Г.

С. Пуела, «мініатюрні інтегровані сенсори, оснащені власними комунікаційними та обчислювальними можливостями, можуть забезпечити новий рівень інформованості про середовище». Результати цього проєкту не лише продемонстрували технічну можливість надмалої інтеграції, а й стали фундаментом для подальших розробок у сфері енергоефективних сенсорних вузлів.

Проєкт PicoRadio, що реалізовувався в рамках Berkeley Wireless Research Center (BWRC), продовжив ці розробки, зосередившись на створенні пристроїв із настільки низьким енергоспоживанням, що вони могли працювати, використовуючи лише енергію з навколишнього середовища — наприклад, сонячну, теплову чи коливальну. В цьому ж напрямі було реалізовано й проєкт μAMPS (micro-Adaptive Multi-domain Power-aware Sensors), який було започатковано Массачусетським технологічним інститутом. Особливість цієї ініціативи полягала в поєднанні апаратних засобів на базі мікроконтролерів, здатних динамічно масштабувати обчислювальну потужність, із програмними алгоритмами, оптимізованими для зменшення енергоспоживання за рахунок гнучкої структури обробки даних. У роботі Ч. Шен, присвяченій енергозберігаючим архітектурам для мережевих сенсорів, підкреслюється, що «самоорганізовані вузли, які можуть працювати на енергії з навколишнього середовища, є основою майбутніх розгортань сенсорних мереж» [9].

Паралельно з академічним напрямом, починаючи з початку 2000-х років, почали з’являтися і перші комерційні продукти, орієнтовані на практичне застосування технологій БСМ. Численні компанії, зокрема Crossbow, Sensoria, Dust Networks, Ember Corporation та Worldsens, активно інтегрували напрацювання університетських лабораторій у серійні рішення. Вони розробляли платформи, що включали готові до розгортання сенсорні вузли з інтегрованими засобами збору, передавання й обробки даних, а також програмне забезпечення для візуалізації та налаштування систем у реальному часі. Комерційні системи мали модульну структуру, що дозволяло

адаптувати їх до різних сценаріїв використання: від екологічного моніторингу та аграрних застосувань до інфраструктурної діагностики й розумних будівель.

Таким чином, історія розвитку безпроводових сенсорних мереж ілюструє поступове перетворення цієї технології з вузькоспеціалізованої військової концепції в універсальний інструмент цивільного й промислового призначення. Завдяки фундаментальним дослідженням, експериментальним реалізаціям і комерціалізації ідей, БСМ стали одним із ключових компонентів Інтернету речей, забезпечуючи невимушений, масштабований і енергоефективний спосіб інтеграції фізичного світу в цифрову інфраструктуру.

1.3 Архітектура сенсорного вузла

Перед розглядом особливостей побудови безпроводових сенсорних мереж доцільно проаналізувати базовий елемент їхньої структури — сенсорний вузол. Сенсорний вузол є функціональною одиницею мережі, яка забезпечує збір, обробку та передачу інформації. Для повного розуміння принципів його роботи необхідно детально розглянути архітектуру вузла, складові компоненти та механізми їх взаємодії.

Підсистема збору інформації включає в себе один або більше сенсорів які є тим елементом який ретранслює, що відбувається навколо сенсорного вузла в процесор, за допомогою аналогово-цифрового перетворювача(АЦП) з використанням мультиплексування для передачі сигналів до процесора. Енергія фізичних явищ не знаходиться у вигляді який може обробити процесор, вона представляє собою безперервний аналоговий сигнал з амплітудою, що розглядається як функція від часу тому для обробки її цифровим процесором використовується АЦП. На даний момент розроблена велика кількість сенсорів за допомогою яких можна вимірювати, фіксувати та оцінювати різні фізичні процеси.

Підсистема обробки даних інтегрує всі інші підсистеми та периферійні пристрої. ЇЇ головне призначення — виконання інструкцій, що забезпечують функціонування датчиків, систем зв'язку та самоорганізації. Вона складається з інтегрального процесора, постійної пам'яті (переважно внутрішньої флеш-пам'яті) для зберігання програм, активної пам'яті для тимчасового зберігання даних вимірювань та внутрішнього годинника. Хоча під час створення бездротового вузла можна вибирати з широкого спектру готових процесорів, до цього вибору слід підходити дуже ретельно, оскільки він впливає на ціну, гнучкість, продуктивність та енергоспоживання вузла. Якщо завдання збору даних чітко визначені на етапі специфікації та не змінюються з часом, розробник може вирішити використовувати програмовану логічну матрицю або цифровий сигнальний процесор. Ці процесори дуже енергоефективні та здатні виконувати найпростіші вимірювальні завдання. Однак, оскільки це не процесори загального призначення, розробка та впровадження вузла на їх основі може бути складною та дорогою. У більшості практичних випадків завдання вимірювання можуть змінюватися або може знадобитися модифікація. Крім того, програмне забезпечення бездротового вузла може вимагати від вас оновлення або налагодження віддалено. Такі завдання вимагають значної кількості обчислювальних ресурсів, і в цьому випадку спеціалізовані енергоефективні процесори не відповідають вимогам. Більшість існуючих сьогодні сенсорних вузлів використовують мікроконтролери. BSM – це технологія, що постійно розвивається, і спільнота розробників все ще активно шукає більш енергоефективні протоколи зв'язку та алгоритми обробки сигналів. Оскільки це вимагає встановлення та оновлення динамічного коду, мікроконтролери є найкращим варіантом.

Підсистема зв'язку Так само, як вибір правильного типу процесора важливий для продуктивності та енергоспоживання сенсорного вузла, спосіб підключення компонентів до процесора впливає на його продуктивність. Швидка та енергоефективна передача даних між підсистемами бездротового

сенсорного вузла має вирішальне значення для загальної ефективності мережі. З іншого боку, практичний розмір вузла накладає обмеження на системні шини. Хоча зв'язок через паралельну шину швидший, ніж через послідовну шину, паралельна шина є громіздкою. Крім того, кожен біт вимагає виділеної лінії, яка має передаватися одночасно, тоді як шина стороннього виробника вимагає лише однієї лінії даних. Через ці обмеження на практиці використовуються лише послідовні шини. Тому можна вибирати між послідовними інтерфейсами, такими як послідовний периферійний інтерфейс (SPI), загальний ввід/вивід (GPIO), безпечний ввід/вивід даних (SDIO), інтегральна схема (IC) та універсальна послідовна шина (USB). Серед них найпоширенішими є SPI та I2C .

Підсистема живлення основною її функцією є постачання електроенергії до інших підсистем. Також вона виконує завдання оптимізації споживання енергії керуючи режимами роботи вузла, зокрема у періоди не активності вона переводить їх в стан зниженого споживання енергії. Ефективність роботи підсистеми живлення є критичним важливою, бо вона визначає тривалість яку сенсорний вузол може функціонувати автономно. Енергетичні ресурси в таких системах обмежені, тому слід приділити особливу увагу впровадженню механізмів енергозбереження та додаткових модулів збору енергії, які в свою чергу дозволять перетворити енергію навколишнього середовища на придатну до використання сенсорним вузлом. Узагальнюючи, підсистема живлення забезпечує підтримку життєдіяльності вузла й підвищує показники енергоефективності і функціональної надійності.

Таблиця 1.1 – Сенсори, що застосовуються в БСМ

Тип сенсора	Вимірюваний параметр	Приклади технологій	Типові застосування
Температурні сенсори	Температура	Термістори, термопари	Моніторинг навколишнього середовища
Сенсори тиску	Атмосферний або механічний тиск	П'єзорезистивні, ємнісні датчики	Контроль інфраструктури, медицина
Оптичні сенсори	Освітленість, інтенсивність світла	Фотодіоди, фототранзистори, ПЗЗ-матриці	Інтелектуальне освітлення, відеоспостереження
Сенсори руху і вібрацій	Прискорення, вібрація	Акселерометри, гіроскопи	Охоронні системи, моніторинг об'єктів
Сенсори вологості	Вологість повітря	Ємнісні та резистивні датчики	Сільське господарство, системи кондиціонування
Акустичні сенсори	Звуковий тиск	Мікрофони, ультразвукові сенсори	Акустичний моніторинг, виявлення подій
Сенсори положення і переміщення	Положення в просторі	GPS-модулі, інклінометри	Моніторинг руху транспортних засобів
Сенсори хімічного складу	Газовий або рідинний склад	ІЧ-датчики газу, електрохімічні сенсори	Виявлення забруднень, контроль безпеки
Сенсори електромагнітних полів	Індукція, магнітне поле	Датчики Холу, магнітометри	Промисловий моніторинг, геофізичні дослідження

1.4 Особливості безпроводових сенсорних мереж

Чим же БСМ відрізняється від традиційних мереж? Порівнюючи ці два підходи до побудови мереж не можна не помітити, що БСМ, як правило, мають вузьку спеціалізацію. На відміну від традиційних мереж перед якими стоїть задача обслуговування широкого спектру додатків середел яких є передача даних, голосу й відео, виконання хмарних обчислень та багато інших сервісів. БСМ орієнтовані на ефективне виконання однієї задачі прикладом якої може бути моніторинг температури, вологості, руху, вібрацій чи тиску. Зумовлюється це тим, що такі мережі проектується як чистина системи, головним завданням якої є – отримання показників сенсорів у реальному часі.

Наступною ключовою відмінністю є – жорсткі обмеження в споживанні енергії якими характеризуються БСМ. Традиційні мережі будуються з метою досягнути високої пропускної здатності, високої надійності, та низьких затримок. Питання енергоспоживання не є пріоритетним. В БСМ вузли живляться від батарей або збирають енергію навколишнього середовища, питання енергозбереження таким чином стає пріоритетним, оскільки термін служби мережі прямо залежить від її енергоефективності. Тому в них діють спеціалізовані протоколи доступу до середовища, алгоритми за якими працює маршрутизація та механізми управління живленням, які створені для мінімізації втрат енергії на кожному з рівнів – від фізичного до прикладного.

Ще одною з особливостей БСМ є їх спосіб розгортання. Якщо при побудові традиційних мереж спочатку готують план, в якому прописано розміщення вузлів, як саме будуть прокладені кабелі, розраховується з яким навантаженням може працювати мережа і ще багато не менш важливих показників. То БСМ, навпаки, розгортається за принципом ad hoc, що означає структура, кількість вузлів, ресурси визначаються на місці розгортання і залежать від умов середовища де система має працювати. З цього випливає

необхідність в самоорганізації, само налаштуванню та автономному виборі топології, яка здатна забезпечити високі показники в зв’язку та енергоефективності.

Додатково варто підкреслити різницю в умовах в яких ці мережі експлуатуються. Коли традиційні мережі в більшості своїй працюють у контрольованому та сприятливому середовищі, де мінімізовані фактори впливу з навколишнього середовища. Безпроводові сенсорні мережі зазвичай вимушені працювати в агресивному середовищі, такому як промислові об’єкти, сільськогосподарські поля, об’єкти гірничодобувної промисловості і звісно ж в умовах застосування військовими. За таких умов не йдеться про легкий фізичний доступ до мережевих компонентів, а іноді він взагалі не можливий, що ставить високі вимоги до надійності вузлів та здатності мереж до відновлення функціонування після виходу з ладу окремих елементів цієї мережі.

Що ще хотілося б відмітити так це відмінність в принципах управління. Для початку подивимось як це влаштовано в традиційних мережах. Там передбачено, що мережа має централізоване управління, завдяки цьому є можливість провести глобальний огляд стану мережі та здійснювати централізоване прийняття рішень. В безпроводових сенсорних мережах же більшість рішень делеговані на рівень окремих вузлів або ж їх кластерів. Що дозволяє забезпечувати гнучкість яка забезпечує працездатність за змін у топології мережі, зменшує навантаження на центральний вузол (за його наявності), також дозволяє зменшити затримки прийняття рішень.

