МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Дослідження математичних методів оцінки надійності бездротової сенсорної мережі

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 122 – "Комп'ютерні науки та інформаційні технології" (освітня програма – "Інформаційні технології проектування")

Науковий керівник роботи:	_____ (підпис)	О.І. Рязанцев (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	Я.О. Кудрявцева (ініціали, прізвище)
Група:		ІТП-16дм

Сєвєродонецьк 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 122 – "Комп'ютерні науки та інформаційні технології"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____20____р.

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Кудрявцевій Ярославі Олексіївні
(прізвище, ім'я,по батькові)

1. Тема роботи Дослідження математичних методів оцінки надійності бездротової сенсорної мережі
керівник проекту (роботи) Рязанцев О.І.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " 18 " 10 2017 року № 207/48
2. Строк подання студентом проекту (роботи) 12.01.2018
3. Вихідні дані до проекту (роботи) матеріали науково-дослідницької практики
4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Опис загальних відомостей про бездротові сенсорні мережі та постановка задачі. Вибір стандарту БСМ. Аналіз особливостей сенсорних мереж. Огляд існуючих засобів моделювання БСМ. Аналіз працездатності БСМ. Охорона праці. Висновки.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслеників)
електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Критська Яна Олександрівна		

7. Дата видачі завдання 18.10.2017

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Аналіз стану питання у науковій літературі. Визначення вимог до роботи.	18.10.2017 – 15.11.2017	
2	Виявлення особливостей імітаційного моделювання БСМ та вибір стандарту моделюваня	16.11.2017 – 25.11.2017	
3	Виявлення особливостей сенсорних мереж.	26.11.2017 – 28.11.2017	
4	Огляд засобів моделювання БСМ та вибір системи моделювання.	29.11.2017 – 10.12.2017	
5	Аналіз працездатності БСМ.	11.12.2017 – 20.12.2017	
6	Розробка заходів з охорони праці.	21.12.2017 – 27.12.2017	
7	Оформлення пояснювальної записки і графічного матеріалу.	28.12.2017 – 05.01.2018	
8	Підготовка та подання магістерської роботи до захисту	06.01.2018 – 12.01.2018	

Студент _____ Кудрявцева Я.О.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Рязанцев О.І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кудрявцева Я.О. Дослідження математичних методів оцінки надійності бездротової сенсорної мережі.

Метою дипломної роботи є вивчення математичних методів оцінки надійності бездротової сенсорної мережі (WSN) та програмних продуктів для моделювання WSN з метою вибору системи, яка найбіьше підходить для оцінки продуктивності системи WSN та оцінки, за її допомогою, потужністі перешкод і передачі радіосигналу для роботи WSN; дослідження надійності та завадостійкості збору та передачі інформації мережею в обраній системі; побудова моделі надійності для передачі пакета даних між двома вузлами у вибраній системі.

Робота полягає в вивченні архітектури мереж бездротових датчиків, вивченні можливих застосувань мереж датчиків, порівнянні алгоритмів маршрутизації в WSN, стандартного вибору, вивченні топологій, потужності розрахунку та часу експлуатації програмним продуктом моделювання WSN.

Ключові слова: ZIGBEE, бездротові сенсорні мережі, використання електроенергії, топологія

АНОТАЦИЯ

Кудрявцева Я.А. Исследование математических методов оценки надежности беспроводной сенсорной сети.

Целью дипломной работы является изучение математических методов оценки надежности беспроводной сенсорной сети (WSN) и программных продуктов для моделирования WSN с целью выбора системы наиболее подходящей для оценки производительности системы WSN и оценки, с ее помощью, мощности помех и передачи радиосигнала для работы WSN; исследования надежности и помехоустойчивости сбора и передачи информации сетью в выбранной системе; построение модели надежности для передачи пакета данных между двумя узлами в выбранной системе.

Работа заключается в изучении архитектуры сетей беспроводных датчиков, изучении возможных применений сетей датчиков, сравнимые алгоритмов маршрутизации в WSN, стандартного выбора, изучении топологий, мощности расчета и времени эксплуатации программным продуктом моделирования WSN.

Ключевые слова: ZIGBEE, беспроводные сенсорные сети, использование электроэнергии, топология

ABSTRACT

The aim of the thesis work is the study of mathematical methods for evaluating the reliability of a wireless sensor network (WSN) and software products for simulating the WSN with the aim of selecting the system most suitable for assessing the performance of the WSN system and evaluating, with its help, the interference and transmission power of the radio signal for the WSN 's operability; investigation of reliability and noise immunity of the collection and transmission of information by the network in the selected system; the construction of a reliability model for transferring a data packet between two nodes in the selected system.

The work is to study the architecture of wireless sensor networks, the study of the possible applications of sensor networks, comparison of routing algorithms in WSN, the standard choice, the study of topologies, the calculation power and operation time by WSN simulation software product.

Keywords: ZIGBEE, wireless sensor network, power consumption, topology

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ZigBee − специфікація мережевих протоколоів верхнього рівня

БСМ – бездротові сенсорні мережі

MAC − Media Access Control. Підрівень канального (другого) рівня моделі OSI, відповідно до стандартів IEEE 802. MAC є одним з розширень моделі OSI

ZCL − ZigBee Cluster Library. Бібліотека ZigBee-кластерів

TCP/IP − набір мережевих протоколів передачі даниxx

FFD − Fully Function Device. Мережевий координатор

OSI − Open Systems Interconnection. Взаємодія відкритих систем

ПЗ − программное забеспечення

ВСТУП

Ім'я бренду (ZigBee) походить від поведінки медових бджіл, так званого «танцю бджіл» - термін, що використовується в бджільництві і етології, яким позначається один із способів комунікації бджіл. Виконуючи цей «танець», бджоли, що виявили нектар, повідомляють іншим членам вулика інформацію про направлення розташування джерела живлення, відстані до нього і кількості пилку і нектару в ньому.

У даній роботі розглядаються стандарти бездротових сенсорних мереж і вивчається стандарт, розроблений інститутом інженерів з електротехніки та електроніки ZigBee для низькошвидкісних мереж 802.15.4. Розглядаються математичні методи оцінки надійності БСМ і програмні продукти для імітаційного моделювання БСМ, проводиться їх аналіз з метою вибору найбільш підходящої системи для оцінки працездатності БСМ, з її допомогою оцінюється вплив перешкод і потужності передачі радіосигналу на працездатність БСМ.

Робота є актуальною, так як в даний час вартість компонентів сенсорних мереж досить велика, щоб мати можливість побудувати мережу значних розмірів для наукових досліджень. І в цьому випадку актуальним є завдання імітаційного моделювання окремих подій і станів цих мереж.

Людство вже більше століття користується електроприладами освітлення і побутовою технікою. З кожним днем їх кількість в наших будинках збільшується і одночасно з цим виникає проблема ефективного управління ними. У зв'язку з цим було розроблено кілька систем «розумного будинку», які взяли на себе відповідальність за управління та енергозбереження, при цьому створюючи максимально комфортні умови для проживання людини. Одним з таких є розумний будинок Wulian, розроблений на основі технології Zigbee – найпрогресивніша пропозиція сучасності.

Зазвичай БСС застосовується для збору даних з пристроїв, оснащених сенсорами: датчиком температури, вологості, освітлення, тобто моніторингу. Дана технологія на протоколі IEEE 802.15.4, являючи собою стандарт безпровідного зв'язку, створює особливу мережу ZigBee, яка відрізняється від Wi-Fi і Bluetooth тим, що може самоорганізовуватися і самовідновлюватися за рахунок використання мініатюрних і мікропотужних пристроїв-радіопередавачів з вбудованим програмним забезпеченням. ПЗ дозволяє приладам, що працюють на основі протоколу ZigBee, знаходити один одного, прокладаючи оптимальні маршрути з метою передачі певних повідомлень.

У разі відключення або виходу з ладу одного з них автоматично прокладається новий маршрут. Крім того, для мережі ZigBee практично не існує перепон і відстаней, так як повідомлення від приладу управління передаються не на конкретний пристрій або датчик, а на найближчий, звідки по ланцюжку здійснюється подальша трансляція до потрібного об'єкту. Бездротова мережа Zigbee складається з чотирьох типів вузлів:

— координатора;

— роутера;

— сплячого пристрою;

— мобільних приладів.

Сплячі і мобільні пристрої використовують режими зниженого енергоспоживання, так як є вузлами з автономним джерелом живлення (акумулятор або батарейка). Як правило, ці пристрої є різними датчиками або контролерами виконавчих пристроїв. Координатори являють собою головні прилади, вони формують бездротові мережі і одночасно є довірчим центром, в якому встановлюється певна політика безпеки і задаються настройки Zigbee пристрої до мережі.

Так само мініатюрні сенсори можуть бути використані в медицині для спостереження за пацієнтами. Пристрої, які пацієнт носить із собою, можуть контролювати роботу життєво важливих органів і в разі якихось небезпечних ситуацій повідомляти лікаря. Невеликі розміри пристроїв дозволяють проводити не тільки «поверхневі» спостереження за пацієнтом, а й досліджувати внутрішні органи людини. Так при проведенні гастроскопії в державних лікарнях, поліклініках застосовують спеціальні апарат з гастроскопіческом трубкою, але не всі пацієнти можуть її проковтнути. На ринку вже існують пристрої у вигляді таблеток для проведення таких досліджень. Ці пристрої на батарейках мають запас енергії, достатній для того, щоб безперервно працювати протягом 24 годин і відправляти свідчення іншого пристрою, яке пацієнт носить із собою протягом цього часу. Після цього лікар може аналізувати отримані результати і поставити точний діагноз. Сенсори можуть використовуватися для автоматичного вмикання освітлення, коли людина входить в кімнату, використовуватися для управління якихось пристроїв (в системі «розумний дім»). Іноді потрібно стежити за рухливістю або руйнуванням будь-яких об'єктів, де важко прокласти кабелі. Для цього знову ж вигідніше застосувати сенсорні мережі, так як датчики мають автономне джерело живлення і вони бездротові. Також технологія бездротових сенсорних мереж може бути використана для передачі звукових даних - як домофонної системи, мультимедіа системи з низьким енергоспоживанням. У 2002 році був створений ZigBee Альянс, який представляє собою співтовариство компаній, які об'єдналися з метою розробки ефективних протоколів для бездротової мережі і забезпечення взаємодії між

різними пристроями різних виробників. Специфікація ZigBee доступна для широкої публіки за умов некомерційного використання. Вхідний рівень членства в альянсі ZigBee, званий Adopter, забезпечує доступ до ще не опублікованим специфікаціям і дозволяє створювати продукти для комерційного використання специфікації. Реєстрація в ході використання специфікації ZigBee вимагає від комерційного розробника приєднання до альянсу ZigBee. «Жодна частина цієї специфікації не може бути використана для виробництва продуктів або продажу без членства в альянсі ZigBee». Відбуваються щорічні конфлікти з приводу оплати загальної публічної ліцензією GNU. Згідно з пунктом правил, використання технологій ZigBee: «Ви повинні бути впевнені в тому, що будь-яка робота, яку ви публікуєте чи поширюєте, якщо вся ця робота або її частина містить програму або витягнута з програми або з будь-якої її частини, вся ця робота повинна бути ліцензована як ціле без передачі третім особам, згідно з умовами даної ліцензії ». З тих пір, як ліцензія GPL не робить різниці між комерційним і некомерційним використанням, неможливо виконати ліцензування стека ZigBee згідно GPL або поєднати виконання ZigBee з ліцензійним кодом GPL. Вимога до розробника приєднатися до альянсу ZigBee також вступає в конфлікт з іншими ліцензіями вільного програмного забезпечення.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ

У наш час бурхливо розвивається технологія бездротових сенсорних мереж. Бездротова сенсорна мережа - розподілена, що самоорганізується мережа безлічі датчиків (сенсорів) і виконавчих пристроїв, об'єднаних між собою за допомогою радіоканалу. Область покриття подібної мережі може становити від декількох метрів до декількох кілометрів за рахунок здатності ретрансляції повідомлень від одного елемента до іншого. Кожен елемент мережі має автономне джерело живлення, мікрокомп'ютер, приймач / передавач. Обмін даними між двома кінцевими пристроями може здійснюватися через ретранслятор, в тому випадку, якщо дальність роботи цих пристроїв не дозволяє їх взаємне виявлення. Таким чином, пристрої з малим радіусом дії за допомогою системи ретрансляторів можуть спілкуватися один з одним.

Одним з перших прообразів сенсорної мережі можна вважати систему СОСУС, призначену для виявлення та ідентифікації підводних човнів [8]. В середині 1990-х років технології бездротових сенсорних мереж стали активно розвиватися. На початку 2000-х років розвиток мікроелектроніки дозволило виробляти для таких пристроїв досить дешеву елементну базу. Бездротові мережі початку 2010-х років в основному базуються на стандарті ZigBee [6].

Багато галузей і сфер діяльності (промисловість, транспорт, комунальне господарство, охорона) зацікавлені у впровадженні сенсорних мереж, і число споживачів безперервно збільшується. Тенденція зумовлена ускладненням технологічних процесів, розвитком виробництва, розширюються потребами приватних осіб в сегментах безпеки, контролю ресурсів і використання товарно-матеріальних цінностей. З розвитком мікроелектронних технологій з'являються нові практичні завдання і теоретичні проблеми, пов'язані з застосуваннями сенсорних мереж в промисловості, житлово-комунальному комплексі, домашніх господарствах. Використання недорогих бездротових сенсорних пристроїв контролю параметрів відкриває нові області для застосування систем телеметрії і контролю, такі як:

— своєчасне виявлення можливих відмов виконавчих механізмів, з контролю таких параметрів, як вібрація, температура, тиск тощо .;

— контроль доступу до віддалених систем об'єкта моніторингу в режимі реального часу;

— забезпечення охорони музейних цінностей;

— забезпечення обліку експонатів;

— автоматична ревізія експонатів;

— автоматизація інспекції та технічного обслуговування промислових активів;

— управління комерційними активами;

— застосування як компонентів в енерго і ресурсозберігаючих технологіях;

— контроль екологічних параметрів навколишнього середовища.

Слід зазначити, що незважаючи на тривалу історію сенсорних мереж, концепція побудови сенсорної мережі остаточно не оформилася і не виразилася в певні програмно-апаратні (платформні) рішення. Реалізація сенсорних мереж на поточному етапі багато в чому залежить від конкретних вимог індустріальної задачі. Архітектура, програмно-апаратна реалізація знаходиться на етапі інтенсивного формування технології, що звертає увагу розробників з метою пошуку технологічної ніші майбутніх виробників.

1.1 Архітектура бездротових сенсорних мереж

БСМ, як було відзначено раніше, складаються з великої кількості розподілених по сенсорному полю сенсорних вузлів, а також інших елементів мережі.