В таблиці 1.1 наведено коротке порівняння традиційних та безпроводових сенсорних мереж з [12]

Таблиця 1.2 – Порівняння традиційних мереж і БСМ [12]

Традиційні мережі	Безпроводові сенсорні мережі
Загальноприйнятий дизайн; обслуговують багато додатків	Одноразовий дизайн; обслуговують один конкретний додаток
Типові обмеження відносяться до пропускної спроможності і затримок; споживання енергії не розглядається	Споживання енергії – головний обмежуючий чинник при проектуванні вузлів і мережі в цілому
Мережа розробляється згідно з планом	Розгортання мережі, її структура і ресурси, як правило, визначаються на місці (ad hoc)
Пристрої і мережа працюють в контрольованому і сприятливому середовищі	Сенсорні мережі часто працюють в “агресивному” середовищі
Підтримка і ремонт є типовими, компоненти мережі легкодоступні	Фізичний доступ до компонент мережі часто ускладнений або неможливий
Компоненти, що вийшли з ладу, ремонтуються і відновлюються	Відмова компонентів передбачена і компенсується за рахунок побудови мережі
Отримання повних відомостей по мережі можливе і централізоване управління можливо	Більшість рішень приймаються без центрального керуючого вузла

1.5 Енергетичні та функціональні обмеження БСМ

Як зазначено в навчальному посібнику Основи побудови безпроводових сенсорних мереж «Тоді як сенсорні мережі мають багато спільних проблем з іншими розподіленими системами, вони можуть мати різноманітні унікальні складнощі і обмеження. Ці обмеження впливають на конструкцію БСМ, що вимагає особливих протоколів і алгоритмів, які відрізняються від своїх аналогів в інших розподілених системах. У цьому розділі описуються найбільш важливі конструктивні обмеження у БСМ.»[12]

1.5.1 Енергетичні обмеження

Основним каменем спотикання в який впираються всі БСМ – це факт того що вузли працюють в умовах обмеженого запасу енергії. Більшість вузлів мережі працюють від автономних джерел енергії, таких як батареї та акумулятори. І після вичерпання заряду вузли які не мають можливості заряду припиняють своє функціонування. Бо часто в таких системах технічне обслуговування або заміна є складною або взагалі не можливою задачею.

Особливо актуально для сенсорів у віддалених регіонах або небезпечних умовах.

Вимоги до тривалості автономної роботи вузлів визначаються параметрами прикладних задач. Наприклад при моніторингу глобальних геофізичних процесів або ж зміни метеорологічних показників на довгій дистанції вузли повинні мати змогу працювати протягом кількох років. В екстрених ситуаціях такі як військові дії чи техногенні катастрофи час роботи може не перевищувати кілька діб, або навіть годин. Незалежно від призначення, енергетична ефективність є одним із пріоритетних завдань під час проєктування БСМ, це вимагає враховувати енергоспоживання на рівнях від фізичного до високорівневих протоколів взаємодії.

Головним джерелом споживання енергії розташований на фізичному рівні є процесор вузла. В БСМ досить поширеними є мікросхеми засновані на базі CMOS, загальна витрата енергії визначається двома компонентами енергією перемикання та витоку. В посібнику Основи побудови безпроводових сенсорних мереж [12] наведено таку формулу розрахунку загальних витрат енергії:

$$E_{CPU} = E_{switch} + E_{leakage} = C_{total}V_{dd}^2 + V_{dd}I_{leak}\Delta t \qquad (1.1)$$

де Ctotal – загальна ємність, перемикається залежно від розрахунку; Vdd – напруга живлення, Ileak – струм витоку, а Δt – тривалість обчислень. Зараз енергія перемикання складає більшу частину споживання . В майбутньому, з розвитком технологій значення енергії витоку може перевищувати половину загального споживання. Деякі методи контролю енергії витоку працюють на основі відключення невживаних компонентів і програмного забезпечення, яке базується основі методів, таких як Dynamic Voltage Scaling (DVS).

Рівень доступу до середовища грає важливу роль в енергоефективності. Якщо сенсорні вузли працюють в у конкурентному режимі, неминуче виникають ситуації конфлікту, в яких кілька вузлів намагаються передати повідомлення. Що призводить до повторних спроб передачі та відповідно збільшення енергоспоживання. Натомість в протоколах не конкурентного типу, зокрема на баз TDMA, передача відбувається в попередньо визначені часові інтервали, що дозволяє вузлам вимикати радіо приймачі у проміжках між передачами. Цей підхід значно виграє в питанні витрат енергії

На мережевому рівні поставлені задачі досягаються шляхом, що враховує не лише відстань до базової станції, а й залишкову енергію у вузлах, що можуть виступати ретрансляторами. Оптимізація маршрутів дозволяє зменшити енергоспоживання на рівні всієї мережі, а також уникнути дисбалансу в питанні заряду вузлів коли один вузол вже не може працювати а інший ще має багато заряду. Додатковий ефект реалізується за рахунок попередньої обробки даних на вузлах. Є багато випадків коли може бути доцільним здійснити стискання фільтрацію або агрегування інформації, для подальшої передачі. Хоч такий підхід дозволяє знизити витрати на передачу, проте потребує додаткові ресурси на обчислення, що в свою чергу тягне за собою необхідність в балансуванні енергоспоживання процесора та радіомодуля.

1.5.2 Самоорганізація

Як зазначено в посібнику Основи побудови безпроводових сенсорних мереж «Для систем, які використовують сенсорні мережі, типовими обмеженнями є робота у віддалених районах і суворих умовах, без підтримки інфраструктури або можливості обслуговування і ремонту. Таким чином, сенсорні вузли мають бути самокерованими (здатні до самоорганізації) відносно налаштування 15 власних параметрів, взаємодії з іншими вузлами,

адаптації до збоїв, змінам довкілля, а також зміни чинників, які впливають на довкілля, без втручання людини.» [12]

Як вже зазначалось вище БСМ розгортається за принципом ad hoc, що означає структура, кількість вузлів, ресурси визначаються на місці розгортання і залежать від умов середовища де система має працювати. Це в мережах, які знаходяться у віддалених і важкодоступних районах має особливу важливість. Візьмемо за приклад сенсори розраховані на роботу в умовах бойових дій, техногенних катастроф або природних лих, вони можуть бути викинуті за допомогою БПЛА, літаків або ж інших не гарантуючих цілісність всіх вузлів методів. В такому випадку багато вузлів можуть навіть не почати роботу, але вузли які змогли вціліти мають самостійно провести налаштування яке включає в себе: визначення своєї позиції та формування зв’язків з іншими вузлами та початок збору даних.

Як правило, сенсорні мережі після свого розгортання мають стабільно працювати без участі людини, що означає технічне обслуговування і ремонт, мають виконуватися наявними ресурсами. В реальних ситуаціях, сенсорні вузли знаходяться під впливом факторів як з зовні так і з середини які створюють перешкоди на шляху побудови надійних сенсорних мереж. Вузол БСМ має бути самокерованим, тобто стежити і адаптуватися до змін у навколишньому середовищі. Водночас вузол має працювати раз з іншими пристроями мережі щоб сформувати топологію або розподілити завдання між сусідніми вузлами. Самоорганізація за визначенням наведеним в посібнику Основи побудови безпроводових сенсорних мереж «термін, який часто використовується для опису здатності мережі до адаптації параметрів конфігурації на основі стану системи і довкілля. Наприклад, сенсорний пристрій може вибрати таку потужність передачі, щоб підтримувати певну міру зв'язку (тобто, зі збільшенням потужності передачі, ймовірніше, що вузол зможе встановити зв'язок з більшою кількістю сусідів)» [12]. В тому ж посібнику можна знайти визначення «Самооптимізація відноситься до здатності пристрою здійснювати моніторинг і оптимізацію використання

власних ресурсів», [12] «Самозахист дозволяє пристрою розпізнавати і протидіяти вторгненням і атакам» [12]. Ще варто відмітити здатність до самостійного відновлення, важлива характеристика яка описує здатність до автономного реагування та усунення мережевих збоїв.

1.5.3 Безпроводові мережі

Використання безпроводових систем для зв'язку між вузлами несе за собою деякі проблеми в розробці БСМ. Такі як зменшення потужності сигналу в умовах поширення в реальному середовищі, через наявність у ньому завад та перешкод для радіо сигналу. «Співвідношення між потужністю, що приймається, потужністю радіочастотного сигналу, що передається, може бути виражене за допомогою закону зворотних квадратів:

$$P_r \propto \frac{P_t}{d^2} \qquad (1.2)$$

який свідчить, що потужністьP_r, що приймається, пропорційна зворотній величині квадрата відстані d від джерела сигналу. Тобто, якщо P_r^x – потужність на відстані x, то збільшення відстані в два рази зменшує потужність на новій відстані до $P_r^y = \frac{P_r^x}{4}$.» [12]

Коли відстань між сенсорним вузлом і базовою станцією зростає, збільшується і вимоги до потужності сигналу що передається, відповідно збільшуючи споживання енергії. Задля зменшення витрат енергії можна реалізувати передачу шляхом серії коротких проміжків, що утворюють багато стрибкову мережу (multi-hop). Ця технологія вимагає взаємодії вузлів між собою для вирішення задачі пошуку найкращого шляху. Це є великою проблемою в мережах робочі цикли, тобто з ціллю збереження енергії вузи періодично припиняють своє функціонування. Наслідком цього є не можливість сусідніх вузлів використовувати їх як ретранслятори.

Вирішенням цієї проблеми є стратегія пробудження за запитом, це дозволяє переконатися що вузол може бути використаний за необхідності. Для цього в пристроях є два радіо модуля великої та малою потужності. Радіо модуль малої потужності використовується з метою отримати сигнал пробудження, і радіо модуль високої потужності що активується при введенні в робочий стан. Ще однією стратегією є адаптивна передача чергування, яка полягає в тому що поки одні вузли знаходяться в режимі енергозбереження інші мають залишатися активними, щоб забезпечувати функціонування мережі.

1.5.4 Децентралізоване управління

В БСМ зазвичай не представляється можливим здійснювати централізоване управління, через їх великий масштаб та енергетичні обмеження. Натомість, сенсорні вузли мають співпрацювати та разом із сусідами задля узгодження локальних рішень за відсутності глобальних даних. Результат цих розподілених алгоритмів буде не оптимальним, але може бути більш енергетично ефективним, за централізовані рішення. Для централізованих рішень базова станція може отримувати інформацію від усіх вузлів мережі, що дозволяє складати оптимальні маршрути, які буде передавати кожному з вузлів потрібний шлях. Децентралізований підхід дозволяє вузлам приймати рішення базуючись на інформації про сусідні вузли та їх відстань до базової станції. Хоч цей підхід може призводити до формування не оптимальних маршрутів проте він більш доцільний при ситуації частої зміни топології, через великі накладні витрати при централізованому управлінні.