Крім сенсорних вузлів в сенсорної мережі може бути присутнім ряд інших елементів, що виконують функції збору, перетворення, обробки, зберігання зібраних сенсорами даних, а також надання їх кінцевим споживачам. Типовий приклад БСМ, яка взаємодіє з мережею загального користування Інтернет, показаний на рисунку 1.1. Загальна прикордонне пристрій БСС може містити в собі ряд функціональних блоків, описаних нижче:

— Колектор даних. Серед цих блоків в першу чергу необхідно відзначити колектор даних (sink) - пристрій, призначений для збору даних від сенсорних вузлів. У загальному випадку вважається, що дані, одержувані сенсорами із зовнішнього середовища, повинні бути перед відправкою кінцевому споживачеві в числі іншого зібрані в одній або декількох точках, що і зумовлює необхідність наявності одного або декількох колекторів даних БСМ (рис. 1.1). З іншого боку, в рамках концепції ІВ можливий сценарій, в якому кінцевий споживач даних отримує інформацію безпосередньо від конкретного сенсорного вузла без участі колектора даних (рис. 1.2).

— Сполучення протоколів. Як вже було сказано вище, БСМ мають ряд особливостей, які вимагають нових підходів до розробки протоколів зв'язку. TCP / IP може бути використаний для організації БСМ далеко не завжди, в зв'язку з чим для сполучення БСМ з іншими мережами, що використовують протокол TCP / IP може бути необхідна наявність шлюзу, який здійснює перетворення протоколів передачі даних (рис. 1.1).

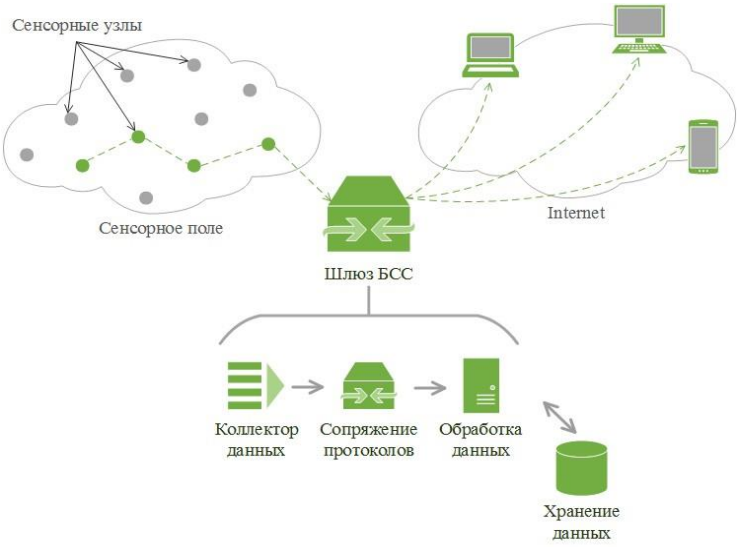


Рисунок 1.1 - Приклад БСМ і системи взаємодії БСМ з мережею загального користування

У той же час, якщо припустити, що до сенсорних вузлів якоїсь БСМ не пред'являється специфічних вимог, що стосуються вартості, розміру, енергоспоживання і відповідно, обчислювальних потужностей і пам'яті пристрою, то використання TCP / IP в таких БСМ виглядає цілком виправданим. В цьому випадку необхідності в високорівневої шлюзі БСМ немає, існує тільки необхідність перетворення протоколів фізичного рівня і рівня ланки даних (рис. 1.2).

Існує досить багато досліджень можливості використання протоколів TCP / IP для БСМ. Наприклад, в [7] наводиться кілька ідей, які можуть дозволити використовувати протоколи TCP / IP навіть в сенсорних вузлах, що не володіють значними обчислювальними потужностями і великим запасом електроенергії, зокрема, стиснення UPD-заголовків, вибір вузлом IP-адреси, виходячи з місця розташування вузла; маршрутизація на основі широкомовної розсилки UDP-пакетів і т.д. Також в [7] стверджується, що для реалізації необхідних протоколів в сенсорному вузлі досить мати всього декількох сотень байт пам'яті. В [8] автори наводять модифікацію протоколу TCP з розподіленим зберіганням пакета в вузлах, через які він проходить по шляху від джерела до одержувача, з метою зменшення шляху повторної пересилки пакета в разі, якщо пакет був скинутий. Така модифікація протоколу TCP робить його більш прийнятним для бездротових мереж, де ймовірність помилки в каналі вище, ніж в провідних мережах (для яких спочатку розроблявся протокол TCP), тому перевірка пакета за порядковим номером і контрольної суми тільки в кінцевому вузлі і повторна пересилання з вузла - джерело, а не з проміжних вузлів, може бути неоптимальною стратегією передачі.

Приклад автономної сенсорної мережі для домогосподарства, побудованої на базі протоколів IP і TCP, наведено в [9]. В [10] також наводиться приклад БСМ для виявлення вторгнень, що використовує дані протоколи.

Додатковим фактором, який може розширити межі застосування протоколів стека TCP / IP в БСМ є стійка тенденція до зменшення габаритів, вартості і енергоспоживання обчислювальних пристроїв при збільшенні їх обчислювальної потужності і обсягу пам'яті. Збереження цієї тенденції може в майбутньому дозволити реалізовувати на базі сенсорних вузлів протоколи, набагато більш складні, ніж це представляється можливим зараз.

Таким чином, всі перераховані вище дані свідчать про те, що тенденцією розвитку БСМ цілком ймовірно може стати відмова від використання специфічних протоколів для БСМ і перехід до максимального використання протоколів стека TCP / IP. У такому випадку необхідність в шлюзі БСМ, що перетворює протоколи від мережевого рівня і вище, фактично пропадає, і, відповідно, набуває актуальності сценарій сполучення БСМ з мережею Інтернет, наведений на рисунку 1.2.

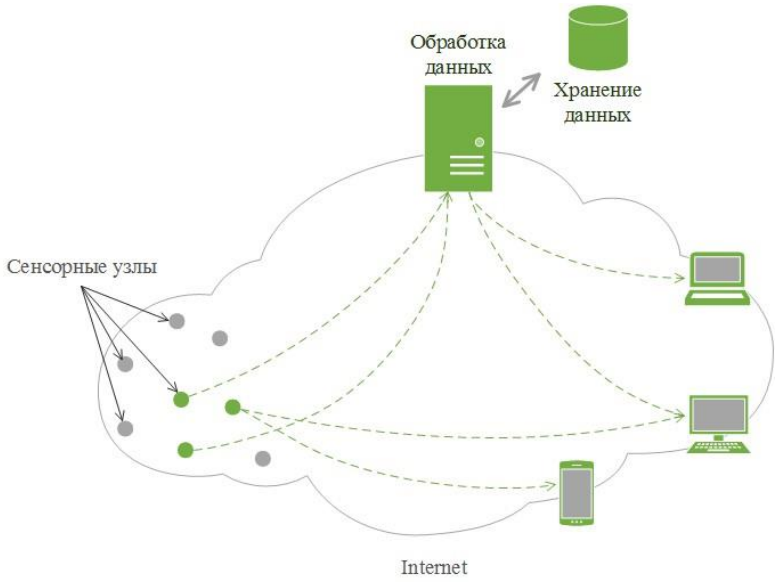


Рисунок 1.2 - Приклад БСМ, що є частиною мережі загального користування Інтернет (концепція IB)

Важливою функцією БСМ є також обробка даних, отриманих від сенсорних вузлів, і надання їх кінцевому споживачеві. Дані функції можуть виконуватися в тому ж пристрої, що реалізує функцію колектора даних і перетворення протоколів, так і бути винесена на окреме обладнання за межі БСМ. Крім того, в складі БСМ можуть перебувати пристрої, відповідальні за попереднє агрегування даних.

Агрегування даних в проміжних вузлах БСМ, яке також по суті є формою обробки даних, дозволяє вирішувати ряд проблем, пов'язаних з енергоспоживанням вузлів. Значна

частина електроенергії витрачатися сенсорним вузлом саме на передачу даних [11], а не на сам процес отримання даних з навколишнього середовища і їх обробку. У зв'язку з цим логічним шляхом зменшення енергоспоживання вузла бачиться зменшення обсягу переданих даних шляхом їх попередньої обробки в проміжних вузлах зв'язку. Крім того, було показано, що для БСМ, в яких дані від сенсорного вузла до шлюза або кінцевому споживачеві даних передаються за допомогою інших вузлів, характерний нерівномірний розподіл мережевого навантаження і, відповідно, енергетичних витрат вузлів, яке залежить від ступеня близькості сенсорного вузла до шлюза [12].

Само по собі агрегування даних в проміжних вузлах можливо через те, що при досить щільному розташуванні сенсорних вузлів на сенсорному полі дані від сусідніх вузлів часто будуть збігатися. Це дає можливості для об'єднання таких частково співпадаючих даних і, таким чином, зменшення обсягу переданої вузлом інформації [13]. За минулі роки було розроблено достатньо технологій і алгоритмів агрегування трафіку, з деякими з них можна познайомитися в [14].

1.2 Топологія БСМ

У бездротових мережах зв'язку існує два режими взаємодії вузлів: інфраструктурний (або керований) і ad hoc (або цільової) режими [1]. Для більш традиційних бездротових і дротових мереж зв'язку характерний інфраструктурний режим, де обмін інформацією між двома вузлами завжди відбувається за допомогою інфраструктурних елементів (точок доступу для бездротових мереж, комутаторів і маршрутизаторів - для дротових).

Даний режим роботи не підходить для більшості БСМ, так як режим і місцевість розгортання БСМ частіше за все не припускають наявності будь-якої інфраструктури. Так, БСМ можуть розташовуватися на важкодоступних територіях або територіях, де відсутні мережі передачі даних або електроживлення. У багатьох сценаріях розгортання БСМ передбачається, що вони будуть розміщені на місцевості мінімально трудомістким методом (наприклад, шляхом розкидання з борта літака або вертольота). Крім того, слід зазначити, що зазвичай розмір площі радіопокриття сенсорного вузла невеликий (це диктується міркуваннями економії електроенергії), тому при використанні інфраструктурного режиму, довелося б досить часто розташовувати інфраструктурні елементи мережі (точки доступу), що, з урахуванням вищеописаних особливостей БСМ, представляється можливим далеко не завжди.

З цих причин для побудови БСМ використовується ad hoc режим функціонування мережі, при якому сенсорні вузли зв'язуються один з одним безпосередньо, без участі точок

доступу. Цей підхід крім переваг більш простого розгортання мережі дає також можливість будувати, так звані, multihop або багатоінтервальні мережі [21]. У таких мережах дані між джерелом і одержувачем можуть передаватися не тільки безпосередньо, але і при необхідності через проміжні вузли (рис 1.3).

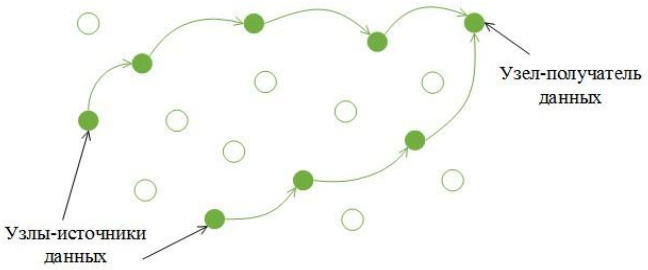


Рисунок 1.3 - Приклад многоінтервальной (multihop) цільової (ad hoc) мережі

Багатоінтервальний підхід до побудови мереж збільшує максимальну відстань між вузлами мережі і шлюзом або колектором даних, що дозволяє розташовувати колектори даних (або шлюзи) рідше і зменшувати розмір зони радіопокриття кожного вузла. Ці дві можливості в сукупності дозволяють знаходити оптимальну з точки зору енергоспоживання і часу життя вузлів стратегію побудови БСМ.

Часто подібну топологію БСМ називають комірковою (mesh) через те, що різні вузли, передаючи дані за допомогою один одного, утворюють пористу структуру (рис. 1.4).

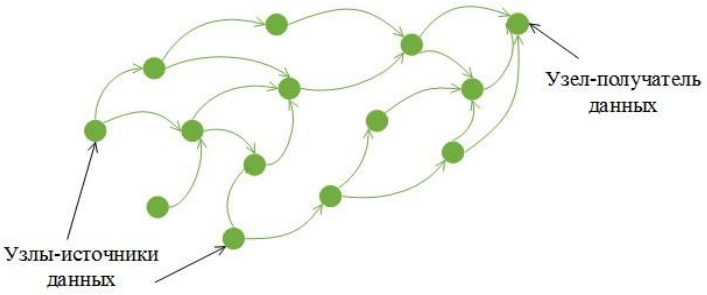


Рисунок 1.4 - Приклад коміркової топології

Безумовно, більш традиційні топології мереж, такі як зірка, шина, кільце, дерево (рис. 1.5), також мають право на застосування в БСМ.

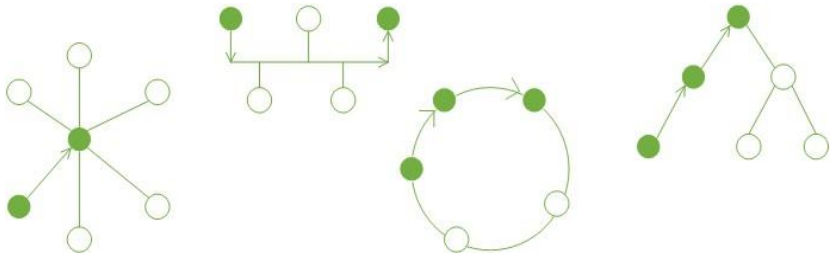


Рисунок 1.5 - Традиційні топології мереж, зліва направо: зірка, шина, кільце, дерево

Слід також зазначити, що багатоінтервальний ad hoc підхід до побудови мережі, на відміну від деяких більш традиційних підходів, дозволяє швидко і більш гнучко змінювати топологію мережі в разі відмови одного з вузлів, що позитивно позначається на тривалості ефективної роботи БСМ.

Багато сценаріїв роботи БСМ припускають, що досить велика кількість сенсорних вузлів буде покривати більшу за площею територію. В такому випадку, при використанні тільки одного шлюзу виникає ряд проблем.

По-перше, як вже було зазначено вище, чим ближче до шлюза знаходиться сенсорний вузол, тим більше транзитного трафіку він буде пропускати через себе, тим інтенсивніше буде витрачатися енергія його джерела електроживлення і тим швидше сенсорний вузол вийде з ладу. В цьому випадку може скластися досить парадоксальна ситуація, при якій віддалені від шлюзу сенсорні вузли все ще будуть функціонувати і збирати інформацію про навколишнє середовище, проте передати цю інформацію шлюзу не зможуть через те, що шлюз занадто далекий від них для прямої передачі, а всі можливі транзитні вузли вийшли з ладу, витративши свій запас електроенергії [21].

Крім того, наявність тільки одного шлюзу (або колектора даних) на велику кількість сенсорних вузлів підвищує вимоги до даного пристрою. Це стосується як необхідність використання автономного джерела електроживлення з більшою ємністю (або навіть підключення до мережі електроживлення), так і вимог до обчислювальних потужностей, так як обсяг оброблюваних шлюзом пакетів даних в загальному випадку прямо пропорційний числу вузлів БСМ. Недотримання цих високих вимог призводить до зменшення терміну ефективної роботи шлюзів (а значить і всієї БСМ), а також великих затримок при обробці інформації шлюзом.

Знайти компроміс в цій ситуації допомагає кластеризация БСМ - поділ її на кілька груп сенсорних вузлів або кластерів, кожен з яких має головний вузол, що виконує роль колектора даних для всіх вузлів кластера (рис. 1.6).

Головні вузли кластерів, як правило, передають інформацію на загальний шлюз БСМ (або кілька шлюзів). Тому за вимогами до електроживлення, обчислювальних потужностей

і надійності головні вузли кластерів повинні знаходитися між сенсорними вузлами і основними шлюзами БСМ [1]. У значної частини досліджень передбачається, що головний вузол кластера вибирається за тим чи іншим алгоритмом з числа рядових сенсорних вузлів БСМ [15], [16], [17] та ін.

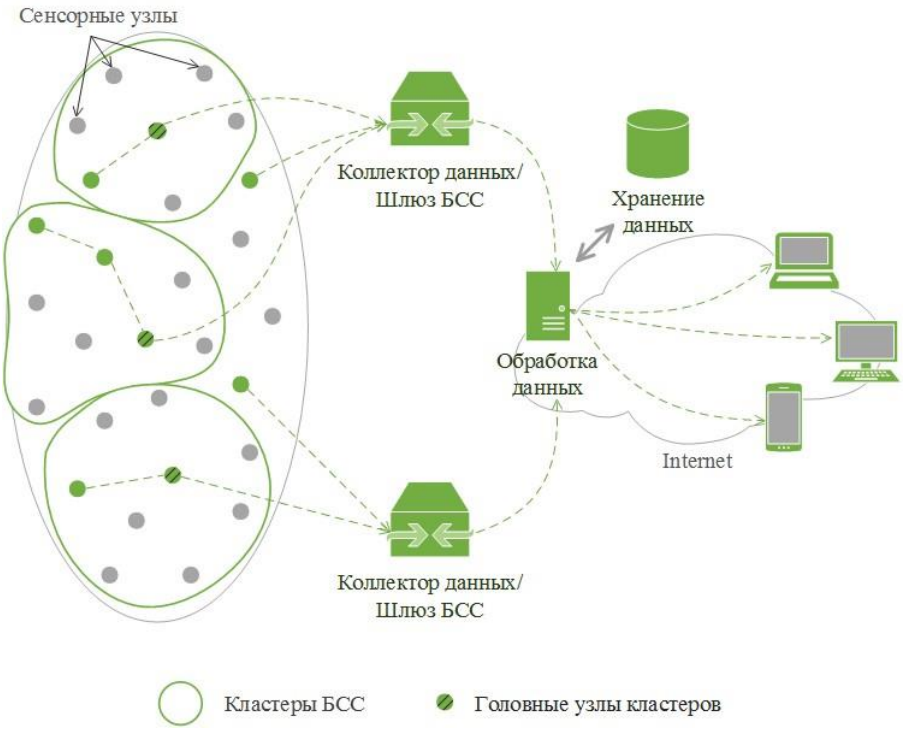


Рисунок 1.6 - Приклад кластеризації БСМ

Головні вузли кластерів можуть виконувати як власне сенсорну функцію, так і бути тільки колекторами даних і транзитними вузлами БСМ. Також частина вузлів БСМ може не належати ніякому кластеру, а відправляти дані безпосередньо на шлюз БСМ.

Як уже було зазначено вище, для багатьох додатків БСМ важливо, щоб розгортання мережі відбувалося максимально просто і з мінімальною участю людини (наприклад, шляхом розкидання сенсорних вузлів з борта літака або вертольота). У таких випадках можливості ручної конфігурації БСМ відсутні або вкрай обмежені, в зв'язку з чим актуальною стає можливість самоорганізації сенсорних вузлів в мережу.

Самоорганізація, відповідно до [18], є зміни, які повинен здійснити кожен з вузлів БСМ в своїй поведінці, для того, щоб взаємодіяти з сусідніми вузлами для виконання певного завдання або досягнення певної мети.

Нижче наведені деякі протоколи, службовці для самоорганізації БСМ. В [19] дано опис розподіленого протоколу SMACS (Self-organizing Medium Access Control for Sensor networks), який на рівні ланки даних здійснює пошук сусідніх вузлів і складання розкладу прийому і передачі кадрів. Інший протокол рівня ланки даних, GSTEB (General Self-

Organization Tree-Based Energy-Balance routing protocol), також здійснює самоорганізацію БСМ на основі даних, отриманих від сусідніх вузлів [20]. Цікавий приклад технології побудови БСМ для транспортних засобів наведено в [21]: система SOTIS (Self-Organizing Traffic-Information System) дозволяє транспортним засобам обмінюватися зібраною інформацією про дорожню ситуацію за допомогою широкомовних пакетів, при цьому топологія мережі, що складається з транспортних засобів, постійно змінюється.

Архітектура сенсорних вузлів значною мірою залежить від функцій, які повинна виконувати дана БСМ. Однак можна виділити загальні для будь-яких БСМ елементи сенсорних вузлів. Невід'ємною частиною сенсорного вузла є власне сенсор, тобто пристрій, що збирає інформацію про навколишнє середовище і об'єктах в ній.

На даний момент в сенсорних мережах використовується велика кількість різноманітних сенсорів: пристроїв, призначених для моніторингу стану навколишнього середовища, промислових об'єктів і об'єктів домашнього господарства (датчики температури, вологості, атмосферного тиску, рівня води, вібрації, вогню і диму і т.д.), різноманітні хімічні датчики, детектирующие наявність тих чи інших хімічних речовин в повітрі або воді, медичні пристрої (датчики температури тіла, пульсу, артеріального тиску, рівня глюкози в крові і т.д.), Датчики швидкості транспортних засобів і завантаженості доріг, сенсори систем безпеки, що дозволяють виявити вторгнення на територію, що охороняється і відстежувати місце розташування будь-якого об'єкта.

Сенсори отримують інформацію із зовнішнього середовища в аналоговому вигляді, в той час як всі подальші дії з обробки і передачі інформації припускають цифрову форму представлення даних, в зв'язку з цим необхідна наявність в сенсорному вузлі аналого-цифрового перетворювача (АЦП).

У сенсорному вузлі міститься також обчислювальна система, що складається з мікроконтролера і запам'ятовує. Дана система виконує (опціонально) попередню обробку та тимчасове зберігання отриманих від сенсора даних, а також реалізує стек протоколів, необхідних для передачі даних по мережі.

Приймач бездротової мережі також є обов'язковим пристроєм сенсорного вузла, призначеним для безпосередньої взаємодії з іншими вузлами БСМ і шлюзом / колектором даних.

Останнім обов'язковим елементом сенсорного вузла є джерело живлення. Для сенсорних мереж «розумного будинку» або промислових об'єктів джерело живлення може бути неавтономним (підключення до мережі електроживлення), але в більшості сценаріїв роботи БСМ передбачається, що джерело все ж буде автономним (гальванічний елемент

або акумулятор, найчастіше невеликих розмірів). У деяких дослідженнях пропонується використовувати для цілей електроживлення сенсорних вузлів сонячні батареї [22].

Додатково сенсорний вузол може бути забезпечений наступними елементами:

— Пристрій для здійснення пересування. Деякі додатки БСМ припускають можливість самостійного пересування сенсорних вузлів. Найбільш часто така особливість зустрічається, звичайно, в БСМ, які передбачають рух сенсорного вузла за рахунок сторонніх систем, наприклад, в разі мережі VANET (Vehicular Ad hoc NETwork) - самоорганізується і не має центральної інфраструктури мережі, призначеної для обміну інформацією між сенсорними вузлами, встановленими на транспортних засобах. При цьому сенсорний вузол змінює своє положення в просторі, проте не за рахунок власної підсистеми руху, а за допомогою транспортного засобу, на борту якого він встановлений.

Інший підхід до мобільних сенсорним вузлів представлений в [24], де описується концепція БССМ в якій роботизовані мобільні сенсорні вузли вирішують ряд проблем стаціонарних БСМ - неоптимальний розташування сенсорних вузлів на сенсорному полі, нерівномірне витрачання електроенергії вузлів і т.д. У той же час такий підхід до побудови БСМ на поточний момент не є поширеним, так як на пересування сенсорних вузлів може витрачатися значна частина електроенергії джерела живлення, що призводить до зменшення терміну автономної роботи такої мобільної БСМ в порівнянні з аналогічною стаціонарної.

— Система позиціонування. Часто в сценаріях роботи БСМ потрібно точно знати розташування того чи іншого сенсорного вузла з метою отримання інформації про те, в якій саме частині сенсорного поля спрацював, наприклад, датчик диму або вторгнення. Крім того, інформація про місцезнаходження сенсорного вузла може використовуватися в службових цілях, наприклад, для автоматичного призначення мережевої адреси [7].

— Актор і цифро-аналоговий перетворювач (ЦАП). Актор - це виконавчий пристрій, яке виконує дію на навколишнє середовище відповідно до отримуваних ним командами. Прикладами акторів можуть служити пристрої, які розпилюють воду, якщо сенсори тієї ж мережі показують зниження вологості повітря, або пристрої, що рухаються або здійснюють інші механічні маніпуляції у відповідь на що прийшла по бездротовій мережі команду. Для роботи акторів потрібно ЦАП, так як керуючі команди приходять в цифровому вигляді, в той час як сам актор аналоговий пристрій. Загальна схема сенсорного вузла показана на рисунку 1.7.

Рисунок 1.7 - Архітектура сенсорного (сенсорно-факторного) вузла

Обов'язкові елементи виділені безперервної лінією, необов'язкові - переривчастою.

1.3 Застосування сенсорних мереж

Зазвичай БСМ застосовується для збору даних з пристроїв, обладнаних сенсорами: датчиком температури, вологості, освітлення, тобто моніторингу. Наприклад, мініатюрні сенсори можуть бути використані в медицині для спостереження за пацієнтами. Пристрої, які пацієнт носить із собою, можуть контролювати роботу життєво важливих органів і в разі якихось небезпечних ситуацій повідомляти лікаря.

Невеликі розміри пристроїв дозволяють проводити не тільки «поверхневі» спостереження за пацієнтом, а й досліджувати внутрішні органи людини. Так при проведенні гастроскопії в державних лікарнях, поліклініках застосовують спеціальні апарат з гастроскопіческом трубкою, але не всі пацієнти можуть її проковтнути. На ринку вже існують пристрої у вигляді таблеток для проведення таких досліджень. Ці пристрої на батарейках мають запас енергії, достатній для того, щоб безперервно працювати протягом 24 годин і відправляти свідчення іншого пристрою, яке пацієнт носить із собою протягом цього часу. Після цього лікар може аналізувати отримані результати і поставити точний діагноз.

Сенсори можуть використовуватися для автоматичного вмикання освітлення, коли людина входить в кімнату, використовуватися для управління якихось пристроїв (в системі «розумний дім»).

Іноді потрібно стежити за рухливістю або руйнуванням будь-яких об'єктів, де важко прокласти кабелі. Для цього знову ж вигідніше застосувати сенсорні мережі, так як датчики мають автономне джерело живлення і вони бездротові.

Також технологія бездротових сенсорних мереж може бути використана для передачі звукових даних - як домофонної системи, мультимедіа системи з низьким енергоспоживанням. Гнучка архітектура, зниження витрат при монтажі виділяють бездротові мережі інтелектуальних датчиків серед інших бездротових і дротових інтерфейсів передачі даних, особливо коли мова йде про велику кількість з'єднаних між собою пристроїв, сенсорна мережа дозволяє підключати до 65000 пристроїв [24]. Постійне зниження вартості бездротових рішень, підвищення їх експлуатаційних параметрів дозволяють поступово переорієнтуватися з провідних рішень в системах збору телеметричних даних, засобів дистанційної діагностики, обміну інформацією. «Сенсорна мережу» є сьогодні усталеним терміном (англ. Sensor Networks), що позначає розподілену, самоорганізується, стійку до відмови окремих елементів мережу з необслуговуваних і які не потребують спеціальної установки пристроїв. Кожен вузол сенсорної мережі може містити різні датчики для контролю зовнішнього середовища, мікрокомп'ютер і радіо приймач. Це дозволяє пристрою проводити вимірювання, самостійно проводити початкову обробку даних і підтримувати зв'язок із зовнішнім інформаційною системою.

Технологія ретранслювання ближнього радіозв'язку 802.15.4 / ZigBee [11], відома як «Сенсорні мережі», є одним із сучасних напрямків розвитку систем, що самоорганізуються, відмовостійких розподілених систем спостереження та управління ресурсами і процесами. Сьогодні технологія бездротових сенсорних мереж, є єдиною бездротовою технологією, за допомогою якої можна вирішити завдання моніторингу та контролю, які критичні до часу роботи датчиків. Об'єднані в бездротову сенсорну мережу датчики утворюють територіально-розподілену систему, що самоорганізується збору, обробки і передачі інформації. Основною областю застосування є контроль і моніторинг Реальні показники можуть відрізнятися фізичних середовищ і об'єктів.

Прийнятий стандарт IEEE 802.15.4 [11] описує контроль доступу до бездротового каналу і фізичний рівень для низькошвидкісних бездротових персональних мереж, тобто два нижніх рівня згідно мережевий моделі OSI. «Класична» архітектура сенсорної мережі заснована на типовому вузлі, який включає в себе:

— радіотракт;
— процесорний модуль;
— елемент живлення;
— різні датчики.

Використання в типовому вузлі сенсорної мережі в якості датчика другого трансивера, що відповідає стандарту ISO 24730-5, дозволяє використовувати сенсорну мережу не тільки для моніторингу параметрів середовищ і об'єктів, а й для визначення

місцезнаходження і моніторингу пересувань об'єктів, забезпечених спеціальними радіочастотними мітками. Побудована з таких вузлів сенсорна мережа утворює бездротову інфраструктуру RTLS.