1.5.5 Обмеження

В навчальному посібнику про обмеження в безпроводових сенсорним мережах сказано так «Тоді як можливості традиційних обчислювальних систем продовжують швидко рости, основним завданням розробки безпроводових мереж являється створення малогабаритних, дешевих і ефективних пристроїв. Призначені для виконання спеціалізованих завдань з невеликим споживанням енергії, типові сенсорні вузли мають обчислювальні здібності і можливості зберігати дані, співрозмірні з комп'ютерними системами минулого десятиліття. Потреба у невеликому форм-факторі і низьке споживання енергії також перешкоджає інтеграції багатьох бажаних компонентів, наприклад, GPS приймачів.» [12]. Побудова програмного забезпечення на різних рівнях керується обмеженнями та вимогами описаними вище. Операційним системам треба мати невеликий об’єм пам’яті та ефективно використовувати ресурси. Що цікаво, відсутність передових технологій спрощує створення операційних систем які мають бути ефективними та не великими. Окрім операційних систем обмеження впливають також на протоколи і алгоритми, які застосовують у безпроводових сенсорних мережах. Таблиці маршрутизації що містять усі потенційні напрямки передачі, зазвичай занадто великі для обмеженої пам’яті сенсорного вузла. Тому там зберігається лише не велика частина як приклад список сусідніх вузлів. Також варто згадати про алгоритми агрегації, вони можуть потребувати порівняно високих обчислювальних можливостей, які не можуть бути забезпечені на базі дешевих сенсорних вузлів. Таким чином завжди стоїть досить не тривіальна задача, забезпечити роботу в дуже обмежених апаратних можливостях

1.5.6 Безпека

Питання безпеки в БСМ стає досить чутливим, бо більшість інформації що збирають сенсори є конфіденційною. А через віддаленість та автономну роботу зростає небезпека вторгнень та атак. Крім того безпроводове середовище спрощує задачу прослуховування мережі для ворога. Загроз звісно є багато але особливо складною в захисті від неї в БСМ є DoS (Denial of Service), українською атака відмови в обслуговуванні, її метою є порушення нормальної роботи мережі. Є різні шляхи якими це можна досягнути одним з яких може бути заглушення, тобто використання потужних безпроводових сигналів для унеможливлення встановлення зв’язку між вузлами. Наслідки можуть варіюватися від сфери в якій застосовується конкретна мережа. Хоч існують готові рішення цих проблем безпеки, але всі вони розраховані на розподілені системи та не підходить для впровадження в БСМ через їх значні вимоги до обчислювальних потужностей, швидкості передачі даних та об’єму пам’яті. Ресурси сенсорних вузлів обмежені і не відповідають цим вимогам. Тому БСМ потребують своїх рішень для шифрування, аутентифікації, створення та поширення секретних ключів.

1.5.7 Інші проблеми

З вже наведеної інформації можна зробити висновок, рішення в БСМ доволі часто відрізняються від рішень в інших мережах. У таблиці 1.2 наведено чим відрізняються традиційні мережі та БСМ. Крім основних обмежень, на конструкцію сенсорних вузлів здатні впливати й інші фактори. Такі як, розміщення сенсора на рухомому об’єкті по типу дрона або транспортного засобу, що змушує топологію мережі до постійних змін. За таких умов маршрутизація, доступ до середовища, та агрегація даних потребують оперативної адаптації.

Сенсорні мережі часто бувають неоднорідними тобто складаються з пристроїв які мають різне апаратне забезпечення. Це добре описано в навчальному посібнику Основи побудови безпроводових сенсорних мереж «Наприклад, вузли датчиків можуть мати більше апаратних ресурсів, якщо їх завдання зондування вимагає більше обчислень і зберігання даних, або якщо вони відповідають за збір і обробку даних, отриманих від інших датчиків в мережі. Крім того, деякі сенсори можуть мати специфічні вимоги до продуктивності і якості, наприклад, низькі затримки для критичних подій або високу пропускну спроможність для відео даних. Як неоднорідність, так і вимоги до продуктивності впливають на дизайн безпроводових датчиків та їх протоколів.» [12]

Також проблема варта уваги це що на відміну від традиційних мереж де давно встановились єдині стандарти. Більшість рішень в БСМ є пропрієтарними тобто є власними рішеннями окремих компаній. Відкриті стандарти з’являються повільно. Це важливо тому, що відкриті стандарти забезпечують сумісність, полегшують розробку та розгортання програмного забезпечення в безпроводових сенсорних мережах.

1.6 Висновки з розділу 1

В першому розділі дипломної роботи було охоплено : загальну характеристику, історію, та особливості БСМ також було викладено архітектуру сенсорного вузла, а особливу увагу приділено енергетичним та функціональним обмеженням безпроводових сенсорних мереж. В розділі наведено дві таблиці перша з яких містить інформацію про те які типи сенсорів використовуються БСМ та приклади їх застосувань. В другій порівнюються традиційні мережі з безпроводовими сенсорними мережами. Ґрунтуючись на представлені про те що собою представляють БСМ та які вимоги вони ставлять перед методами управління доступом можна сміливо переходити до другого розділу

2 МЕТОДИ УПРАВЛІННЯ ДОСТУПОМ ДО СЕРЕДОВИЩА В БСМ

2.1 Роль і функції MAC-рівня

Модель OSI – абстрактна мережева модель для комунікацій і розроблення мережевих протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії.

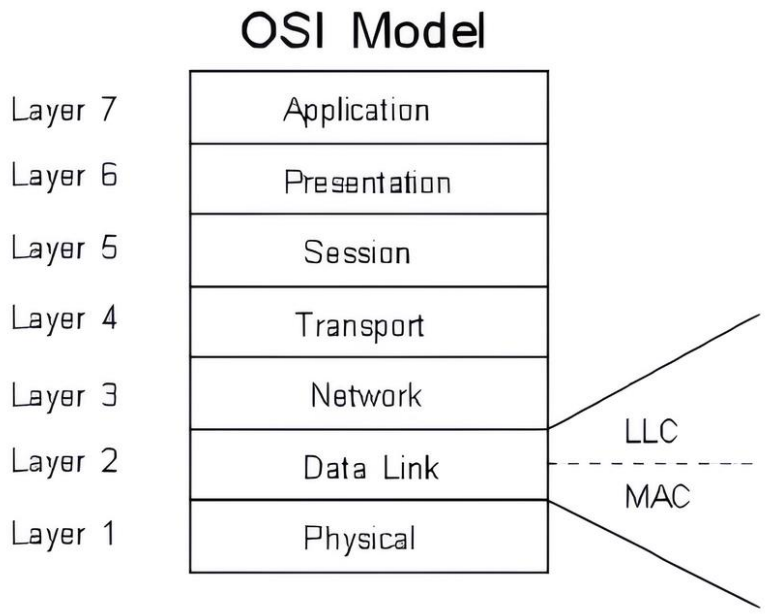


Рисунок 2.1 – Open Systems Interconnection Basic Reference Model (OSI) [6]

MAC (Medium Access Control (MAC)) – належить до канального рівня моделі OSI. «Шар MAC займається методом контролю доступу і визначає, як Використання фізичної передачі контролюється і забезпечує жетонне кільце Протоколи, які визначають, як працює кільце токенів.» [6]

2.2 Класифікація протоколів:

Згідно класифікації в [8] «MAC-протоколів випливає шість ключових характеристик: Розділення каналів та доступ, топологія, споживання енергії, ініціація передачі, навантаження трафіку та масштабованість, дистанція.

Розділення каналів та доступ в [8] описано так «Ключовим фактором у розробці протоколу MAC для ad hoc мереж є спосіб використання доступного середовища. Попередні підходи передбачали спільний канал для всіх станцій, тоді як новіші підходи використовували кілька каналів для більш ефективного використання середовища. Більшість запропонованих протоколів припускають, що базовий фізичний канал використовує радіочастотні (РЧ) сигнали. Нещодавно для ad hoc мереж були запропоновані інші технології фізичного рівня: надширокосмуговий радіозв'язок (UWB) та акустичний зв'язок . UWB - це схема передачі без несучої, яка обіцяє вищі швидкості передачі та більш складні механізми контролю доступу, ніж сучасна РЧ-технологія. Акустична технологія спирається на зв'язок через прості мікрофони та динаміки, які вже повсюдно поширені в багатьох мобільних пристроях. Ця технологія також багато років використовується в підводному зв'язку, оскільки акустичні сигнали поширюються далі, ніж РЧ-сигнали у воді. Існування кількох кандидатних технологій передачі даних породжує концепцію мультимодальних вузлів, які можуть переміщатися між мережами з різними фізичними каналами для досягнення деяких цілей повсюдних обчислень. Наприклад, вузол може переміститися з радіочастотної мережі в область, де існують лише вузли UWB. Для підтримки зв'язку вузол повинен бути оснащений для обох технологій зв'язку. Іншим прикладом мультимодальних вузлів є поверхневий буй у мережі підводних датчиків. Такий вузол зазвичай має акустичний модем для зв'язку з підводним середовищем. У цьому розділі ми класифікуємо протоколи як одноканальні або багатоканальні. Крім того, ми класифікуємо багатоканальні протоколи на основі їх механізму розділення каналів. У

рамках кожної стратегії розділення каналів ми описуємо метод доступу до каналу окремих вузлів.»

Згідно інформації в [8] «Спеціальні мережі зазвичай включають вузли з різними можливостями та ресурсами. Вузли також можуть бути мобільними, тому топологія активної мережі може часто змінюватися. Тому ефективний протокол – це той, який передбачає максимально узагальнену топологію. Мережа також повинна мати можливість адаптуватися до можливостей гетерогенних вузлів таким чином, щоб оптимізувати продуктивність та мінімізувати споживання енергії. Топологію мережі зазвичай можна описати з точки зору ієрархії та стрибків. Мережа може мати централізовану, кластерну або плоску топологію. У централізованому випадку один вузол або базова станція контролює та керує всіма іншими вузлами в мережі. Кластерні топології призначають один вузол у кожній групі вузлів для обробки локалізованого центрального керування групою. Плоскі топології розглядають повністю розподілений підхід, де всі вузли є одночасно вузлами та маршрутизаторами, а поняття централізованого керування відсутнє. Ми проводимо подальшу характеристику топологій протоколів, досліджуючи стрибкову природу мережі. Деякі протоколи припускають, що вузлам потрібно спілкуватися лише з досяжними сусідами, і їх називають протоколами з одним стрибком. Інші протоколи припускають, що вузли повинні спілкуватися за межами своїх досяжних сусідів, і що іноді пакет має бути ретрансльований через багато проміжних вузлів, щоб дістатися до місця призначення. Ми називаємо ці протоколи багатострибковими. Однострибкові протоколи є простими, але обмежувальними, оскільки вони пропонують обмежену підтримку для більших мереж. Багатострибкові протоколи є більш загальними за обсягом та більш масштабованими, хоча вони вносять додаткову складність у механізми доступу до каналу. У запропонованих протоколах існує кілька комбінацій ієрархії та стрибків: однострибкова плоска топологія, багатострибкова плоска топологія, кластерна топологія, централізована топологія. У цьому розділі протоколи класифікуються

відповідно до їх топології та досліджується, як кожен вибір топології впливає на продуктивність мережі.»

Споживання енергії характеризується в [8] «Основним фактором при проектуванні протоколів MAC для ad hoc мереж є споживання енергії окремими вузлами та загальне споживання енергії мережею. Збереження енергії важливе для будь-якого типу мобільного вузла, незалежно від того, чи працює він у ad hoc чи інфраструктурній мережі, через обмежений заряд батареї. В інфраструктурних мережах ресурсомістка базова станція відповідає за керування доступом до каналів та їх розподілом, тоді як вузли споживають більшу частину своєї енергії для передачі даних. Однак в ad hoc мережах відсутність базової станції покладає тягар керування на один або кілька вузлів. Крім того, відсутність централізованого контролера збільшує ймовірність колізій та конфліктів призначення каналів, що призводить до більшого споживання енергії у вигляді керуючої сигналізації та повторних передач. Тому очевидно, що ми можемо досягти значної оптимізації енергоспоживання в цих мережах завдяки ретельному проекту протоколу MAC.». Також там же описано різні режими енергоспоживання та керування передачею живлення.

Класифікація протоколів за принципом ініціації передачі «Деякі протоколи використовують підхід, ініційований відправником, для передачі даних; інші обирають підхід, ініційований одержувачем. Вибір стратегії ініціації передачі залежить від типів додатків, які мережа має підтримувати. Історично протоколи, ініційовані відправником, були найпоширенішими донедавна.» [8].