Типовий вузол може бути представлений наступними типами пристроїв:

— пристрій з повним набором функцій FFD (Fully Function Device): здійснює глобальну координацію, організацію та установку параметрів мережі; найбільш складний з типів пристроїв, вимагає найбільший обсяг пам'яті і джерело живлення; підтримка 802.15.4; додаткова пам'ять і енергоспоживання дозволяють виконувати роль координатора мережі; підтримка всіх типів топологій («точка-точка», «зірка», «дерево», «чарункова мережа»); здатність звертатися до інших пристроїв в мережі;

— пристрій з обмеженим набором функцій (RFD - Reduced Function Device): підтримує обмежений набір функцій 802.15.4; підтримка топології «точка-точка», «зірка»; не виконує функції координатора; звертається до координатора мережі і маршрутизатора;

1.4 Платформи

Через відсутність чіткої стандартизації в сенсорних мережах, існує кілька різних платформ. Всі платформи відповідають основним базовим вимогам до сенсорних мереж: мала споживана потужність, тривалий час роботи, малопотужні приймально-передавачі і наявність сенсорів. До основних платформ можна віднести MicaZ, TelosB, Intel Mote 2.

Типовий вузол MicaZ мікропроцесор: MSP430 F1611; 8 Мгц частота; 48 Кб флеш-пам'яті для програм; 10 Кб RAM для даних; UART; SPI шина; вбудований 12-бітовий ADC / DAC; DMA контролер радіо: ChipCon CC2420; зовнішня флеш-пам'ять: 1024 Кб; 16-pin додатковий коннектор; три програмованих LEDs; JTAG порт; опціонально: сенсори освітленості, вологості, температури.

На рисунку 1.8 харчування від двох батарей AA.Mote 2: 320/416/520 МГц PXA271 XScale мікропроцесор; 32 МБ Флеш-пам'яті; 32 МБ ОЗУ; mini-USB інтерфейс; I-Mote2 коннектор для зовнішніх пристроїв (31 + 21 pin); radio: ChipCon CC2420; світлодіодні індикатори; живлення від трьох батарей AAA.

Рисунок 1.8 - Плата Intel Mote 2

Основним стандартом передачі даних в сенсорних мережах є IEE802.15.4, який спеціально був розроблений для бездротових мереж з малопотужними приймально-передавачами.

Ніяких стандартів в галузі програмного забезпечення в сенсорних мережах немає. Існує кілька сотень різних протоколів обробки і передачі даних, а також систем управління вузлами. Найбільш поширеною операційною системою є система з відкритим кодом - TinyOs. Багато розробники часто пишуть свою систему управління, часто на мові Java. Програма управління сенсорного вузла під управлінням операційної системи TinyOs пишеться на мові nesC.

Будь-яке середовище передачі (радіо ефір, Ethernet і т.д.) обмежена на увазі того, що одночасно їй може скористатися тільки один або обмежене число користувачів.

Протоколи канального рівня (MAC - Medium Access Control) займаються управлінням доступу до єдиної середовища передачі даних

Класифікація MAC протоколів:

— Протоколи на основі конкуренції. Вузли конкурують за доступ до середовища передачі. Приклади: ALOHA (Pure and Slotted), CSMA

— Протоколи за розкладом. Вузли передають в різних підканалах. Приклади: FDMA, TDMA, CDMA

Властивості MAC протоколів:

— уникнення колізій - основне завдання MAC протоколів;

— енергетична ефективність - важлива властивість в сенсорних мережах.

— MAC контролює трансивер;

— масштабованість і адаптивність - MAC протоколи повинні вміти адаптуватися;

— затримка - важливість залежить від конкретного додатка;

— пропускна здатність залежить від програми Goodput;

— справедливість - в сенсорних мережах може бути неоднорідний розподіл трафіку.

Найбільш важливими факторами в сенсорних мережах є енергетична ефективність, уникнути колізій і адаптивність. Енергетична ефективність один з найголовніших чинників в сенсорних мережах. Основні джерела втрат енергії:

— колізії - атрибут «конкурентних» протоколів;

— пасивне прослуховування каналу - для малопотужних трансиверів, витрати енергії на прийом повідомлення можуть бути більше, ніж на його передачу;

— verhearing - може бути домінуючим фактором при великого навантаження і щільності вузлів;

— Control Packet Overhead - зменшують ефективну goodput.

Розглянемо найбільш популярні MAC: Co-ordinated Adaptive Sleeping. Комбінування основних достоїнств протоколів «за розкладом» (TDMA) і «конкурентних» протоколів (CSMA). синхронізоване розклад Розклад підібрано таким чином, що, коли вузли хочуть передати інформацію, вони прокидаються синхронно. Несинхронізована передача. Коли вузол прокинувся і хоче передати інформацію, він робить це за допомогою алгоритму CSMA / CA.

Основний компроміс - жертвуючи затримками / справедливістю покращуємо енергетичну ефективність. S-MAC намагається зменшити витрати енергії за рахунок:

— Пасивний прийом - періодичне засинання.

— Колізії - використання RTS / CTS

— Overhearing - вимикання радіо, коли передача не призначається для цього вузла.

— Службові пакети - передача повідомлень.

переваги:

— значно ефективніший, ніж звичайний CSMA / CA;

— планує час сну і час активності для забезпечення енергетично ефективної передачі при задовільних затримках.

недоліки:

— алгоритмічно складніше;

— істотні витрати на організацію (розклад);

— комбінує виявлення несучої RTS / CTS і засипання за розкладом в один MAC протокол, що може перешкодити при оптимізації під конкретні програми.

B-MAC: Versatile Low-power medium access for sensor networks.

Поділ канального рівня і контролю доступу до середовища, дає кращу оптимізацію під конкретні програми. Сон без розкладу (Unscheduled sleep). Зменшує кількість службової інформації. Але передавача необхідно більше зусиль, щоб пробудити приймач від сну. Пробудження без розкладу (Unscheduled wakeup). Тимчасові інтервали між пробудженнями дуже короткі. Може бути використаний CSMA / CA або інші app-specific алгоритми.

У наступному розділі розглядаються загальні вимоги до алгоритмів маршрутизації, виконується огляд і порівняння таких алгоритмів.

1.5 Вимоги до алгоритмів маршрутизації в БСМ

У зв'язку з необхідністю скорочення використання обчислювальних ресурсів (радіо, батарея, датчики), протоколи маршрутизації в бездротових сенсорних мережах, повинні відповідати таким вимогам [12]:

— Автономність. Видалення певного вузла мережі не повинно вплинути на її роботу. Так як в мережі не повинно бути центрального вузла, будь-хто може виконувати функції маршрутизації віддаленого.

— Енергоефективність. Протоколи маршрутизації повинні максимально ефективно використовувати харчування.

— Масштабованість. Бездротові сенсорні мережі складаються з сотень вузлів, тому протоколи маршрутизації повинні працювати з цією кількістю вузлів.

— Стійкість. Датчики можуть раптово припинити роботу через зовнішні причини або витрати заряду акумулятора. Протоколи маршрутизації повинні впоратися з цією можливістю - коли струм в вузлах пропадає, повинен бути використаний альтернативний маршрут.

— Гетерогенность пристроїв. Хоча в більшості випадків застосування бездротових сенсорних мереж покладаються на однорідність вузлів, введення різних видів датчиків може дати значну перевагу.

— Мобільність. У багатьох випадках вузли можуть переміщатися в процесі функціонування. Протоколи маршрутизації повинні враховувати це.

Особливості та обмеження бездротових сенсорних мереж породжують особливі вимоги до протоколів маршрутизації. Зазвичай виділяють наступні технічні характеристики:

— Заснованність на атрибутах. У таких алгоритмах, вузол відправляє запити в певні області мережі і чекає відповіді від датчиків, розташованих в цій області. Вибір атрибутів залежить від програми. Важливою особливістю цієї схеми є те, що зміст повідомлення з даними аналізується на кожному етапі маршрутизації.

— Енергоефективність. У таких алгоритмах вибираються ті маршрути, які, як очікується, максимально сприяють збереженню енергії в мережі. Для цього маршрут складається з вузлів з більш високими енергетичними ресурсами.

— Агрегація даних. Щодо близько розташовані вузли можуть давати схожі дані, які можуть бути об'єднані з деякими допустимими втратами точності.

Сенсорні додатки значно залежать від комунікації між вузлами, так як це необхідно для виконання певних процедур або алгоритмів. Фактично, існує три основних види алгоритмів маршрутизації бездротових сенсорних мереж:

— Централізовані алгоритми: Вони виконуються на вузлі, який має знання про всю мережі. Ці алгоритми досить дороги у використанні через високу вартість передачі даних для отримання стан всієї мережі.

— Розподілені алгоритми: комунікація здійснюється передачею повідомлень.

— Місцеві алгоритми: вузли використовують дані, отримані з ближньої області. З використанням цієї інформації, алгоритм може виконуватися на одному вузлі.

Використовувані алгоритми є важливим фактором для прийняття до уваги при виборі алгоритму маршрутизації. Якщо використовуються місцеві алгоритми, то важлива висока комунікаційна зв'язність близько розташованих вузлів. При централізованих алгоритмах об'єднання повідомлень є великим плюсом. Розподілені алгоритми повинні забезпечувати надійний зв'язок між будь-якими двома вузлами мережі. При виборі місцевих алгоритмів слід враховувати, що використання додаткових засобів визначення положення (наприклад, GPS) може підвищити ціну таких мереж значно.

Класифікація за способом розрахунку шляхів:

— Proactive protocols - Всі шляхи розраховуються заздалегідь, до того, як вони будуть потрібні;

— Reactive protocols - Шляхи розраховуються на вимогу;

— Hybrid protocols - Комбінація двох підходів.

1.6 Огляд алгоритмів маршрутизації в БСМ

Алгоритм SPIN: Sensor Protocols for Information via Negotiation.

Базові ідеї протоколів SPIN - обмін вимірюваними даними може бути витратним, але обмін даними про вимірювальні даних (мета-даними) може бути і немає. Вузли повинні проводити моніторинг і адаптуватися до змін їх власних енергетичних ресурсів.

Потенційно кожен вузол є базовою станцією і доставка інформації відбувається від кожного до кожного. Протокол використовує мета-дані і систему «переговорів». Семантика мета-даних не специфицируется протоколом і залежить від конкретних додатків. Протокол може адаптуватися в залежності від кількості енергії, що залишилася на вузлах. Протокол працює по time-driven манері і доставляє інформацію до всіх вузлів мережі навіть, якщо вони її не замовляли.

Алгоритм SPIN має три стадії роботи і відповідно можуть передаватися три типи повідомлень:

— ADV - використовується для розповсюдження інформації про нові дані. Містить мета-дані.

— REQ - для запиту цих даних.

— DATA - це самі дані.

Якщо вузол хоче послати нові дані, він спочатку посилає ADV повідомлення своїм сусідам, якщо хтось із сусідів зацікавлений в отриманні цих даних, то він посилає REQ повідомлення, і далі отримує дані (DATA-повідомлення).

Існує кілька протоколів сімейства SPIN:

— SPIN-1: стандартний протокол.

— SPIN-2: протокол використовує інформацію про залишилася енергії.

— SPIN-BC: для поширення broadcast повідомлень.

— SPIN-PP: для передачі повідомлень точка-точка (point-to-point).

— SPIN-EC: подібний до попереднього, але з використанням інформації про енергію (energy heuristic).

— SPIN-RL: розроблений для нестабільних каналів (lossy channels) [40].

Протоколи сімейства SPIN добре підходять для додатків, де вузли мобільні, так як їм потрібно тільки локальна інформація про сусідів.

Недоліком SPIN протоколів є те, що вони не гарантують доставку даних.

Алгоритм Directed Diffusion - сенсорна мережа розглядається як віртуальна база даних. Реалізована обробка запитів від БС. Запит поширюється по всій мережі (флудинг) або передається обраній групі вузлів. У відповідь вузли, що мають запитувані дані, посилають їх назад на БС. Проміжні вузли можуть об'єднувати дані. Diffusion - це data-centric і application-aware протокол в якому всі дані генеруються сенсорними вузлами позначаються парами атрибутів.

Основна ідея протоколу Directed Diffusion - це комбінування даних від різних джерел на проміжному вузлі (in-network aggregation), усуваючи надмірність і зменшуючи кількість передач, таким чином продовжуючи час життя мережі.

Основні елементи Directed Diffusion:

— Naming. Дані позначаються за допомогою атрибутів.

— Interests. Вузол запитує дані, посилаючи запит (interest) на певні дані.

— Gradients. Градієнти (gradients) встановлені в межах мережі, щоб доставляти дані збігаються із запитом.

— Reinforcement БС «встановлює» (reinforce) певні маршрути, щоб доставляти дані з більшою швидкістю (дані про швидко мінливих події).

— Based naming Завдання позначаються списком атрибутів - парами значень.

Опис завдання визначає запит (interest) на дані, які збігаються з атрибутами. БС періодично посилає (broadcast) запит (interest) на дані всіх своїх сусідів.

Кожен вузол зберігає interest cache. Кожен запис відповідає індивідуальним запитом. Не містить інформації про БС. Об'єднання (aggregation) збігаються запитів. Кожен запис в кеші має кілька полів. Відмітка про час прийому останнього збігається запиту. Кілька градієнтів: швидкість даних, тривалість, напрямок.

Використовує обробку / об'єднання даних усередині мережі. Досягає бажаного глобального поведінки за допомогою локального взаємодії. Емпірично адаптується до навколишнього оточення.

Алгоритм Rumor Routing - це варіант Directed Diffusion. Використовується, коли кількість подій (events) мале, а кількість запитів (queries) велике. За допомогою флудинг поширюються не запити, а інформація про події. Довго живуть пакети, звані агентами, поширюють (flood) інформацію про події по мережі. Коли вузол виявляє подія, він додає його в таблицю подій і генерує агента. Агенти подорожують по мережі, поширюючи інформацію про локальному подію. Час життя агента (Time-To-Live).

Коли вузол генерує запит, вузол знає маршрут до відповідного події може відповісти, заглядаючи в свою таблицю подій. Немає необхідності використовувати флудинг для поширення запитів. Тільки один шлях між джерелом і приймачем. Rumor Routing працює добре тільки, коли кількість подій мало. Витрати на підтримку великої кількості агентів і таблиці подій.

Алгоритм LEACH: Low-Energy Adaptive Clustering Hierarchy - вузли саме організовуються в кластери і вибирають cluster head. Всі вузли, які не є cluster head'амі, передають інформацію cluster head'у. Cluster head приймає дані, виробляє їх обробку і передає на базову станцію. Періодично відбувається випадкова зміна cluster head'a і перекластерізація.

На рисунку 1.9 показані дві фази: організація кластерів і передача даних cluster head'у і на базову станцію.

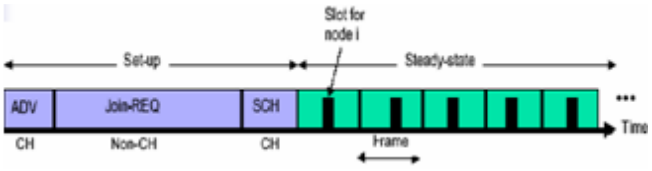


Рисунок 1.9 - Схема роботи алгоритму LEACH

На початковому етапі кожен вузол пропонує себе в якості cluster-head'a з певною ймовірністю. Вузли, які не стали cluster-head'амі, можуть стати ними згодом. Рішення приймається на основі заданої щільності cluster-head'ов в мережі для розподілу енергетичного навантаження по мережі, cluster-head'и періодично переізбераются. Вузол cluster-head розсилає свій статус інших вузлів мережі. Кожен вузол вибирає до якого кластеру він хоче приєднатися на основі енергетичної ефективності. Коли все вузли організувалися в кластери, cluster-head створює розклад для кожного вузла.

Формування кластеру. Кожен cluster head посилає ADV повідомлення, за допомогою CSMA / CA протоколу. Повідомлення містить ID вузла і заголовок, який показує, що це ADV повідомлення. На основі сили сигналу від кожного cluster-head'a кожен вузол вибирає до якого кластеру приєднатися. Кожен вузол посилає (за допомогою CSMA / CA) join-request повідомлення своєму cluster-head'у. Повідомлення містить ID cluster-head'a і самого вузла. Кожен cluster-head створює TDMA розклад. Це гарантує уникнення колізій при передачі повідомлень і економію енергії.

На исунку 1.10 показана фаза передачі. Вузли передають дані свого відведений час. Після отримання повідомлень від усіх вузлів cluster-head формує свої повідомлення. Потім cluster-head передає ці повідомлення на базову станцію. Для зменшення колізій cluster-head'и використовують CDMA коди. Перед початком передачі вузол-cluster-head прослуховує канал. Якщо канал вільний, він передає інформацію на базову станцію.

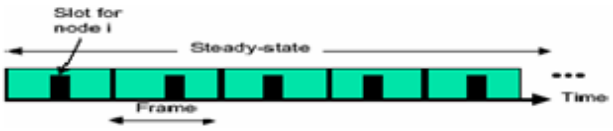


Рисунок 1.10 - Алгоритм LEACH: Фаза передачі

Переваги:

— Використання адаптивного самоорганізованого протоколу дозволяє розподілити енергетичне навантаження по всій мережі.

— Дозволяє проводити обробку даних на cluster-head'е, що може зменшити кількість даних переданих по мережі.

— Оптимальна кількість кластерів може бути визначено заздалегідь залежно від топології мережі і відношення витрат на обробку / передачу інформації.

Перша «смерть» вузла відбувається у вісім разів пізніше, ніж при використанні прямої передачі і статичних кластерних протоколів. Поліпшення LEACH. Формує не

кластери, а ланцюжки. Дані передаються по ланцюжку і один вузол їх посилає. Перевершує LEACH за енергетичними показниками. Великі затримки для вузлів на кінцях ланцюжка. Ієрархічний PEGASIS. Використання CDMA: Threshold sensitive Energy Efficient Network, event-driven protocol for time-critical applications. Вузол постійно моніторірует середу, але передає інформацію тільки, якщо значення змінюється значно. Немає переодической передачі. Критичні дані передаються негайно. Посилає своїм вузлам «жорсткий» (hard) і «м'який» (soft) поріг:

— Жорсткий поріг: вузол посилає інформацію CH тільки, якщо значення знаходиться в інтересуемого межах.

— М'який поріг: вузол посилає інформацію CH тільки, коли значення змінилося як мінімум на значення порога.

Кожен вузол в кластері періодично ставати CH.

Ієрархічну кластеризацію, згадану раніше, можна побачити на рисунку 1.11.

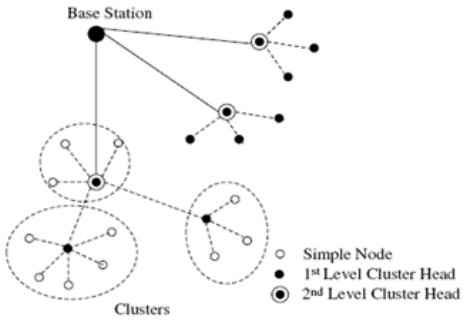


Рисунок 1.11 - Ієрархія вузлів в алгоритмі TEEN

Добре підходить для додатків критичних до часу. Менші енергетичні витрати. Менші витрати, ніж проактивні протоколи. «М'яка» межа може адаптуватися. «Жорстка» межа може варіюватися в залежності від додатків. Не підходить для періодичного моніторингу.

Алгоритм APTEEN: Adaptive Threshold sensitive Energy Efficient Network. Розширення TEEN як для підтримки і періодичного моніторингу, так і для реакції на критичні події. На відміну від TEEN вузол повинен зібрати і передати дані, якщо вони не були послані за певний період часу (count time), який встановлюється CH. У порівнянні з алгоритмом LEACH, TEEN & APTEEN споживають меншу кількість енергії.

Недоліки. Накладні витрати і складність формування багаторівневих кластерів і організації порогових функцій.

Алгоритм SOP: Self - Organization Protocol. Архітектура підтримує різнотипні вузли. Стаціонарні вузли роутери використовуються як основа мережі. Мобільні або стаціонарні

сенсорні вузли посилають інформацію на роутери. Сенсорний вузол може бути частиною мережі тільки в разі, якщо він може передати інформацію на роутер безпосередньо. Дана архітектура вимагає можливості адресації кожного вузла.

Переваги:

— Підходить для додатків, де потрібна зв'язок з певним вузлом.

— Невеликі витрати на підтримку таблиці маршрутизації.

— Збереження збалансованої маршрутної ієрархії.

— Збереження енергії: використання обмеженого підмножини вузлів.

Недоліки:

— Даний протокол не є протоколом «на вимогу» особливо, що стосується організаційної фази.

— Існування безлічі розривів підвищує ймовірність реорганізації мережі (витратна операція).

Алгоритм GAF: Geographic Adaptive Fidelity. - based протокол, що враховує енергетичні ресурси вузла.

Кожен вузол знає свої координати через GPS. Асоціює себе з точкою на віртуальній решітці. Вузли, які вважають, що знаходяться в одній точці, рівнозначні в термінах «вартості» маршрутизації пакета.

Вузол 1 може досягти будь-якої з вузлів 2, 3 або 4, отже, вузли 2,3,4 еквівалентні (рисунок 1.12). Будь-які 2 можуть перебувати в сплячому режимі без впливу на маршрутизацію.

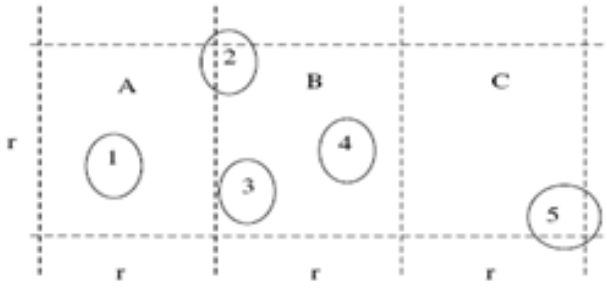


Рисунок 1.12 - Досяжні вузли в алгоритмі GAF

Розроблено переважно для MANET, але може бути використаний і для сенсорних мереж.

При обліку мобільності кожен вузол оцінює час свого «залишення» решітки і посилає цей час сусідам. Сусідні вузли регулюють час сну, щоб забезпечити маршрутизацію.

Протокол погано масштабується. Тільки активні вузли посилають інформацію, тому точність інформації не дуже висока.

Алгоритм GEAR: Geographic and Energy Aware Routing.

Обмежує кількість пересилаються запитів в directed diffusion. Розглядає тільки певний район мережі замість всієї мережі в цілому. Кожен вузол зберігає estimated cost & learning cost на досягнення БС через своїх сусідів. Estimated cost = f (що залишилася енергія, відстань до точки призначення)

Фаза 1: Пересилання пакетів в певний район.

Пересилання пакета сусідньому вузлу з мінімальною функцією f (найближчий до БС і має найбільшу енергію)

Якщо всі вузли знаходяться далі, ніж сам вузол відправник, то вибирається один із сусідів сну основі learned cost.

Фаза 2: Пересилання пакета в межах потрібної області.

Застосовується будь рекурсивне відправлення повідомлень. Район ділитися на 4 підобласті і надсилається 4 копії пакета (рисунок 1.13). Повторюється до тих пір, поки не залишаться райони з одним вузлом. Застосовується обмежений флудинг. Застосовується, коли щільність вузлів мала.

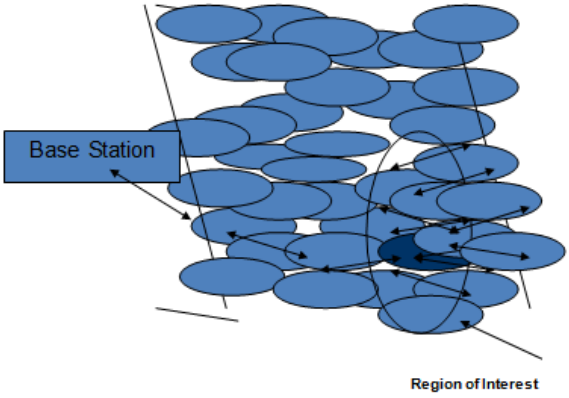


Рисунок 1.13 - Відправлення повідомлення в алгоритмі GEAR

Протоколи маршрутизації з багатьма маршрутами (Multipath routing)

Підвищення надійності передачі інформації, за рахунок існування декількох маршрутів. Збільшує енергетичні витрати. Збільшує кількість трафіку в мережі. Тому не розглядається.

1.7 Порівняння алгоритмів маршрутизації в БСМ

Порівняємо різні алгоритми маршрутизації в бездротових сенсорних мережах (таблиця 1.1).

Таблиця 1.1 - Порівняння протоколів маршрутизації

Протокол	Заснований на атрибутах	Енергоефективність	Місцевого типу	Multipath	QoS	Ієрархічний
SPIN	так					
Directed Diffusion	так					
Rumor	так					
COUGAR	так					
ACQUIRE	так					
GAF		так	так			
LEACH		так				так
PEGASIS		так			так	так
TEEN		так				так
DirQ						так
SHRP		так		так	так	так
SAR				так	так	
Maximum Lifetime		так		так		
Energy Aware		так		так		
M-MPR		так	так	так		

Основними алгоритмами маршрутизації, оптимізованими для підвищення енергоефективності бездротових сенсорних мереж, є: GAF, LEACH, PEGASIS, TEEN, SHRP, M-MPR.

1.8 Постановка задачі

Після проведеного аналізу літератури можна сформувати задачу для розгляду: розглянути математичні методи оцінки надійності бездротової сенсорної мережі і програмні продукти для імітаційного моделювання БСМ, провести їх аналіз з метою вибору системи, найбільш підходящою для оцінки працездатності БСМ. За допомогою обраної системи оцінити вплив перешкод і потужності передачі радіосигналу на працездатність БСМ.

Для досягнення поставленої мети необхідно вирішити такі завдання:

— вивчити стандарти бездротових сенсорних мереж;

— дослідити надійність передачі пакета даних між двома вузлами в обраній системі;

— побудувати модель надійності передачі пакета даних між двома вузлами в обраній системі;

— дослідити стійкість і надійність збору інформації мережею в обраній системі.

1.9 Висновок до першого розділу

— Була розглянута та топологія архітектура БСМ.

— Розглянуті галузі застосування та платформи сенсорних мереж.

— Оглянуті та виділені вимоги до алгоритмів маршрутизації БСМ.

— Проведення порівняння алгоритмів.

— Сформульовані задачі магістерської роботи.

2 ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Варто зазначити, що через дороге обладнання та складні настройки сенсорних мереж, широке поширення одержали різні системи імітаційного моделювання БСМ.

У наш час БСМ є актуальною темою досліджень. Багато аспектів роботи і побудови таких мереж не стандартизовані. Створення стенду для тестування БСМ є дуже дорогим. Запуск реальних експериментів на стенді також складний. Крім того, стабільність в значній мірі непередбачувана, оскільки багато чинників впливають на результати експерименту. Важко ізолювати один аспект дослідження від інших. Крім того, запуск реальних експериментів завжди забирає багато часу. Тому в області БСМ моделювання має велике значення для розвитку цієї сфери. Протоколи, схеми, навіть нові ідеї можуть бути оцінені в дуже великих масштабах. Системи імітаційного моделювання БСМ дозволяють користувачам ізолювати різні чинники параметрами налаштування.

Отже, імітаційне моделювання має важливе значення для вивчення БСМ, будучи поширеним способом для тестування нових додатків і протоколів у цій області. Це призвело до бурхливого розвитку систем моделювання БСМ в останні роки [6].

Однак отримання точних висновків з результатів моделювання не є тривіальним завданням. Є два ключові аспекти в моделюванні БСМ: правильність імітаційної моделі і придатність конкретних інструментів для реалізації даної моделі. Фундаментальною проблемою є вибір між точністю моделі і продуктивністю з масштабованістю.

2.1 Особливості моделювання БСМ

Моделювання починається з опису реальної системи. Такий опис являє собою імітаційну модель, побудовану на основі розуміння величин, атрибутів, подій, каналів і т. д. Тому, розробник моделі описує ці структури моделювання в термінах сутностей і їх відносин і реалізує поведінку цих суб'єктів і реакцію на події. Системи моделювання БСМ чітко відокремлюють реалізацію процесу моделювання від опису моделі та примірників досліджуваної системи: ядро процесу моделювання та основних об'єктів моделі поставляються у вигляді набору програмних бібліотек на мові програмування високого рівня, як правило, Java або C ++. Деякі види скриптових мов програмування (TCL, наприклад) або мови розмітки (XML, наприклад), як правило, використовуються для опису моделі, тобто встановлення (оголошення) відносин між суб'єктами. Ці засоби дозволяють однаковий і ефективний підхід до опису моделі та її конфігурації. Крім того, деякі

бібліотеки часто включають підтримку графічного представлення або збору статистичних даних і аналізу.

Таким чином, система моделювання зазвичай складається з базової бібліотеки для моделювання, бібліотеки допоміжних засобів і системи опису та конфігурації моделей. Сама форма розгортання пакета залежить від реалізації. Деякі пакети надають засоби, які переводять опис моделей в об'єкти мови реалізації моделювання. Інші забезпечують візуальний інтерфейс.

Найважливішими властивостями пакетів моделювання БСМ є [6]:

— повторне використання і доступність;

— продуктивність і масштабованість;

— підтримка скриптових мов і інших способів опису моделей;

— засоби візуалізації і налагодження.

Повторне використання і доступність. Моделювання використовується для тестування нових методів в різних умовах реального середовища. Дослідники, як правило, зацікавлені в порівнянні продуктивності нової техніки від існуючих пропозицій. Таким чином, два ключові аспекти: чи включає інструмент моделювання реалізацію різних загальних моделей, наскільки легко змінити або інтегрувати нову модель з уже існуючими.

Перше питання, в основному, залежить від того, як давно система існує, і як багато людей використовують її [8]. Відомі системи моделювання мають багато доступних моделей і дуже ймовірно, що нові успішні моделі будуть додані в наступних випусках. Другий аспект тісно пов'язаний з конструкцією пакета моделювання. Акуратний, з чистою структурою інтерфейсів і високою модульність пакет дозволяє користувачеві легко додавати або змінювати функціональність. Готові до використання моделі дозволяють користувачам швидко створювати реалістичні сценарії моделювання і зосередитися на моделюванні більш конкретних деталей БСМ.