Ще одною характеристикою за якою можна виділити групу протоколів є навантаження трафіку та масштабованість на основі викладеної в [8] ін формації можна зробити такий висновок про категорії поділені за цією ознакою. Багатоканальні протоколи та енергоефективні протоколи демонструють кращу продуктивність для мереж з високим навантаженням та високою щільністю. Протоколи TDMA та протоколи на основі резервування

найкраще працюють для мереж, де переважає голосовий трафік та трафік у режимі реального часу. Протоколи, які добре працюють для вибіркових сценаріїв, не підходять для загальної ad hoc мережі.

Останньою описаною в [8] характеристикою за якою поділяють протоколи дистанція на якій вони працюють. «Дальність передачі – це просто відстань радіопокриття одного вузла» [8]. «Ширина смуги пропускання – це швидкість каналу, на якій протокол моделюється або моделюється.» [8]. «Просторова ємність, яку також називають просторовою ефективністю, є мірою швидкості передачі інформації на квадратний метр і може сприйматися як міра щільності для протоколу.» [8].

Але не можна складати класифікацію ґрунтуючись лише на одному джерелі тому розглянемо інші підходи наприклад класифікація в [4] «характеризує різні аспекти роботи протоколів і поділяє їх на 3 категорії (із рукостисканням, управлінням маршрутизацією, використанням тонів зайнятості).»

Що таке протоколи з рукостисканнями звісно тут це слово використано в переносному значенні. Протоколи на основі рукостискання в бездротових сенсорних мережах – це клас протоколів доступу до середовища, в яких передача даних між вузлами здійснюється шляхом узгодження (сигналів запиту). Ця процедура і називається «рукостискання» дозволяє координувати взаємодію вузлів, зменшуючи ймовірність колізій, оптимізуючи споживання енергії та підвищуючи надійність передачі. Основною особливістю є алгоритм передачі в чотири кроки який діє за таким принципом першим кроком є ініціація відправник надсилає запит на передачу (RTS), другим кроком є підтвердження одержувач відповідає підтвердженням готовності прийняти дані (CTS), третім кроком передача даних: відправник надсилає дані, четвертим кроком є підтвердження прийому: одержувач підтверджує успішний прийом (ACK).

Протоколи керування маршрутизацією в бездротових сенсорних мережах це набір правил та алгоритмів, які спрацьовують, коли сенсорні

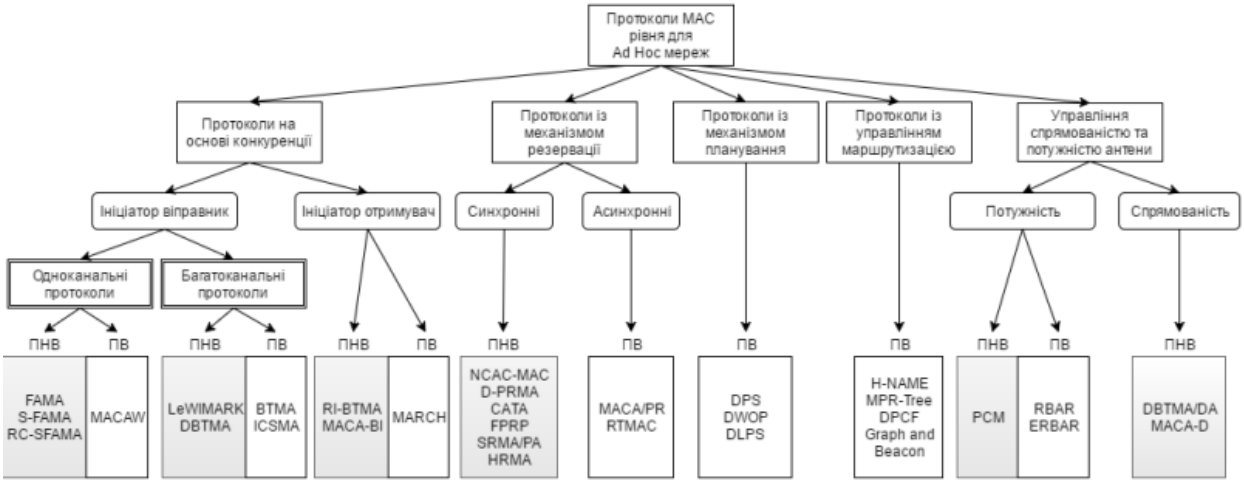
вузли передають дані від джерела (вимірювального вузла) до пункту призначення (звичайної базової станції або колекторного вузла). Вони забезпечують побудову маршруту, вибір оптимальних шляхів та адаптацію до змін топології, енергетичних ресурсів та трафіку. На відміну від традиційних мереж, протоколи маршрутизації в БСМ повинні працювати в умовах обмеженої енергії, пам'яті, обчислювальних можливостей та високої динаміки мережі. Вони не просто використовують шлях, який повинен пройти пакет, а формують логіку взаємодії вузлів таким чином, щоб забезпечити збір та доставку інформації з мінімальними витратами енергії та часу. Основні функції протоколів маршрутизації в БСМ: Вибір маршруту — визначення компонентів вузла, через які повинні проходити пакети даних. Адаптація маршруту — оновлення маршрутів у разі зміни доступності вузла (наприклад, при розряді або фізичному пошкодженні акумулятора). Балансування навантаження — уникнення перевантаження окремих вузлів, які часто використовуються як транзитні вузли. Агрегація даних — об'єднання подібних або дубльованих повідомлень для зменшення обсягу переданих даних. З урахуванням якості зв'язку та енергоспоживання — маршрут вибирається не лише на основі мінімальної кількості переходів, але й на основі вибору показників якості каналу та залишкової енергії вузлів.

Суть методу полягає в тому, що під час передачі даних один вузол одночасно випромінює спеціальний «сигнал зайнятості» (busy signal) на окремій частоті або в окремому каналі. Інші вузли, які могли б розпочати передачу, сприймають цей сигнал як індикатор зайнятості середовища та трактують його як власну передачу. Таким чином, використання сигналу «зайнято» дозволяє уникнути одночасного доступу кількох вузлів до каналу та, відповідно, запобігти колізіям до їх виникнення. Для коректної роботи протоколи сигналу зайнятості зазвичай передбачають: два радіоканали або діапазони частот один для передачі даних, другий для сигналу зайнятості. Два приймачі або трансивери на вузлі (або послідовне перемикання режимів), що дозволяє одночасно слухати та передавати. Протоколи з

використанням тонів зайнятості працюють за таким принципом. Спочатку відбувається підготовка до передачі коли вузол має дані для передачі, він спочатку перевіряє канал даних, щоб побачити, чи вільний він від передач іншими вузлами. Наступний крок передача сигналу зайнятості якщо канал вільний, вузол починає передавати сигнал зайнятості на окремому каналі (наприклад, на іншій частоті). Це сигналізує іншим вузлам, що хтось використовує середовище. Наступний крок передача даних одночасно з тоном зайнятості вузол передає власні дані по основному каналу. Наступний крок прийом та затримка іншими вузлами вузли, які мають намір передавати, виявляють наявність тону зайнятості та відкладають власну передачу на випадковий або запрограмований час. Наступний крок завершення передачі після завершення передачі даних вузол припиняє сигнал тону зайнятості, і середовище вважається вільним.

Продовжимо розглядати підходи до класифікації протоколів в [1,2,5] Показано кілька версій класифікації, які мають спільні критерії та структуру, але деякі протоколи, що входять до неї. У ній протоколи відрізняються способом доступу до каналу: на основі конкуренції (вільний доступ), з механізмом резервування, планування тощо. В основу наведеної далі класифікації покладено [1,2,5] з урахуванням особливостей наведених в [8,4]. В наведену класифікацію потрапили: протоколи на основі конкуренції, із механізмом резервації, із механізмом планування, із управлінням маршрутизацією, із управлінням потужністю та спрямованістю.

В статті Максимов, В. В., and Литвин О.О. "КЛАСИФІКАЦІЯ ПРОТОКОЛІВ MAC РІВНЯ ДЛЯ AD-HOC МЕРЕЖ." Наведено чудову схему в якій «Основний акцент зроблено на здатність протоколів вирішувати проблеми прихованих та незахищених вузлів»[11]



ПНВ – вирішення проблеми прихованих та незахищених вузлів
ПВ – вирішення проблеми прихованих вузлів

Рисунок 2.2 – Класифікація протоколів MAC рівня для Ad-Hoc мереж [11]

2.2.1 Протоколи на основі конкуренції

В статті "КЛАСИФІКАЦІЯ ПРОТОКОЛІВ MAC РІВНЯ ДЛЯ AD-HOC МЕРЕЖ." Протоколи на основі конкуренції описані так «Для протоколів на основі конкуренції характерна відсутність резервування ресурсів, а кожного разу, перед передаванням пакету вузол узгоджує із сусідами доступ до сумісно використовуваного каналу. Дані протоколи поділяються за ознакою ініціації передавання на протоколи із ініціатором відправником та отримувачем. Протоколи, в яких ініціатором виступає відправник, поділяються на одноканальні, в яких вся ширина смуги пропускання використовується як одне ціле, та багатоканальні, в яких ширина смуги пропускання поділяється на кілька каналів, що дозволяє підтримувати одночасне передавання кількома вузлами, та розділяти по різних каналах передавання службових та інформаційних пакетів. До одноканальних протоколів, в яких вирішується ПНВ ввійшли: FAMA, S-FAMA, RC-SFAMA. Серед багатоканальних проблему ПНВ вирішують протоколи Le-WIMARK та DBTMA. Протоколи із ініціатором отримувачем, які вирішують проблему ПНВ це: RI-BTMA, MACA-BI, а ПВ MARCH.» [11]

FAMA (Floor Acquisition Multiple Access) – Протокол множинного доступу Floor Acquisition Multiple Access (FAMA) вимагає, щоб станція отримала контроль над поверхом (тобто бездротовим каналом) перед передачею пакетів даних. Це досягається за допомогою механізму встановлення зв'язку, що включає обмін керуючими пакетами Request-To-Send (RTS) та Clear-To-Send (CTS) у поєднанні з визначенням несучої для уникнення колізій.

S-FAMA (Slotted Floor Acquisition Multiple Access) — Протокол базується на дисципліні доступу до каналу, яка називається множинним доступом до поверху (FAMA), яка поєднує як зондування несучої (CS), так і діалог між джерелом і приймачем перед передачею даних. Новий протокол використовує часові слоти і тому називається Slotted FAMA. Часові слоти усувають необхідність надмірно довгих керуючих пакетів, тим самим забезпечуючи економію енергії.

RC-SFAMA(RTS Competition Slotted Floor Acquisition Multiple Access) – запроваджує механізм конкуренції (Request To Send) RTS, щоб запобігти високій частоті відмов мережі, спричиненій проблемою кількох спроб RTS. Завдяки механізму конкуренції RTS передача корисних даних може бути успішно завершена, коли виникає ситуація кількох спроб RTS.

Le-WIMARK (Low Energy Wireless Medium Access through Record Keeping) – У LE-WiMARK вузли періодично передають повідомлення про стан Status Message (SM), що містить інформацію про свій поточний стан, вказуючи, чи вузол перебуває в режимі очікування, передає чи приймає, а також до/від кого. Вузли, які отримують SM, зберігають інформацію, що міститься в ньому, у локальній матриці. Прийнята потужність SM також зберігається і використовується як показник рівня потужності, необхідного для успішного досягнення передачі відповідної станції.

DBTMA (Dual Busy Tone Multiple Access) – у цьому для захисту пакетів RTS та DATA використовуються два тональні сигнали зайнятості відповідно. Тональний сигнал зайнятості передачі transmit busy tone (BTt)

вмикається відправником для захисту пакета RTS, а тональний сигнал зайнятості прийому (BTr) вмикається приймачем для захисту пакета DATA.