Продуктивність і масштабованість. Продуктивність і масштабованість є серйозною проблемою систем моделювання БСМ. Зазвичай обмеження накладає ефективність мови програмування і комп'ютерного обладнання.

Крім того, тип моделювання має на увазі деякі обмеження: режим емуляції має на увазі роботу в реальному часі, тому воно не може бути скільки завгодно довгим.

Такі речі як взаємодія з навколишнім середовищем, поширення радіохвиль, рухливість вузлів збільшують потребу в ресурсах для системи моделювання. Моделювання декількох сотень тисяч вузлів залишається складною проблемою [8].

Підтримка скриптових мов і інших способів опису моделей. Конфігурація БСМ як мінімум вимагає відповіді на питання: скільки вузлів є, де кожен вузол поміщається, чи

переміщаються вони, як використовується енергія, яке фізичне середовище, як генеруються події і т.д. Величезна кількість змінних, що беруть участь у визначенні експерименту БСМ вимагає використання спеціальних мов опису з високим рівнем семантики. Крім того, цілком імовірно, що велика кількість вихідних даних утворюються також через безліч реплік експериментів. Тому важлива відповідна вихідна мова, що дозволяє отримати точні і ясні результати експериментів.

Засоби візуалізації та налагодження. Графічна підтримка для моделювання цікава в трьох аспектах:

— З метою налагодження. Практичним способом швидко виявити погану поведінку є візуальне спостереження і стеження за виконанням моделювання.

— Як інструмент візуального моделювання. Ця особливість зазвичай полегшує і прискорює розробку невеликих експериментів або складу основних модулів. Однак при великих масштабах моделювання це не дуже практично.

— Як результат моделювання, що дозволяє швидко візуалізувати результати без додаткової обробки даних.

2.2 Вибір стандарту

Існує безліч різних стандартів бездротових мереж, проте їх всіх можна розділити на три групи:

— WPAN (WirelessPersonalAreaNetwork - бездротова персональна мережа).

— WLAN (WirelessLocalAreaNetwork - бездротова локальна мережа).

— WMAN (WirelessMetropolitanAreaNetwork - бездротова мережа масштабу міста).

З цих груп найбільш підходящими можуть бути стандарти групи WPAN, так як вони розраховані на низькошвидкісні мережі.

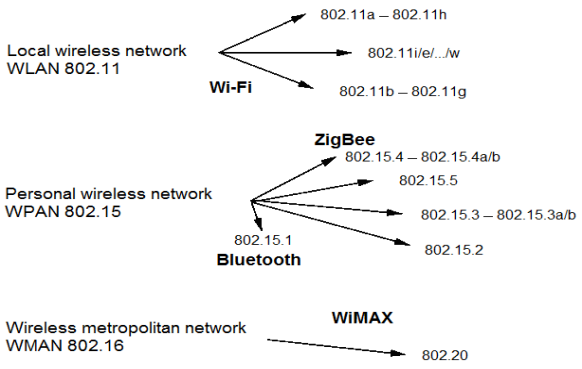


Рисунок 2.1 - Стандарти бездротових мереж

WPAN бездротова мережа, призначена для організації бездротового зв'язку між пристроями різного типу на обмеженій площі (наприклад, в рамках квартири, офісного робочого місця). Стандарти, що визначають методи функціонування мережі, описані в сімействі специфікацій IEEE 802.15.

IEEE 802.15.3 розроблявся як високошвидкісний стандарт WPAN-мереж для високотехнологічних побутових пристроїв (призначених, як правило, для передачі мультимедійних даних). Використання смуги 2,4 ГГц і технології модуляції O-QPSK (Offset Quadrature Phase Shift Keying, квадратурная маніпуляція фазовим зрушенням зі зміщенням) дозволяють досягати швидкості передачі в 55 Мб/с на відстань до 100 метрів. Захист даних може здійснюватися за стандартом AES. У модифікації стандарту 802.15.3a передбачається збільшити пропускну здатність до 480 Мб/с, а в разі специфікації 802.15.3b пропускна спроможність складе від 100 до 400 Мб/с. Цей стандарт передбачено під досить великі швидкості при передачі даних, а, отже, пристрої, що працюють на ньому, будуть мати високе енергоспоживання [8].

802.15.4 і Zigbee часто ототожнюються, адже в основі стандарту Zigbee лежить стандарт 802.15.4. Однак консорціум ZigBee Alliance вніс ряд змін і розширив його. Стандарт 802.15.4 є відкритим і його можна вільно скачати з Інтернету і використовувати. Zigbee ж є наполовину відкритим стандартом: так при використанні його в комерційних цілях необхідно вступати в ZigBee Alliance. До мінусів цього стандарту можна віднести його закритість, а також велика область застосування, а не «заточенність» під конкретні цілі [8].

Стандарт Bluetooth (802.15.1) на сьогоднішній день добре розвинений і застосовується для зв'язку мобільних телефонів, КПК, периферії. Однак він не розрахований на мережі з низьким енергоспоживанням, що істотно обмежує його поширення в сенсорних мережах. Пристрої за стандартом Bluetooth можуть об'єднуватися в піко мережі (не більше 7 на одну мережу). У мережі є провідний і ведений пристрій. Для обміну даними використовується, так званий, нижній ISM-діапазон (Industry, Science and Medicine - промисловий, науковий і медичний) 2,4-2,5 ГГц, який поширений в побутових приладах і бездротових мережах. Для використання цих частот ліцензія не потрібна. Потужність передавача-кристала становить 1 - 2,5 мВт і дальність дії до 10 м, а при збільшенні потужності до 100 мВт - 100 м. Даний стандарт міг би підійти для розробки, однак на ринку немає пристроїв, що працюють за цим стандартом з низьким енергоспоживанням - вони тільки передбачаються до випуску на ринок.

Стандарт Wibree розроблений фірмою Nokia в 2001 році. Wibree призначений для роботи пліч-о-пліч з Bluetooth. Він працює в діапазоні 2,4 ГГц з фізичною швидкістю

передачі 1 Мбіт/с. Основні області застосування включають такі пристрої, як наручний годинник, бездротові клавіатури, іграшки та спортивні датчики, де низьке енергоспоживання є одним з ключових вимог. Цей стандарт можна віднести до стандарту Bluetooth, тому у нього є такі ж недоліки - кількість пристроїв, що підключаються обмежена, відсутні на ринку модулі з низьким енергоспоживанням.

Порівняльна характеристика деяких стандартів виглядає наступним чином (таблиця 2.1).

Таблиця 2.1 – Порівняння стандартів безпровідних мереж

Параметри	Bluetooth	Wibree	ZigBee
Частота	2,4 ГГц	2,4 ГГц	2,4 ГГц
Споживана потужність	100 мВт	~10 мВт	30 мВт
Термін роботи батареї	до 6 місяців	1 - 2 роки	0,5 - 2 роки
Діапазон	10 - 30 м	10 м	10 - 75 м
Швидкість передачі	1 - 3 Мб/с	1 Мб/с	25-250 Кб/с
Ціна	3$	3,2$	2$
Топології	Зірка, точка-точка, змішана		
Безпека	128- бітове шифрування		
Час відгуку	3 с	3 с	15 мс

Найбільш відповідний стандарт 802.15.4, так як він є відкритим, призначений для низькошвидкісних мереж з низьким енергоспоживанням.

2.3 Опис стандарту IEEE 802.15.4

Стандарт 802.15.4 призначений для організації двох нижніх рівнів еталонної моделі OSI в бездротової сенсорної мережі - фізичний (PHY) і канальний (підрівень MAC) (рис.2.2). Ці шари пропонують послуги вищих верств. Інтерфейси між шарами служать для визначення логічних зв'язків.

Фізичний рівень надає дві послуги: фізичне обслуговування даних і фізичне обслуговування управління. Завдання рівня - активація/дезактивація радіо-приймача, вибір каналу, визначення рівня енергії (energy detection), передача і отримання пакетів через фізичне середовище. MAC рівень надає наступні послуги: обслуговування даних і обслуговування управління на канальному рівні. Завдання рівня - сигнальне управління, доступ до каналу, управління GTS, твердження пакетів, підтвердження доставки пакетів, з'єднання (асоціація) і роз'єднання (дізассоціація) з пристроями, крім того забезпечення механізму безпеки

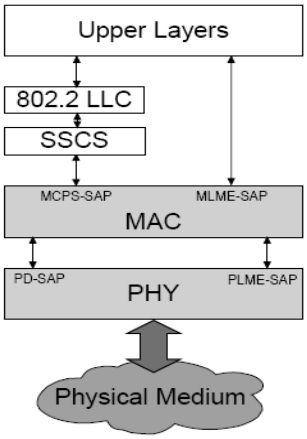


Рисунок 2.2 - Архітектура рівнів

Стандарт визначає протокол і взаємозв'язок пристроїв в наступних трьох неліцензованих радіодіапазонах:

— 868,0 - 868,6 МГц (Європа, один канал);

— 902 - 928 МГц (Північна Америка, всього 10 каналів, крок центральних частот - 2 МГц, сама нижня з них - 906 МГц);

— 2450 МГц (решта світу, всього 16 каналів, крок центральних частот 5 МГц, сама нижня з них - 2405 МГц).

Швидкості передачі даних в каналах при цьому складають від 20 Кбіт/с (в діапазоні 868 МГц) до 250 Кбіт/с (2450 МГц). В радіоканалі використаний метод широкосмугової передачі з розширенням спектра прямий послідовністю (DSSS) і паралельної (PSSS). Вся використовувана «широка» смуга частот ділиться на деяке число підканалів. Кожен переданий біт інформації перетворюється по заздалегідь зафіксованому алгоритму в послідовність з n біт, і ці n біт передаються одночасно і паралельно, використовуючи всі n підканалів.

У кожен інформаційний біт, що передається (логічний 0 або 1) вбудовується послідовність, так званих, чіпів. Чіпові послідовності, що вбудовуються в інформаційні біти, називають шумоподібним кодами (PN-послідовності), що підкреслює ту обставину, що результуючий сигнал стає шумоподібним і його важко відрізнити від природного шуму. Завдяки цьому можна використовувати одну і ту ж ділянку радіоспектра двічі - звичайними вузькосмуговими пристроями і «поверх них» - широкосмуговими.

Модуляція даних - квадратурна фазова зі зрушенням (O-QPSK). Формування сигналу в квадратурній схемі відбувається так само, як і в модуляторі QPSK, за винятком того, що кодуючі біти квадратурної складової несучої Q мають тимчасову затримку на

тривалість одного елемента T. Зміна фази при такому зміщенні кодуючих потоків, визначається лише одним елементом послідовності, а не двома. В результаті стрибки фази на 180° відсутні, оскільки кожен елемент послідовності, що надходить на вхід модулятора синфазного або квадратурного каналу, може викликати зміну фази на 0, 90 або 270° (-90°). Серйозним недоліком фазової модуляції є та обставина, що при декодуванні сигналу приймач повинен визначати абсолютне значення фази сигналу, так як у фазовій модуляції інформація кодується саме абсолютним значенням фази сигналу. Для цього необхідно, щоб приймач мав інформацію про «еталонний» синфазний сигнал передавача. Тоді шляхом порівняння сигналу з еталонним можна визначити абсолютний зсув фази.

Всі пристрої стандарту можна класифікувати по функціональності і за призначенням.

За функціональністю можна виділити два типи пристроїв: повнофункціональні (FFD) і полуфункціональні (RFD). Повнофункціональний пристрій може з'єднуватися з будь-яким пристроєм в мережі, а полуфункціональні - тільки з FFD.

За призначенням існують три різні типи пристроїв ZigBee:

— Координатор ZigBee (ZC) - найбільш відповідальна пристрій, формує шляхи древа мережі і може зв'язуватися з іншими мережами. У кожній мережі є один координатор ZigBee. Він управляє мережею - призначає PANID мережі, роздає короткі адреси, вибирає частоту.

— Маршрутизатор ZigBee (ZR) - може виступати в якості проміжного маршрутизатора, передаючи дані з інших пристроїв. Він також може запускати функцію додатка.

— Кінцеве пристрій ZigBee (ZED) - його функціональна навантаженість дозволяє йому обмінюватися інформацією з материнським вузлом (або координатором, або з маршрутизатором), він не може передавати дані з інших пристроїв. Таке ставлення дозволяє вузлу більшу частину часу перебувати в сплячому стані, що дозволяє економити енергоресурс батарей. ZED вимагає мінімальну кількість пам'яті, і тому може бути дешевше у виробництві, ніж ZR або ZC.

Виділяють наступні топології мережі: зірка і точка-точка (мережа рівноправних вузлів)

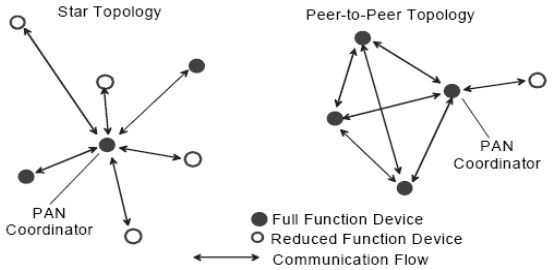


Рисунок 2.3 − Топология сети

У топології «зірка» обмін даними відбувається між центральним головним контролером, званим PAN-координатором і іншими відомими пристроями. Він є первинним пристроєм в мережі і тому може живитися від стаціонарного джерела.

У топології «рівноправних вузлів» також є PAN-координатор, однак будь-який пристрій, на відміну від топології «зірка», може зв'язатися з іншим, поки вони знаходяться в межах один одного. Таким чином, «рівноправні вузли» можуть утворювати більш складні мережеві освіти, наприклад, петлю або кластерне дерево (рис. 2.4). В цьому випадку RFD пристрої з'єднуються з деревовидної кластерної схемою як листове пристрій в кінці гілки.

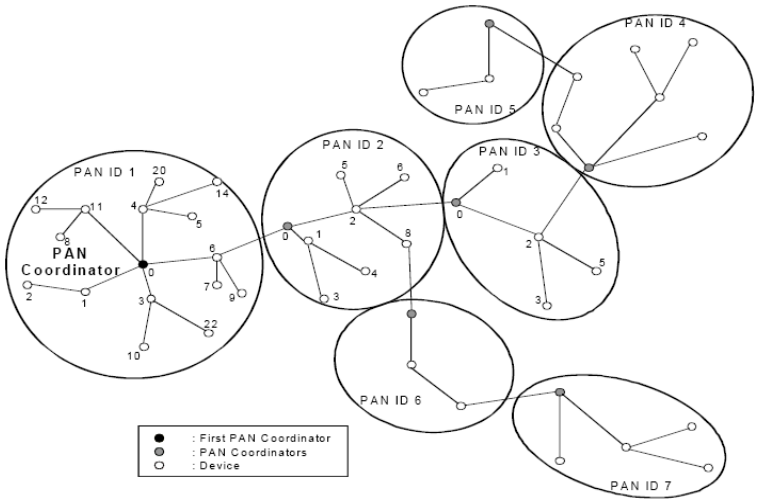


Рисунок 2.4 - Кластерна топологія

Всі пристрої повинні підтримувати унікальні 64-розрядні адреси. Ці адреси використовуються для адресації в межах даної мережі. Щоб зменшити трафік мережі передбачено використання 16-розрядних адрес, що призначаються координатором мережі.