RI-BTMA (Receiver-Initiated Busy Tone Multiple Access)– У протоколі множинного доступу з ініціюванням приймачем сигналу зайнятості, подібному до BTMA, доступна пропускна здатність поділяється на два канали: канал даних для передачі пакетів даних і канал керування для передачі сигналів керування та тонів зайнятості. Вузол може передавати по каналу даних, лише якщо він виявить, що тон зайнятості відсутній на каналі керування.

MACA-BI (Multiple Access with Collision Avoidance – By Invitation)– це протокол, що ініціюється одержувачем, і він зменшує кількість таких обмінів керуючими пакетами. Замість того, щоб відправник чекав на отримання доступу до каналу, MACA-BI вимагає, щоб одержувач запитував у відправника надсилання даних, використовуючи пакет «Готов до отримання» (RTR) замість пакетів RTS та CTS. Таким чином, це двосторонній обмін (RTR-DATA) на відміну від тристороннього обміну (RTS-CTS-DATA) MACA.

MARCH (Media Access with Reduced Handshake) – Протокол доступу до медіа даних зі зменшеним числом це протокол, що ініціюється приймачем. MARCH, на відміну від MACA-BI, не вимагає жодного механізму прогнозування трафіку. Протокол використовує широкомовну природу трафіку від всеспрямованих антен для зменшення кількості підтверджень, що беруть участь у передачі даних.

2.2.2 Протоколи із механізмом резервації

«Протоколи із механізмом резервації поділяються на синхронні та асинхронні. В даних протоколах для здійснення передавання відбувається резервування пропускної здатності, також підтримується QoS. В протоколах, які входять до категорії синхронних вирішуються проблеми ПНВ: NCAC-

MAC, D-PRMA, CATA, FPRP, SRMA/PA, HRMA, а в асинхронних, лише проблема ПВ: MACA/PR, RTMAC» [11]

NCAC-MAC (Network Coding Aware Cooperative Medium Access Control) – Метою розробки NCAC-MAC є покращення пропускної здатності мережі шляхом інтеграції мережевого кодування в кооперативні комунікації на рівні MAC.

D-PRMA (Distributed Packet Reservation Multiple Access) – це схема на основі TDMA, де канал поділяється на кадри фіксованого та однакового розміру вздовж часової осі. Кожен кадр складається з s слотів, а кожен слот – з m мініслотів. Кожен мініслот можна додатково розділити на два поля керування: RTS/BI та CTS/BI (BI розшифровується як «індикація зайнятості»).

CATA (Collision Avoidance Time Allocation) – це гібридний протокол, який дозволяє вузлам конкурувати за часові слоти та резервувати їх. Крім того, CATA одночасно підтримує одноадресну, багатоадресну та широкомовну передачу. Схема конкуренції та резервування базується на уникненні колізій, а часові слоти організовані в синхронний кадр. На відміну від протоколу ADAPT, CATA не використовує базовий протокол розподілу для призначення слотів передачі. Тому кожен слот поділяється на п'ять міні-слотів. Перші чотири міні-слоти (позначені як CMS1 - CMS4) використовуються для захисту та резервування часових слотів шляхом обміну короткими керуючими пакетами. Останній міні-слот (позначений як DMS) використовується для передачі пакета даних.

FPRP (Five-Phase Reservation Protocol) – це протокол керування доступом до середовища на основі конкуренції для бездротових ad hoc мереж. FPRP використовує п'ятифазний процес резервування для встановлення розподілу слотів на основі множинного доступу з часовим поділом. Він дозволяє вузлу резервувати лише один слот в інформаційному кадрі. Після того, як вузол зарезервував слот, він припиняє конкуренцію за інші слоти. В результаті в решті слотів може бути менше конкуруючих

вузлів, тому часові слоти в інформаційному кадрі не використовуються FPRP повністю.

SRMA/PA (Soft Reservation Multiple Access with Priority Assignment) – є протокол м’якого резервування множинного доступу з призначенням пріоритетів (SRMA/PA). Протокол SRMA/PA дозволяє розподіленим вузлам конкурувати за часові слоти та резервувати їх за допомогою механізму «уникнення колізій» та «м’якого резервування», подібного до RTS/CTS, доповненого розподіленим та динамічним керуванням пріоритетом доступу, що практично забезпечує здатність розподіленого планування гарантувати вимоги QoS інтегрованих послуг.

HRMA (Hop-Reservation Multiple Access) – це багатоканальний протокол MAC, що базується на простих напівдуплексних радіостанціях з розширеним спектром та дуже повільною стрибкоподібною перебудовою частоти (FHSS). Він використовує механізм резервування та встановлення зв'язку, щоб пара вузлів, що зв'язуються, могла резервувати стрибок частоти, тим самим гарантуючи передачу даних без колізій навіть за наявності прихованих терміналів.

2.2.3 Протоколи із механізмом планування

«У протоколах із механізмом планування для доступу до середовища, перед передаванням відбувається планування пакетів для забезпечення пріоритетів серед потоків. Протоколи даної категорії орієнтовані на вирішення проблеми ПВ: DPS, DWOP, DLPS» [11]

DPS (Distributed Priority Scheduling) – це технологія, яка додає тег пріоритету вузла заголовка лінійного пакета до пакетів підтвердження та даних. Контролюючи передані пакети, кожен вузол підтримує таблицю планування в існуючому 802.11. Таблиця планування є оцінкою його відносного пріоритету в управлінні доступом до середовища.

DWOP (Distributed Wireless Ordering Protocol) – Протокол розподіленого бездротового упорядкування складається зі схеми доступу до середовища та механізму планування. Він базується на запропонованій схемі розподіленого пріоритетного планування. DWOP гарантує, що пакети отримують доступ до середовища відповідно до порядку, визначеного ідеальним опорним планувальником, таким як FIFO (перший прийшов - перший вийшов), віртуальний годинник або найперший термін..

DLPS (Distributed Laxity-based Priority Scheduling) – Рішення щодо планування за схемою розподіленого планування пріоритетів на основі нестабільності (DLPS) приймаються на основі станів сусідніх вузлів та зворотного зв'язку від вузлів призначення щодо втрат пакетів. Пакети записуються на основі їх рівномірних бюджетів нестабільності (ULB) та коефіцієнтів доставки пакетів потоків. Нестабільність пакета – це час, що залишився до його кінцевого терміну.

2.2.4 Протоколи із управлінням маршрутизацією

«Протоколи, такі як: H-NAME, MPR-Tree, DPCF, Graph and Beacon використовують управління шляхом маршрутизації, та дозволяють вирішувати проблему ПВ.» [11]

H-NAME (Hybrid Node Activation Multiple Access) – це гібридний протокол керування доступом до середовища передавання, який поєднує детерміновані та стохастичні механізми доступу з динамічним керуванням активністю вузлів мережі. Основна ідея полягає у зменшенні енергоспоживання та кількості колізій шляхом переходу частини вузлів у сплячий режим та активації лише тих, які мають визначену пріоритетність, енергетичний потенціал або потребу в передачі даних. H-NAME може комбінувати підходи TDMA (через попереднє резервування часових слотів) і CSMA (через конкурентний доступ у неконтрольованих слотах), адаптуючи стратегію залежно від трафіку, топології та мережевих умов.

MPR-Tree (Multi-Packet Reception Tree) — це розподілений MAC-протокол, заснований на ієрархічному механізмі розділення вузлів (splitting tree), який розроблено для мереж із підтримкою багаторазового приймання пакетів (multi-packet reception, MPR). Протокол використовує ітеративну процедуру резервування, у якій вузли передають запити на доступ у заздалегідь визначені часові слоти відповідно до дерева розділення. На кожному етапі вузли, що зіткнулись у попередньому слоті, поділяються на підгрупи, і процес повторюється до досягнення колізійно-вільного передавання. Використання MPR дозволяє приймачу одночасно обробляти кілька передавань, що значно підвищує пропускну здатність у порівнянні з класичними MAC-протоколами на основі TDMA або CSMA.

DPCF (Distributed Point Coordination Function) – розширює роботу функції координації точок (PCF), визначеної в стандарті IEEE 802.11, для роботи в бездротових мережах без інфраструктури. У PCF центральний координатор точок опитує користувачів, щоб отримати доступ до каналу, і колізії даних повністю уникаються, що забезпечує високу продуктивність. Щоб поширити свою високу продуктивність на мережі без інфраструктури, у цій статті пропонується DPCF як комбінація функції розподіленої координації (DCF) та PCF. Загальна ідея полягає в поєднанні динамічного, тимчасового та спонтанного механізму кластеризації на основі DCF з виконанням PCF у кожному кластері.

2.2.5 Протоколи управління спрямованістю та потужністю антени

«Остання категорія описує протоколи із управлінням потужністю та спрямованістю антени. Серед протоколів із управлінням потужністю вирішує проблему ПНВ: PCM, а проблему ПВ: RBAR, ERBAR. Управління спрямованістю дає можливість вирішувати проблему ПНВ, до цієї категорії належать протоколи DBTMA/DA, MACA-D.» [11]

PCM (Power Control MAC) – Протокол керування потужністю дозволяє вибирати потужність передачі для кожного пакета. У PCM пакети RTS/CTS передаються з максимальним рівнем потужності Pmax. Але пакети даних передаються з нижчим рівнем потужності. Щоб уникнути потенційної колізії, спричиненої зменшенням зони зондування несучої, під час передачі пакетів DATA PCM періодично збільшує потужність передачі до Pmax. Пакети ACK передаються з мінімально необхідною потужністю для досягнення вузла джерела.

RBAR (Receiver-Based AutoRate) – Основна ідея RBAR полягає в тому, щоб дозволити приймачу вибрати відповідну швидкість для пакета даних під час обміну пакетами RTS/CTS. Переваги цього підходу включають: механізми оцінки якості каналу та вибору швидкості тепер знаходяться на приймачі. Це дозволяє механізму оцінки якості каналу безпосередньо отримувати доступ до всієї інформації, наданої йому приймальним обладнанням (наприклад, кількість компонентів багатопроменевості, коефіцієнт помилок символів, сила прийнятого сигналу тощо), для точнішого вибору швидкості.

ERBAR (Enhanced Receiver-Based AutoRate) – цей протокол покращує RBAR двома способами. По-перше, пропонується модифікований механізм віртуального зондування несучої для зменшення проблеми прихованого терміналу. По-друге, розроблено новий алгоритм адаптації швидкості для покращення пропускної здатності.

DBTMA/DA (Dual Busy Tone Multiple Access with Directional Antennas) – призваний адаптувати протокол DBTMA для використання зі спрямованими антенами, що ще більше збільшує ефективну пропускну здатність каналу. На відміну від інших протоколів MAC на основі спрямованих антен, наш протокол, який називається DBTMA/DA, здатний резервувати пропускну здатність каналу з більшою зернистістю, не покладаючись на додаткову підтримку локації. Проведено моделювання, щоб

продемонструвати кращу мережеву продуктивність DBTMA/DA порівняно з DBTMA та протоколами MAC IEEE 802.11a.

MACA-D (Multiple Access with Collision Avoidance – Directional) є варіацією базового протоколу MACA, адаптованою для використання з спрямованими антенами в бездротових ad hoc мережах. Його основна мета — покращити ефективність доступу до середовища передачі, зменшуючи колізії та підвищуючи пропускну здатність мережі.

2.3 Порівняльна характеристика методів

У межах дослідження було проведено порівняльний аналіз 25 MAC-протоколів, що використовуються в бездротових сенсорних мережах. Розгляд охоплював як класичні (TDMA, CSMA/CA), так і гібридні рішення, включаючи протоколи з механізмами енергозбереження, підтримкою MPR, пріоритетного доступу та спрямованих антен. Для кожного з протоколів проаналізовано ключові характеристики: тип доступу, метод ініціації передачі, спосіб уникнення колізій, підтримка QoS, енергоефективність та складність реалізації.

В перелік протоколів потрапили: FAMA, S-FAMA, RC-SFAMA, Le-WiMARK, DBTMA, RI-BTMA, MACA-BI, MARCH, NCAC, D-PRMA, CATA, FPRP, SRMA/PA, HRMA, DPS, DWOP, DLPS, H-NAME, MPR-Tree, DPCF, PCM, RBAR, ERBAR, DBTMA/DA, MACA-D.

Першим критерієм є тип доступу до середовища передачі, який відображає основний принцип організації зв'язку між вузлами мережі. Основними підходами є метод доступу з часовим поділом (TDMA), в якому час розділяється на фіксовані слоти, призначені окремим вузлам, а також конкурентний доступ з визначенням несучої та уникненням колізій (CSMA/CA), де вузли самостійно приймають рішення про передачу даних після перевірки доступності каналу. Окрему категорію складають гібридні

протоколи, які поєднують особливості обох підходів та адаптуються до змін умов мережі.

Наступною характеристикою є механізм ініціації передачі, який визначає, хто саме починає процедуру зв'язку: передавальний чи приймальний вузол. У першому випадку вузол, який має дані, ініціює передачу (як у класичних рішеннях, таких як MACA або FAMA), у другому - приймач, який надсилає сигнал готовності до прийому (наприклад, у протоколах з типом Ready-To-Receive). Деякі гібридні протоколи передбачають змінну ініціацію залежно від контексту.

Особлива увага приділяється методам уникнення колізій, які зменшують ймовірність одночасної передачі кількома вузлами. Серед найпоширеніших механізмів – обмін службовими повідомленнями (RTS/CTS), використання окремого каналу для передачі сигналу зайнятості, попереднє резервування часових слотів або використання систем пріоритетності.

Показник енергоефективності дозволяє оцінити здатність протоколу знижувати споживання енергії, що критично важливо для автономних сенсорних вузлів. Високий рівень енергозбереження досягається, зокрема, шляхом динамічного перемикання вузлів у пасивні стани, регулювання потужності передачі або обмеження активності за відсутності запитів.

Функція можливості множинного прийому (MPR) вказує на здатність протоколу ефективно використовувати фізичні можливості приймача для одночасної обробки кількох сигналів. Такий підхід може значно збільшити пропускну здатність мережі, але вимагає спеціалізованої апаратної підтримки.

Використання спрямованих антен є додатковим фактором, що впливає на ефективність протоколу MAC. Деякі рішення передбачають передачу у вузькоспрямованому режимі, що знижує рівень колізій, але вимагає складнішої процедури вирівнювання напрямків за наявності мобільності.

Складність реалізації – це комбінована характеристика, яка включає необхідність синхронізації, обсяг накладної інформації, необхідність централізованого або розподіленого управління та сумісність з апаратними обмеженнями мережевих пристроїв.

Останнім критерієм є підтримка якості обслуговування (QoS), яка забезпечує гарантії щодо затримок, пропускної здатності або пріоритетів. Це особливо важливо в системах реального часу, де потрібне розділення трафіку за рівнем критичності.

Таким чином, вищезазначені характеристики дозволяють провести глибокий функціональний аналіз MAC-протоколів та на основі порівняння визначити їх придатність для використання в різних типах бездротових сенсорних мереж. Повна порівняльна характеристика розглянутих протоколів наведена у додатку А.

2.4 Висновки з розділу 2

У другому розділі наведено огляд та класифікацію основних методів керування доступом до середовища в бездротових сенсорних мережах (БСМ). Проаналізовано особливості конкурентних, планувальних, резервувальних протоколів, а також протоколів, орієнтованих на маршрутизацію та управління потужністю антен. Встановлено, що конкурентні методи, зокрема, CSMA/CA, характеризуються простою реалізацією, але обмежені в ефективності в умовах високого навантаження та наявності прихованих вузлів. Методи з попереднім резервуванням часу або частоти забезпечують кращий детермінізм, але вимагають синхронізації та суворо реагують на зміни топології. Алгоритми планування демонструють високу ефективність у стабільних мережах, але їх важко реалізувати в умовах динамічної структури. Порівняльний аналіз протоколів показав, що жоден з підходів не є універсальним для всіх умов роботи БСМ.

3 ВИРІШЕННЯ ПРОБЛЕМИ ПРИХОВАНОЇ СТАНЦІЇ

3.1 Суть проблеми прихованої станції

Проблема прихованої станції виникає в безпроводових сенсорних мережах, коли вузли, що не перебувають в зоні де можуть чути один одного, одночасно передають данні до спільного приймача, тим самим спричиняє колізію. Яка призводить до втрати пакетів та зниження ефективності використання радіоканалу. Особливої актуальності набуває в мережах, де стоять жорсткі вимоги до енергоспоживання, через їх обмеження радіусу дії вузлів. Добре ця проблема описана в наступному фрагменті статті:

«У бездротових ad-hoc мережах, враховуючи обмежений спектр, змінні в часі характеристики поширення, розподілений контроль доступу і енергетичні обмеження, виникає багато проблем для можливості створення «ефективного» MAC протоколу та забезпечення надійного зв’язку із високою швидкістю передавання даних. Одними з основних виступають проблеми прихованих та незахищених вузлів (рис.3.1). Під проблемою прихованого вузла розуміється колізія через одночасне передавання вузлами, які мають між собою двоскачковий зв’язок, пакетів до їх спільного односкачкового сусіда. Проблема незахищеного вузла – нездатність вузла здійснювати передавання іншим вузлам через здійснення передавання своїм сусідом.» [11]

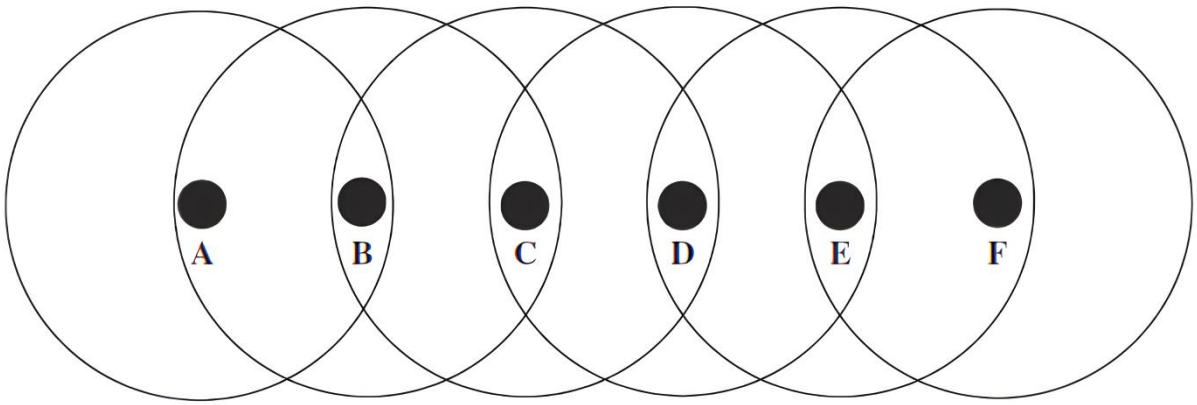


Рисунок 3.1 – Проблема прихованого терміналу[12]

3.2 Моделювання проблемної ситуації

Для ілюстрації проблеми прихованої станції в середовищі OMNeT++ було реалізовано спрощену модель бездротової сенсорної мережі. Модель створює топологію з кількома вузлами, що мають частково перекриваючі зони покриття, що відтворює умови, за яких можливі неузгоджені передачі та, відповідно, колізії. Візьмемо за основу таку задачу :

«Розглянемо топологію мережі на рис. 3.1 , де кола позначають зв'язок і діапазон завад кожного вузла, тобто, кожен вузол може почути безпосередніх сусідів зліва і справа. Припустимо, що RTS/ CTS не використовується.

(a) Вузол B в даний час передає вузлу A, а вузол C хоче передати вузлу D. Чи може вузол C здійснити передачу (тобто здійснити передачу не викликаючи колізій), чи зважиться він на це?

(b) Вузол C передає вузлу B, а вузол E хоче передати вузлу D. Чи дозволено вузлу E здійснити передачу і чи буде він її здійснювати?

(c) Вузол A передає вузлу B, а вузол D передає вузлу C. Яким іншим вузлам дозволено здійснити передачу у той же час?

(d) Вузол A передає вузлу B, а вузол E передає вузлу F. Яким іншим вузлам дозволено здійснити передачу у той же час?» [12]

3.2.1 Опис топології мережі

Структура мережі описана у файлі HiddenNetwork.ned. У ньому визначено вузли A, B, C, D, E, F, а також зв'язки між ними з урахуванням обмеженої зони видимості

```
package hiddennodesimulation;

import hiddennodesimulation.Node;

network HiddenNetwork
{
    submodules:
        A: Node {
```

```
            parameters:
                @display("p=100,100");
        }
        B: Node {
            parameters:
                @display("p=200,100");
        }
        C: Node {
            parameters:
                @display("p=300,100");
        }
        D: Node {
            parameters:
                @display("p=400,100");
        }
        E: Node {
            parameters:
                @display("p=500,100");
        }
        F: Node {
            parameters:
                @display("p=600,100");
        }
    connections allowunconnected:
        A.out++ --> B.in++;
        B.out++ --> A.in++;

        B.out++ --> C.in++;
        C.out++ --> B.in++;

        C.out++ --> D.in++;
        D.out++ --> C.in++;

        D.out++ --> E.in++;
        E.out++ --> D.in++;

        E.out++ --> F.in++;
        F.out++ --> E.in++;
}
```

3.2.2 Поведінка вузла

Логіка обробки подій у вузлі реалізована у файлах Node.h та Node.cc. Вузол може ініціювати передачу, відповідати на вхідні повідомлення та змінювати свій стан у відповідь на виявлення активності в середовищі:

Node.h – оголошення класу вузла, внутрішніх змінних та сигналів

```
#ifndef __HIDDENNODESIMULATION_NODE_H_
#define __HIDDENNODESIMULATION_NODE_H_

#include <omnetpp.h>
```

```
using namespace omnetpp;

class Node : public cSimpleModule
{
  private:
    bool channelBusy = false;
    bool busySignalSeen = false;
    bool hasCollision = false;

    cMessage *selfMsg = nullptr;
    cMessage *clearChannelMsg = nullptr;

  protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
};

#endif
```

Node.cc – реалізація поведінки: ініціалізація, передача даних, виявлення сигналів, реакція на повідомлення зайнятості/даних

```
#include <omnetpp.h>
#include "Node.h"

using namespace omnetpp;

Define_Module(Node);

void Node::initialize()
{
    selfMsg = new cMessage("selfMsg");
    clearChannelMsg = new cMessage("clearChannel");

    if (par("sendMessage").boolValue()) {
        scheduleAt(simTime() + uniform(0, 1), selfMsg);
    }
}

void Node::handleMessage(cMessage *msg)
{
    if (msg == selfMsg) {
        if (!channelBusy && !busySignalSeen) {
            EV << getName() << " is broadcasting busy signal.\n";

            int n = gateSize("out");
            for (int i = 0; i < n; ++i) {
                send(new cMessage("busy"), "out", i);
            }

            cMessage* dataEvent = new cMessage("sendData");
            scheduleAt(simTime() + 0.01, dataEvent);

            channelBusy = true;
            scheduleAt(simTime() + par("channelBusyTime"), clearChannelMsg);
        } else {
```

```
            EV << getName() << " senses the channel is busy or heard busy signal.
Will retry.\n";
            scheduleAt(simTime() + par("channelBusyTime") + uniform(0.1, 0.5),
selfMsg);
        }
    }

    else if (strcmp(msg->getName(), "sendData") == 0) {
        EV << getName() << " is broadcasting DATA.\n";

        int n = gateSize("out");
        for (int i = 0; i < n; ++i) {
            send(new cMessage("data"), "out", i);
        }

        delete msg;
    }

    else if (msg == clearChannelMsg) {
        channelBusy = false;
        hasCollision = false;
        EV << getName() << ": channel is now free.\n";
    }

    else if (strcmp(msg->getName(), "clearBusyInfo") == 0) {
        busySignalSeen = false;
        EV << getName() << ": busy info timeout expired.\n";
        delete msg;
    }

    else {
        const char* name = msg->getName();

        if (strcmp(name, "busy") == 0) {
            if (!busySignalSeen) {
                EV << getName() << " senses busy signal. Marking temporary busy.\n";
                busySignalSeen = true;
                scheduleAt(simTime() + par("channelBusyTime"), new
cMessage("clearBusyInfo"));
            } else {
                EV << getName() << " received busy while already in busySignalSeen
state.\n";
            }
            delete msg;
        }

        else {
            if (channelBusy) {
                hasCollision = true;
                EV << getName() << " received a " << name << " WHILE BUSY: COLLISION.
Discarding.\n";
            } else {
                EV << getName() << " received a " << name << "\n";
                channelBusy = true;
                scheduleAt(simTime() + par("channelBusyTime"), clearChannelMsg);
            }
            delete msg;
        }
    }
}
```