Вузли ZigBee мереж, в яких виконання функцій прийому-передачі радіосигналів становить лише одну зі складових повного переліку функціональних властивостей, називають приладами (на відміну від вузлів середньошвидкісних і високошвидкісних WPAN, де по відношенню до одного з елементів вузла використовується поняття пристрій; іншим елементом є хост). Радіотехнологічні аспекти передачі повідомлень, якими

вичерпувались функції пристроїв розглянутих раніше стандартів WLAN і WPAN, в LR-WPAN приладах є лише базовою складовою частиною (рис.2.5), Функції, відповідні верхнім рівням стека протоколів, в ZigBee мережах також виконуються приладами. Розглянуті нижче телекомунікаційні можливості мереж ZigBee в основному обмежуються радіотехнологіческімі аспектами.

2.4 Топологія ZigBee мереж.

Відповідно до можливостей мікроконтролерів приладів, останні поділяють на дві категорії:

— повнофункціональні прилади (Full Functional Devices - FFD);

— обмежено функціональні прилади (Reduced Functional Devices - RFD).

Критерій приналежності приладу до FFD або RFD полягає в повноті їх трансиверів, а роль ZigBee специфікацій - в регламентації взаємодій-наслідком їх мікроконтролерів.

Функцій, які прилад здатний виконувати як елемент мережі.

FFD здатні виконувати функції координатора (Coordinator) мережі - форматувати її створення, асоціювати інші прилади до склада її абонентів, синхронізувати роботу абонентів, «обжити» передавальними ланками ланцюжка передачі повідомлень.

Можливості RFD обмежуються виконавчими функціями - вони можуть бути асоційованими абонентами, але не здатні виконувати функції координатора (зауважимо, що згідно з ZigBee специфікаціям, регламентуючим два верхніх рівня стека протоколів LR-PAN, прилади підрозділяються на 3 категорії: ZigBee координатори - ZC, ZigBee маршрутизатори - ZR і ZigBee кінцеві прилади - ZED; RFD за своїми функціями аналогічні ZED).

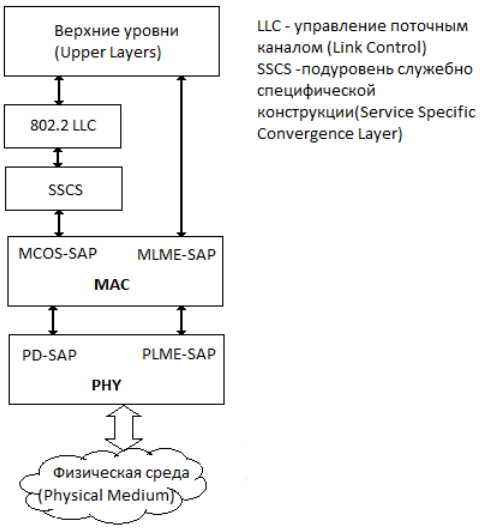


Рисунок 2.5 - Рівнева архітектура протоколів приладів LR-WPAN

3 ОСОБЛИВОСТІ СЕНСОРНИХ МЕРЕЖ

3.1 Топологія типу кластерного дерева

Сенсорні мережі відрізняються від класичних персональних мереж розмірами площі, на якій їх прилади можуть бути розташовані. У класичних WPAN відстань між приладами обмежується сферою персонального радіовпливу (radio sphere of influence, personal operating space) з лінійними розмірами порядку одиниць метрів; завдяки цьому забезпечується прямий (Point- to-Point) зв'язок між приладами. Територія покриття сенсорних мереж може перевищувати розміри сфери персонального радіовпливу, і, відповідно, передача повідомлень між віддаленими абонентами мереж можлива лише за допомогою багаторівневої ретрансляції проміжними вузлами.

ZigBee мережі є здатними до самоорганізації (Ad-Hoc) мережами. Стандартом передбачені дві топології ZigBee мереж, прилади яких розташовані в межах перекриваються сфер персонального радіовпливу:

— топологія типу зірка (рис.3.1) виконує функції її координатора (PAN coordinator). Кінцеві прилади мережі можуть бути повнофункціональними (FFD) або обмежено функціональними (RFD);

— повнозв’язна топологія (Pear-to-Pear Topology), в якій кожен з приладів є повнофункціональним і здатний підтримувати зв'язок з будь-яким іншим приладом. Координована передача повідомлень забезпечується одним з приладів, який іменується координатором PAN (функції координатора може виконати будь-який з приладів).

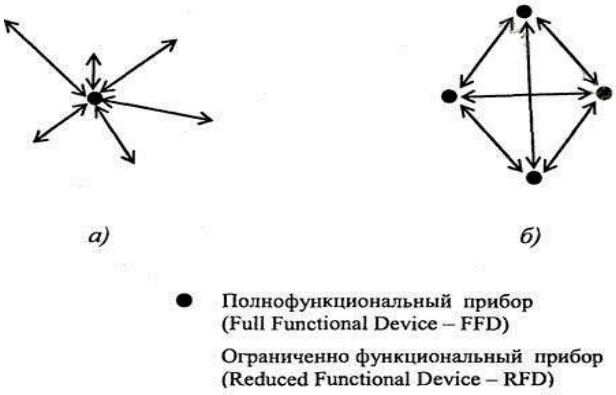


Рисунок 3.1 - Компонування ZigBee мереж з перекриваються сферами персонального радіовпливу приладів: (а) топологія типу зірка; (Б) повнозв’язна топологія

Мережі, в яких сфери персонального радіовпливу окремих приладів територіально розділені, мають топологію типу дерево і кластерне дерево

Топологія типу дерево (Tree Topology) являє собою комбінацію топологій типу зірка (рис. 3.2). Комбінація топологій полягає в ступінчастому (ієрархічному) розгалуженні вихідної «зірки»: кінцеві прилади попереднього ступеня є вершинами «зірок» наступного. Прилад, який утворює вершину всього дерева, є загальним координатором мережі (ZigBee Coordinator); прилади, відповідні проміжним вершинам, називаются маршрутизаторами (ZigBee Router).

Маршрутизатор ZigBee є повнофункціональним приладом стандарту IEEE 802.15.4, яке не є координатором ZigBee, але може бути координатором або маршрутизатором повідомлень між ZigBee-приладами і пристроєм, приєднує нові прилади до мережі. Будь-який пристрій стандар¬та IEEE 802.15.4 (RFD або FFD), яка не є ні координатором ZigBee, ні маршрутизатором, називають кінцевим пристроєм (ZigBeeEnd Device).

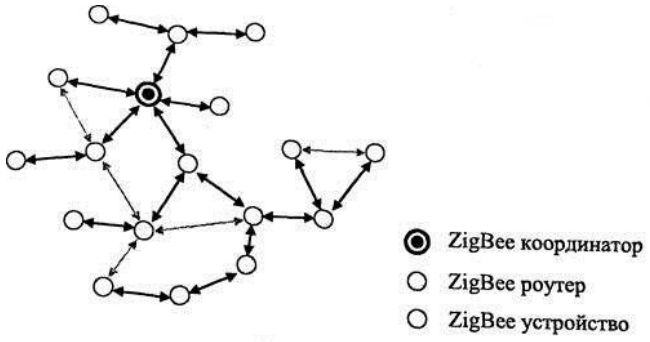


Рисунок 3.2 − Топологія ZigBee мереж типу дерево

3.1.1 Топология типа кластерного дерева

Характеризується тим, що елементами «дерева» є не окремі вузлы мережі, а елементарні мережі, що називаються кластерами (рис.3.3). В кожному з кластерів є координатор мережі (PAN coordinator). Координатор вихідного кластера називається «Першим координатором PAN» (First PAN coordinator). Координатори кластерів нижчих сткпенів зв’язані с FFD-приладами кластерів попередніх (більш високих) ступенів. Кожна мережа при її утворенні привласнює собі умовне ідентифікаційне позначення (PAN Identifier – PAN ID). Кластери розгалуджених мереж мають різні ідентифікатори, що позначаються умовними номерами – PAN ID1,..PAN ID7.

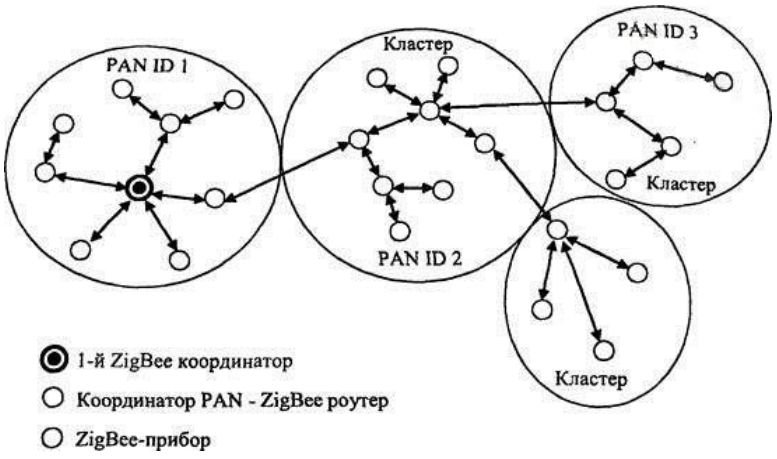


Рисунок 3.3 - Топологія ZigBee мережі типу кластерне дерево

3.1.2 Застосування LR-PAN в промисловості, сільському господарстві та медицині

Припускає, що кількість вузлів сенсорної мережі може бути дуже великим. Стандарт передбачає можливість наявності в мережі до 216 приладів. Важливі споживчі властивості приладів складаються в їх низької вартості і низькому рівні споживаної потужності. Електричне живлення сенсорних вузлів повинно здійснюватися від хімічних джерел живлення без їх заміни протягом тривалого часу (порядку десятків місяців). Прийнятна періодичність моніторингу може бути невисокою (яка обчислюється хвилинами). Це означає, що коефіцієнт заповнення часу передачею повідомлень (Duty Cycle) кожного вузла мережі невеликий, причому його зменшення забезпечує збільшення тривалості беззмінної роботи джерел живлення. Потужність, що споживається вузлами при передачі повідомлень, має величину порядку одиниць і часткою мілівата, а з урахуванням коефіцієнта заповнення споживана середня потужність обчислюється мікроватами.

3.1.3 Застосування бездротових сенсорних мереж

Поряд з їх низькою вартістю і енергоспоживанням стимулюється наявністю інших істотних експлуатаційних властивостей: високою надійністю (Reliability), адаптивністю до умов роботи (Adaptability), зручністю нарощування (Scalability) мережі. Реалізації цих властивостей сприяє гнучкість топології сенсорних мереж.

3.2 Частотний ресурс і частотні характеристики каналів зв'язку ZigBee

Відповідно до призначення ZigBee мереж частотний ресурс, що виділяється для їх застосування, лежить в діапазонах частот, призначених для виробничого, наукового, медичного (ISM) і побутового (Domestic) використання. Для застосування ZigBee приладів передбачається використання трьох діапазонів: 868-868.6 МГц, 902-928 МГц і 2450-2483.5 МГц. Загальна кількість частотних каналів у всіх перерахованих діапазонах становить 27. Розподіл каналів за діапазонами, їх нумерація і сітка використовуваних частот ілюструються даними таблиці 3.1, а також рис. 3.3.

Таблиця 3.1 - Розподіл каналів

Частотний діапазон, МГц	Число частотних каналів	Номера каналів	Крок сітки частот, МГц	Співвідношення, що визначають середні частоти каналів, МГц
868-868.6	1	к=0	—	868.3
902-928	10	J=1,2,…,10	2	f~ 906 + 2
2400-2483.5	16	&=11,12,…,26	5	2405 + 5(*-11)

Загальна риса радіотехнологій каналів всіх трьох використовуваних частотних діапазонів 0-ї канальної «сторінки» полягає в застосуванні радіосигналів з розширеним спектром. Швидкості передачі інформаційних бінарних сігналів (Bit Rate) в каналах різних частотних діапазонів становлять 20, 40 і 250 кбіт / с. Чіпові швидкості розширених по спектру сигналів відповідно дорівнюють 300, 600 і 2500 кбіт / с. Значення коефіцієнтів розширення спектра (Spreading Factor - SF) каналів до - 0-н 10 збігаються (дорівнюють 15); в каналах 3-го діапазону (до = 11-26) SF = 8.

Таблиця 3.2 - Характеристики радіоканалів 0-й канальної сторінки ZigBee

Номера каналів	Бітова швидкість, кбит/с	Символи, що передаються		Роширення спектру		Метод модуляції
		Тип	Символьна швидкість, кс им в/с	Спосіб	Чіповая швидкість, кчип/с	
0	20	Бінарні	20	DSSS	300	DBPSK
1-10	40	Бінарні	40	DSSS	600	DBPSK
11-26	250	16-ричні	62,5	DSSS	2000	OQPSK

Всі пристрої повинні підтримувати унікальні 64-розрядні адреси. Ці адреси використовуються для адресації в межах даної мережі. Щоб зменшити трафік мережі передбачено використання 16-розрядних адрес, що призначаються координатором мережі.

У стандарті також визначено опціональне використання суперструктури (superframe). Вона визначається координатором і зв'язується маяками (beacon). Ці маяки передаються в першому слоті кожної суперструктури. Існує два її види - з активним і неактивним періодами. Протягом неактивного періоду координатор може перейти в малопотужний режим. Якщо використовувати суперструктуру не обов'язково, то координатор перестане посилати маяки. Маяки слугують для синхронізації пристроїв з PAN-координатором під час з'єднання. Будь-який пристрій, що бажає зв'язатися протягом CAP (період доступу), конкурує з іншими пристроями, використовуючи CSMA-CA механізм. Усі транзакції завершуються до наступного маяка. Для додатків, що вимагають низький рівень очікування або вимагають пропускну здатність для специфічних даних, координатор виділяє спеціальні суперструктури - гарантовані тимчасові слоти (GTS). GTS формується у вільний період (CFP), який завжди з'являється в кінці активної суперструктури, після CAP.