3.2.3 Налаштування параметрів та подій

Файл конфігурації omnetpp.ini визначає початкові умови моделювання, час подій, параметри середовища та призначення вузлів, які передаватимуть дані. Для кожного зі сценаріїв було розроблено окремий Config де буде відрізнятись параметр sendMessage в залежності від того які вузли відправляють повідомлення в даному сценарії :

```
[General]
network=hiddennodesimulation.HiddenNetwork
sim-time-limit=30s

[ConfigA]
description="(a) B sends to A, C wants to send to D but hears B - does not send"
*.A.sendMessage = false
*.B.sendMessage = true
*.C.sendMessage = true
*.D.sendMessage = false
*.E.sendMessage = false
*.F.sendMessage = false

*.*.channelBusyTime = 2

[ConfigB]
description="(b) C sends to B, E wants to send to D, does not hear C - causes
collision"
*.A.sendMessage = false
*.B.sendMessage = false
*.C.sendMessage = true
*.D.sendMessage = false
*.E.sendMessage = true
*.F.sendMessage = false

*.*.channelBusyTime = 2

[ConfigC]
description="(c) A sends to B, D sends to C. E to F allowed. F to E causes
collision."
*.A.sendMessage = true
*.B.sendMessage = false
*.C.sendMessage = false
*.D.sendMessage = true
*.E.sendMessage = false
*.F.sendMessage = false

*.*.channelBusyTime = 2


 [ConfigD]
description="(d) A sends to B, E sends to F. D to C allowed. C to D blocked."
*.A.sendMessage = true
*.B.sendMessage = false
*.C.sendMessage = false
```

```
*.D.sendMessage = false
*.E.sendMessage = true
*.F.sendMessage = false

*.*.channelBusyTime = 2
```

3.2.4 Результати моделювання

(a) Так, вузол C не спричинить зіткнення у вузлі A. Однак, оскільки вузол C може почути передачу вузла B, він не буде передавати.

(b) Передача вузла E не заважатиме передачі C до B, однак його власна передача до D не буде успішною, оскільки вона конфліктуватиме з передачею вузла C. Вузол E не знає про передачу вузла C і тому розпочне свою передачу.

(c) Вузлу E дозволено передавати до вузла F. Вузол F також може передавати до вузла E, але ця передача буде конфліктувати у вузлі E з передачею вузла D.

(d) Вузлу C заборонено передавати, оскільки його передача буде конфліктувати з передачею вузла A у вузлі B. З іншого боку, вузлу D дозволено передавати до вузла C.

3.3 Шляхи вирішення

Одним з класичних методів уникнення колізій у межах з фіксованою структурою є синхронізація передачі за часом «Множинний доступ з поділом за часом (TDMA протокол) дозволяє декільком пристроям використовувати ту ж смугу частот, але використовуючи при цьому періодичні часові вікна (кадри, frames), що складаються з фіксованої кількості інтервалів передачі для поділу доступу до середовища від різних пристроїв. Графік відображає, який вузол може передавати дані протягом певного інтервалу, тобто, одному інтервалу присвоюється не більше одного вузла. Основною перевагою TDMA протоколу є те, що вузли не змагаються за отримання доступу до середовища, тим самим уникаючи колізій. Недоліком TDMA протоколу є те,

що при необхідності внести зміни до топологічної схеми мережі, потрібно змінити розподіл інтервалів. Крім того, TDMA протоколи можуть бути неефективними в їх пропускній спроможності, коли інтервали мають фіксований розмір (а розмір пакетів може відрізнятися), а також коли інтервали, що виділені вузлу, не використовуються у кожній ітерації кадру.» [12]

У випадках з динамічною топологією доцільно використовувати адаптивні методи доступу до середовища,наприклад CSMA/CA «CSMA/CA (множинний доступ з контролем несучої і запобіганням колізій) протокол є різновидом CSMA протоколу, спрямованого на підвищення ефективності шляхом запобігання колізій. У CSMA/CA протоколі вузли зчитують середовище, але не отримують миттєвий доступ до каналу, коли він знаходиться в режимі очікування. Замість цього, вузол очікує період часу, який називають міжкадровим інтервалом DCF (DIFS), плюс випадкове значення відстрочки, яке є кратним розміру інтервалу). У разі, коли декілька 130 вузлів намагаються отримати доступ до середовища, переможе той, у якого буде найкоротший період відстрочки.»[12]

Ще одним дієвим методом вирішення проблеми прихованого вузла є використання механізму RTS/CTS (Запит на надсилання Дозволити надсилання). Його суть полягає у використанні керуючих повідомлень – RTS (запит на надсилання) та CTS (дозволити надсилання) – перед фактичною передачею даних. Коли передавач має намір передавати дані, він спочатку надсилає RTS приймачу. Якщо ефір вільний, приймач відповідає CTS, сигналізуючи всім іншим сусіднім вузлам, що канал буде зайнятий. Завдяки цьому вузли, які не чують відправника, але чують одержувача, зможуть утриматися від передачі. Такий підхід дозволяє значно зменшити ймовірність колізій у мережах з обмеженою видимістю між вузлами.

Також з цією проблемою може допомогти використання пріоритетів у плануванні передачі. Наприклад, вузли, які довше чекають на передачу, або вузли, що мають критично важливі дані, можуть отримати вищий пріоритет

під час розподілу доступу до ефіру. Такий підхід дозволяє зменшити ймовірність того, що вузли з високим навантаженням будуть постійно витіснятися іншими активними учасниками мережі. У моделі це можна реалізувати, зберігаючи позначку часу останньої передачі та динамічно налаштовуючи пріоритет у логіці планування.

Одним з шляхів рішення може бути механізм повторної передачі сигналу зайнятості одержувачем, що дозволяє уникнути колізій у випадках, коли приховані вузли не чують передавач, але мають намір передати одержувачу. Приймач, після початку прийому або виявлення зайнятості каналу, самостійно поширює сигнал зайнятості в навколишнє середовище. Це дозволяє вузлам, які можуть бачити лише приймач, дізнатися про активність на каналі, покращуючи узгодженість дій у мережах без централізованого контролю поширення сигналу.

Таблиця – 3.1 Порівняння методів вирішення проблеми прихованого вузла

Метод уникнення колізій	Переваги	Недоліки	Сценарії застосування
TDMA	Уникнення колізій за рахунок розкладу	Складна синхронізація	Реального часу мережі з фіксованими пристроями
CSMA/CA	Адаптація до навантаження мережі	Можливість колізій у високому навантаженні	Wi-Fi, мобільні мережі з динамічним трафіком
RTS/CTS	Зменшення ймовірності колізій	Затримки через обмін службовими повідомленнями	Багатокористувацьке середовище з перешкодами
Пріоритетний доступ до каналу	Критичні дані передаються першими	Можливе голодування менш пріоритетних вузлів	Індустріальні IoT-системи
Ретрансляція busy-сигналу	Покращення обізнаності вузлів про стан мережі	Затримки через каскадну ретрансляцію	Мережі з прихованими вузлами або обмеженим оглядом

3.4 Моделювання після впровадження RTS/CTS

Вибір механізму RTS/CTS як методу запобігання колізіям у бездротових сенсорних мережах зумовлений його здатністю ефективно вирішувати проблему досягнутої станції, що є однією з ключових перешкод для надійної передачі даних у децентралізованому середовищі. На відміну від простих методів прослуховування каналів (таких як CSMA), RTS/CTS забезпечує двостороннє узгодження передачі між відправником і приймачем перед фактичним відправленням основного пакета даних. Це дозволяє сусідньому вузлу отримувати інформацію про плановану передачу, навіть якщо він не може безпосередньо чути відправника, та утримуватися від створення перешкод. Таким чином, RTS/CTS мінімізує ймовірність колізій, особливо в умовах часткового перекриття зон покриття, що робить його ефективним та розумним вибором для моделювання протоколів доступу в багатовузлових бездротових сенсорних мережах.

Запропонований фрагмент коду, реалізований у `Node.cc`, описує логіку роботи вузла бездротової мережі, що моделює механізм передачі повідомлень з урахуванням зайнятості каналу. На етапі ініціалізації вузол, залежно від параметра `sendMessage`, планує початкову передачу повідомлення. Якщо канал вільний і вузол не чує сигналу зайнято, він надсилає повідомлення про зайнятість (busy) на всі виходи та через короткий проміжок часу ініціює передачу даних. Якщо вузол чує сигнал зайнято або сам є передавачем, він відкладає власну передачу на випадкову затримку. Також реалізовано механізм очищення статусу зайнятості через певний час (`clearChannelMsg`) та виявлення колізій: якщо вузол отримує дані під час власної передачі (`channelBusy`), така ситуація інтерпретується як колізія, і повідомлення ігнорується. Таким чином, код моделює базовий протокол доступу до середовища з уникненням колізій шляхом локального моніторингу каналу.

```
#include "RTSCTSNode.h"

Define_Module(RTSCTSNode);

void RTSCTSNode::initialize()
{
    selfMsg = new cMessage("startRTS");
    sendDataMsg = new cMessage("sendDATA");
    rtsTimeoutMsg = new cMessage("rtsTimeout");
    clearChannelMsg = new cMessage("clearChannel");

    targetName = par("target").stringValue();

    if (par("sendMessage").boolValue()) {
        scheduleAt(simTime() + uniform(0, 1), selfMsg);
    }
}

void RTSCTSNode::handleMessage(cMessage *msg)
{
    if (msg == selfMsg) {
        if (!channelBusy) {
            sendRTS();
            waitingForCTS = true;
            receivedCTS = false;
            scheduleAt(simTime() + par("rtsTimeout").doubleValue(), rtsTimeoutMsg);
        } else {
            EV << getName() << ": Channel busy, deferring RTS.\n";
            scheduleAt(simTime() + par("channelBusyTime").doubleValue() +
uniform(0.1, 0.3), selfMsg);
        }
    }

    else if (msg == rtsTimeoutMsg) {
        if (!receivedCTS) {
            EV << getName() << ": CTS timeout. Retrying RTS.\n";
            waitingForCTS = false;
            scheduleAt(simTime() + uniform(0.2, 0.6), selfMsg);
        }
    }

    else if (msg == sendDataMsg) {
        sendDATA();
    }

    else if (msg == clearChannelMsg) {
        channelBusy = false;
        receiving = false;
        hasCollision = false;
        EV << getName() << ": Channel cleared.\n";
    }

    else {
        const char* name = msg->getName();

        if (strcmp(name, "RTS") == 0) {
            const char* recv = msg->par("receiver").stringValue();
            if (strcmp(recv, getName()) == 0) {
                if (!channelBusy) {
                    EV << getName() << " received RTS addressed to me. Sending
CTS.\n";
```

```
                    sendCTS();
                } else {
                    EV << getName() << " received RTS addressed to me, but channel is
busy. Ignoring.\n";
                }
            } else {
                EV << getName() << " overheard RTS not for me. Marking channel busy
temporarily.\n";
                channelBusy = true;
                cancelEvent(clearChannelMsg);
                scheduleAt(simTime() + par("channelBusyTime").doubleValue(),
clearChannelMsg);
            }
            delete msg;
        }

        else if (strcmp(name, "CTS") == 0) {
            if (waitingForCTS && !receivedCTS) {
                EV << getName() << " received CTS. Preparing to send DATA.\n";
                receivedCTS = true;
                waitingForCTS = false;
                scheduleAt(simTime() + 0.01, sendDataMsg);
            }
            delete msg;
        }

        else if (strcmp(name, "DATA") == 0) {
            if (receiving) {
                hasCollision = true;
                EV << getName() << ": COLLISION detected! Discarding DATA.\n";
            } else {
                receiving = true;
                EV << getName() << " received DATA.\n";
                channelBusy = true;
                cancelEvent(clearChannelMsg);
                scheduleAt(simTime() + par("channelBusyTime").doubleValue(),
clearChannelMsg);
            }
            delete msg;
        }

        else {
            EV << getName() << ": Unknown message: " << name << "\n";
            delete msg;
        }
    }
}

void RTSCTSNode::sendRTS()
{
    EV << getName() << ": Sending RTS to " << targetName << "\n";

    cMessage *rts = new cMessage("RTS");
    rts->addPar("receiver") = targetName;

    int n = gateSize("out");
    for (int i = 0; i < n; ++i)
        send(rts->dup(), "out", i);

    delete rts;
}
```

```
void RTSCTSNode::sendCTS()
{
    EV << getName() << ": Sending CTS.\n";

    channelBusy = true;
    cancelEvent(clearChannelMsg);
    scheduleAt(simTime() + par("channelBusyTime").doubleValue(), clearChannelMsg);

    int n = gateSize("out");
    for (int i = 0; i < n; ++i)
        send(new cMessage("CTS"), "out", i);
}

void RTSCTSNode::sendDATA()
{
    EV << getName() << ": Sending DATA.\n";

    int n = gateSize("out");
    for (int i = 0; i < n; ++i)
        send(new cMessage("DATA"), "out", i);

    channelBusy = true;
    cancelEvent(clearChannelMsg);
    scheduleAt(simTime() + par("channelBusyTime").doubleValue(), clearChannelMsg);
}
```

omnetpp.ini

```
[General]
network = rtsctsproject.RTSCTSNetwork

sim-time-limit = 30s

########################################
[ConfigRTSCTS_A]
description = "RTS/CTS: (a) B sends to A, C wants to send to D but hears B - does not
send"
*.A.sendMessage = false
*.B.sendMessage = true
*.B.target = "A"
*.C.sendMessage = true
*.C.target = "D"
*.D.sendMessage = false
*.E.sendMessage = false
*.F.sendMessage = false

*.*.channelBusyTime = 2
*.*.rtsTimeout = 1
########################################
[ConfigRTSCTS_B]
description = "RTS/CTS: (b) C sends to B, E wants to send to D, does not hear C -
causes collision"
*.A.sendMessage = false
*.B.sendMessage = false
*.C.sendMessage = true
*.C.target = "B"
*.D.sendMessage = false
```

```
*.E.sendMessage = true
*.E.target = "D"
*.F.sendMessage = false

*.*.channelBusyTime = 2
*.*.rtsTimeout = 1
########################################
[ConfigRTSCTS_C]
description = "RTS/CTS: (c) A sends to B, D sends to C. E to F allowed. F to E causes
collision."
*.A.sendMessage = true
*.A.target = "B"
*.B.sendMessage = false
*.C.sendMessage = false
*.D.sendMessage = true
*.D.target = "C"
*.E.sendMessage = false
*.F.sendMessage = false

*.*.channelBusyTime = 2
*.*.rtsTimeout = 1
########################################
[ConfigRTSCTS_D]
description = "RTS/CTS: (d) A sends to B, E sends to F. D to C allowed. C to D
blocked."
*.A.sendMessage = true
*.A.target = "B"
*.B.sendMessage = false
*.C.sendMessage = false
*.D.sendMessage = false
*.E.sendMessage = true
*.E.target = "F"
*.F.sendMessage = false

*.*.channelBusyTime = 2
*.*.rtsTimeout = 1
```

3.5 Висновки з розділу 3

Під час моделювання, проведеного в середовищі OMNeT++ 6.0.1 на основі реалізованого коду в Node.cc, було успішно відтворено поведінку бездротової мережі з базовим механізмом запобігання колізіям. Вузли надсилали повідомлення відповідно до топології та параметрів, зазначених у omnetpp.ini. Висновок після впровадження RTS/CTS вдалося повністю уникнути колізій. Це повністю вирішило проблему прихованої станції і як рішення цієї проблеми показало себе чудово проте не кращим чином вливає енергоспоживання вузлів через значне збільшення повідомлень.

ВИСНОВКИ

За результатами виконання дипломної роботи було здійснено комплексне дослідження особливостей побудови БСМ та методів управління доступом до середовища. На основі аналізу функціональних характеристик БСМ виявлено ключові обмеження, які зумовлюють використання спеціалізованих протоколів управління доступом. До таких обмежень віднесено енергетичну залежність вузлів, обмеження обчислювальних ресурсів, випуск фіксованої інфраструктури та потреби в самоорганізації.

Було систематизовано класифікацію MAC-протоколів, які застосовуються в БСМ, та проведено порівняльний аналіз їх ефективності. Розглянуто переваги та недоліки конкурентних, планових, резервних протоколів, а також методів із керуванням маршрутизацією. Показано, що один із існуючих протоколів не є універсальним, і вибір конкретного рішення має обґрунтовуватися на врахуванні топології мережі, енергетичних умов та вимог до надійності передачі.

Особливу увагу було виділено проблеми досягнутої станції — одну з найбільш критичних для багатьох сценаріїв у БСМ. На основі розробленої моделі в середовищі OMNeT++ змодельована конфліктна ситуація, яка викликала шкоду до колізій, та виведену поведінку вузлів у разі наявності RTS/CTS-механізмів. У рамках роботи пропонується реалізація механізму ретрансляції сигналу зайнятості з боку отримувача, що дозволяє розширити інформованість отриманих вузлів про стан каналу. Це рішення продемонструвало свою ефективність у змодельованій мережі та є перспективним для використання в децентралізованих конфігураціях.

Таким чином, можна зробити висновок про доцільність підключення класичних методів доступу з адаптивними механізмами відкритої службової інформації про канал зайнятості, що забезпечує підвищення стійкості та надійності функціонування БСМ в умовах частих колізій та прихованих вузлів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D. A. Moltchanov. MAC protocols// TUT, 2011
2. J. P. Sheu. MAC Protocols for Ad Hoc Wireless Networks// 2014
3. Kumar, Srikanta, and David Shepherd. "SensIT: Sensor information technology for the warfighter." Proc. 4th Int. Conf. on Information Fusion. 2001.
4. L. Boroumand, R. H. Khokhar, L. A. Bakhtiar. A Review of Techniques to Resolve the Hidden Node Problem in Wireless Networks// Smart Computing Review, vol. 2, no. 2, April 2012.
5. MAC Protocols for Ad Hoc and Sensor Networks// Computer and Communication Systems, [WSN] Winter 2011/2012
6. OSI Reference Model [Електронний ресурс]. – Режим доступу: https://www.rhyshaden.com/osi.htm.
7. Pottie G. J., Kaiser W. J. Wireless Integrated Network Sensors. Commun. ACM. 2000. Vol. 43, No. 5. P. 51–58
8. R. Jurdak, C. V. Lopes. A survey, classification and comparative analysis of medium access control protocols for ad hoc networks// IEEE Communications, 2004, volume 6, no. 1.
9. Shen C. Low Power Systems for Wireless Microsensors. ACM Trans. Embedded Comput. Syst. 2001. Vol. 1, No. 1. P. 1–19.
10. Дорош, Віталій. "Види атак на безпровідні сенсорні мережі." *Збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій “* (2010): 85-85.
11. Максимов, Володимир Васильович, and Олександр Олександрович Литвин. "КЛАСИФІКАЦІЯ ПРОТОКОЛІВ MAC РІВНЯ ДЛЯ AD-HOC МЕРЕЖ." *Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ»* (2016).

12. Основи побудови безпроводових сенсорних мереж [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Інженерія та програмування інфокомунікацій» спец. 172 Електронні комунікації та радіотехніка / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Кравчук та ін. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2024. – 313 с.

ДОДАТКИ

ДОДАТОК А

.

Підтримка QoS	Складність реалізації	Використання спрямованих антен	Підтримка MPR	Підтримка енергозбереження	Механізм уникнення колізій	Ініціація передачі	Тип доступу	Протокол
Ні	Середня	Ні	Ні	Низька	RTS/CTS	Від передавача	CSMA/CA	FAMA
Ні	Середня	Ні	Ні	Середня	RTS/CTS у слотах	Від передавача	CSMA/CA + TDMA	S-FAMA
Ні	Висока	Ні	Ні	Середня	RTS-конкуренція	Від передавача	CSMA/CA + TDMA	RC-SFAMA
Так	Висока	Ні	Ні	Висока	Busy tone + таблиці	Від передавача	Гібридний	Le-WiMARK
Ні	Середня	Ні	Ні	Середня	Dual Busy Tone	Від передавача	CSMA/CA	DBTMA
Ні	Середня	Ні	Ні	Середня	Busy Tone	Від приймача	CSMA/CA	RI-BTMA
Ні	Низька	Ні	Ні	Середня	RTR (замість RTS/CTS)	Від приймача	CSMA/CA	MACA-BI
Ні	Середня	Ні	Ні	Середня	RTR	Від приймача	CSMA/CA	MARCH
Так	Висока	Ні	Ні	Середня	Кодування + кооперація	Від приймача	Гібридний	NCAC
Ні	Середня	Ні	Ні	Середня	Busy tone + резервування	Від передавача	TDMA	D-PRMA
Так	Висока	Ні	Ні	Середня	CMS + DMS мініслоти	Від передавача	TDMA	CATA
Ні	Середня	Ні	Ні	Середня	5-фазне резервування	Від передавача	TDMA	FPRP
Так	Висока	Ні	Ні	Середня	RTS/CTS + пріоритет	Від передавача	Гібридний	SRMA/PA
Ні	Висока	Ні	Ні	Середня	Резервування хопів	Від передавача	TDMA (FHSS)	HRMA
Так	Середня	Ні	Ні	Низька	Пріоритетна вставка	Від передавача	CSMA/CA	DPS
Так	Середня	Ні	Ні	Середня	FIFO черга + контроль	Від передавача	CSMA/CA	DWOP
Так	Середня	Ні	Ні	Висока	Laxity-based	Від передавача	CSMA/CA	DLPS
Можливо	Висока	Ні	Ні	Висока	TDMA/CSMA + активація	Гібридна	Гібридний	H-NAME
Ні	Висока	Ні	Так	Середня	Splitting tree	Від передавача	TDMA	MPR-Tree
Так	Висока	Ні	Ні	Середня	Опитування + кластер	Від координатора	Гібридний	DPCF
Ні	Середня	Ні	Ні	Висока	RTS/CTS + контроль	Від передавача	CSMA/CA	PCM
Ні	Середня	Ні	Ні	Низька	Rate-aware CTS	Від приймача	CSMA/CA	RBAR
Ні	Середня	Ні	Ні	Низька	Покращений RBAR	Від приймача	CSMA/CA	ERBAR
Ні	Висока	Так	Ні	Середня	Busy tone + напрямки	Від передавача	CSMA/CA	DBTMA/DA
Ні	Середня	Так	Ні	Середня	RTS/CTS з напрямками	Від передавача	CSMA/CA	MACA-D