Згаданий механізм CSMA-CA працює за принципом прослуховування частот протягом певного часу і виявлення вільної частоти для передачі даних. Якщо канал зайнятий, то вузол «відсторонюється» і чекає певний час, перш ніж знову почати спробу відправки пакета. Уникнення колізій використовується для того, щоб поліпшити продуктивність CSMA, віддавши мережу єдиному передавальному пристрою. Ця функція покладається на «стислий сигнал» в CSMA / CA. Поліпшення продуктивності досягається за рахунок зниження ймовірності колізій і повторних спроб передачі. Але очікування «стисненого сигналу» створює додаткові затримки, тому інші методики дозволяють досягти кращих результатів.

Модель пересилання даних містить в собі три види транзакцій. Перший вид - передача даних координатору, другий - передача від координатора, третій вид - передача між рівними пристроями. У топології типу «зірка» застосовується тільки перші два види транзакцій, так як дані йдуть між координатором і пристроєм. У топології «рівноправних вузлів» можливі всі три види транзакцій.

Пересилання даних координатору відбувається в наступному порядку:

— пристрій шукає маяк, що посилається координатором. Коли маяк знайдений, пристрій синхронізується;

— далі в певний момент часу (за механізмом CSMA-CA) відправляються самі дані;

— отримавши дані, координатор відправляє пристрою підтвердження про успішний прийом даних.

У разі, якщо маяк не використовується, дані відразу пересилаються координатору за механізмом CSMA-CA. При отриманні даних він також відправляє підтвердження (рис.3.4).

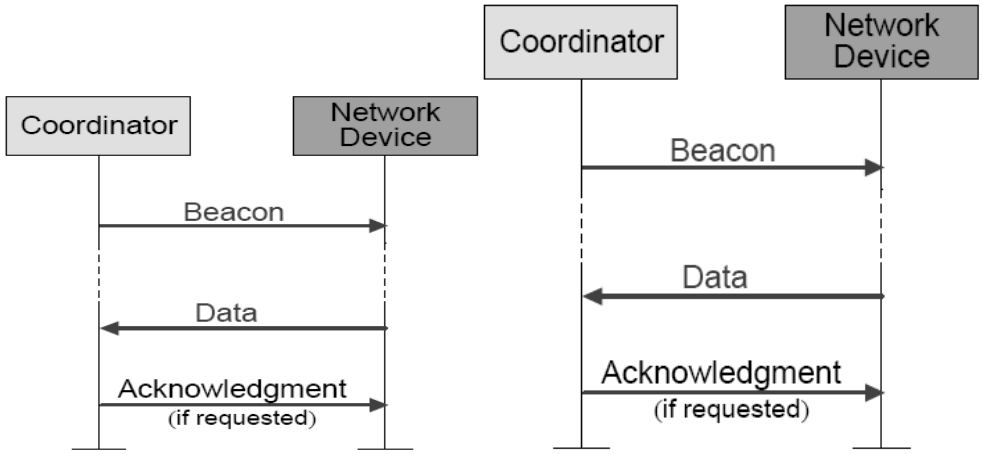


Рисунок 3.4 - Схема передачі даних координатору з використанням і без використання маяка

Пересилання даних від координатора (рис. 3.5):

— координатор інформує пристрій в маяку про наявність даних;

— пристрій, отримавши маяк, відправляє MAC команду запиту даних;

— у відповідь координатор відправляє підтвердження про успішний прийом;

— відразу за підтвердженням пересилаються самі дані;

— по прибуттю даних пристрій відправляє координатору підтвердження про успішне отримання.

Якщо маяк не використовується, то координатор накопичує дані і при отриманні запиту від пристрою відправляє їх.

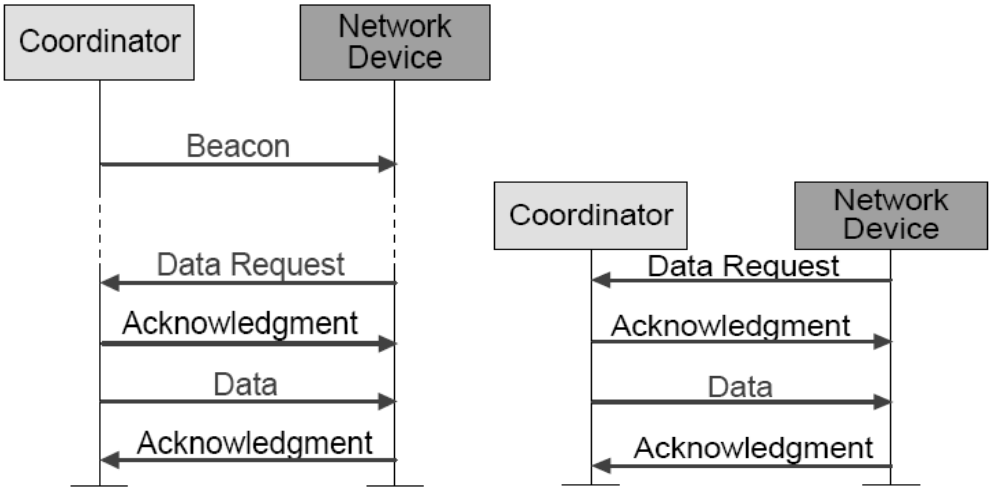


Рисунок 3.5 − Схема передачі данних від координатора з використанням та без використаня маяка

Під час передачі даних між рівноправними пристроями дані можуть передаватися, як і в перших двух випадках, після синхронизації.

Стандартом визначається чотири типи пакетів:

— сигнальний пакет (beaconframe), який використовуєтья координатором, щоб передаваи маяки;

— пакет даних (dataframe), який використовуєтья для передачі данних;

— пакет підтвердження (acknowledgmentframe), який використовується для підтвердження успішного прийому;

— командний пакет, який використовується для управління об'єкта MAC.

Сигнальний пакет має наступну структуру (рис. 3.6).

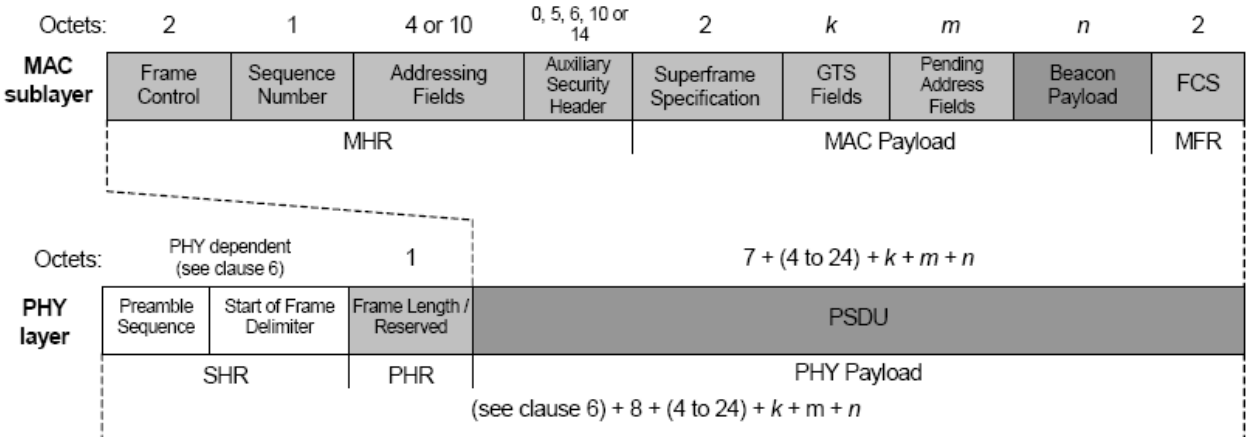


Рисунок 3.6 - Структура сигнального пакета

Пакет даних має наступну структуру (рис. 3.7).

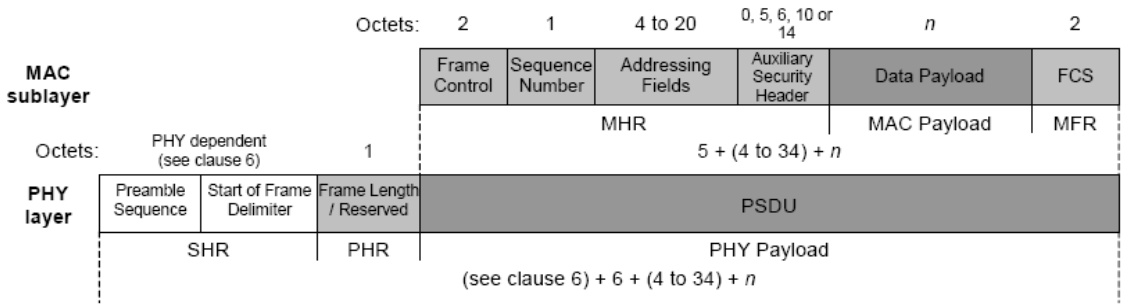


Рисунок 3.7 - Структура сигнального пакета

Пакет підтвердження має наступну структуру (рис. 3.8).

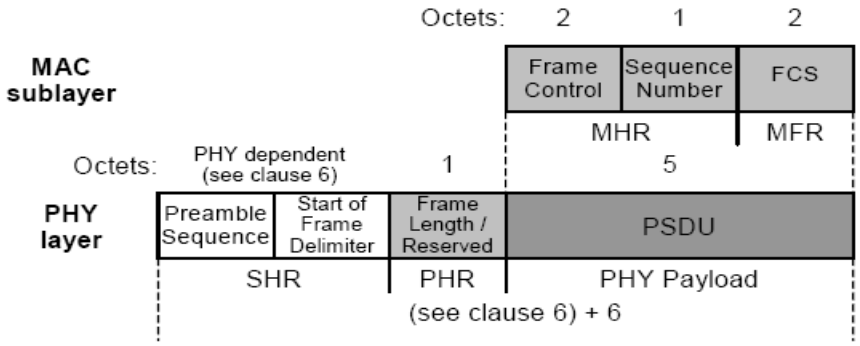


Рисунок 3.8 - Структура пакета підтвердження

Командний пакет має наступну структуру (рис. 3.9).

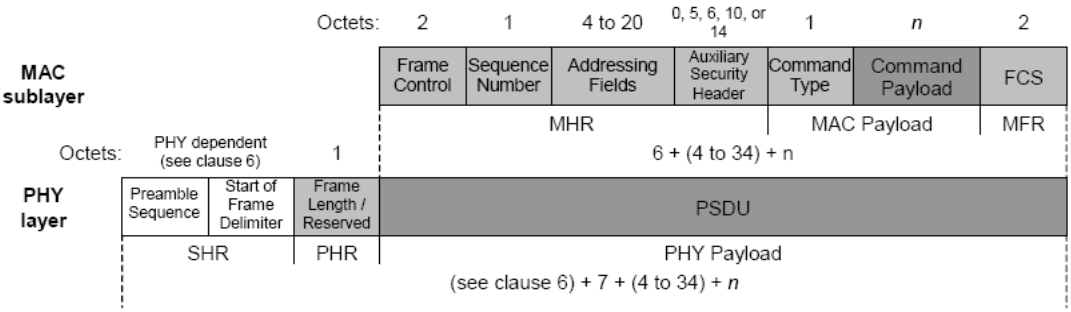


Рисунок 3.9 - Структура командного пакета

Для перевірки цілісності пакету в ньому міститься так звана контрольна сума (16-бітове поле FCS). Алгоритм обчислення контрольної суми носить назву циклічного надлишкового коду (CRC). Для отримання контрольної суми, необхідно згенерувати поліном G (x). Основна вимога до поліному: його ступінь повинна дорівнювати довжині контрольної суми в бітах. При цьому старший біт полінома обов'язково має дорівнювати

«1». З файлу береться перше слово. Якщо старший біт в слові "1", то слово зсувається вліво на один розряд з подальшим виконанням операції XOR. Відповідно, якщо старший біт в слові "0", то після зсуву операція XOR не виконується. Після зсуву (множення) втрачається старий старший біт, а молодший біт звільняється (обнуляється). На місце молодшого біта завантажується черговий біт з файлу. Операція повторюється до тих пір, поки не завантажиться останній біт файлу.

Після проходження всього файлу, в слові залишається залишок, який і є контрольною сумою.

В даному стандарті 802.15.4 передбачається захист даних за допомогою симетричних ключів шифрування. Криптографічний механізм передбачає:

— конфіденційність даних (передана інформація відома тільки тим, кому вона призначена);

— справжність даних (захист від зміни даних в дорозі);

— дублювання даних (повторна передача даних).

3.3 Ефективна швидкість передачі даних

У стандарті 802.15.4 для частот в діапазоні 2,4 ГГц визначена максимальна швидкість передачі 250 Кбіт / с. На практиці вона виявляється менше через додаткові службові полія, які включені в кожен переданий пакет. У стандарті визначено алгоритм доступу до середовища передачі даних CSMA / CA.

Розрахуємо час, витрачений на підготовку до передачі даних:

а) Кожен раз, коли пристрій передає дані, воно чекає випадковий проміжок часу з діапазону $[0,2^{BE}-1]$, після чого визначає зайнятість каналу (CCA). Якщо канал вільний, пристрій передає дані, інакше він знову чекає випадковий проміжок часу. Зазвичай показник BE встановлюється рівним 3, тому в самому гіршому випадку час, витрачений на підготовку до передачі, дорівнюватиме:

$$InitialBackOffPeriod + CCA = (2^3 - 1) \cdot aUnitBackOffPeriod + CCA = 7 \cdot 0{,}32 + 0{,}128 = 2{,}368$$

мс.

Час CCA дорівнює 8 символьним періодам, час aUnitBackOffPeriod дорівнює 20 символьним періодам, 1 символьний період дорівнює 16 мкс.

Тепер розглянемо необхідний час на передачу даних:

б) Відповідно до стандарту 802.15.4 максимальний розмір корисного навантаження фрейма дорівнює:

$$aMaxMACFrameSize = aMaxPHYPacketSize - aMaxFrameOverhead, \quad (3.1)$$

де $aMaxFrameOverhead = 25$, $aMaxPHYPacketSize = 127$.

Як видно, розмір корисної частини залежить від довжини службових полів. Пізніша версія стандарту 802.15.4b дозволяє збільшити корисне навантаження фрейму, коли використовуються короткі адреси (16 біт замість 64). У цьому випадку обсяг даних буде дорівнює 114 байтам.

Таким чином, час передачі даних складе:

$$\frac{(aMaxPHYPacketSize + SHR + PHR) \cdot 8}{250 \cdot 10^3} = \frac{(127 + 5 + 1) \cdot 8}{250 \cdot 10^3} = 4{,}256 \text{ мс.} \quad (3.2)$$

в) Після відправки пакета даних необхідно відправити кадр підтвердження. Кадр підтвердження прийому даних складається з 11 байт. Якщо прийняти швидкість на вході 250 Кбіт / с, то передача займе 0,352 мс. Слід зазначити, що при передачі підтверджень не використовується алгоритм вирішення конфліктів CSMA-CA.

Перед відправкою підтвердження є затримка в 192 мкс, пов'язана з тим, що пристрій має перейти з режиму прийому в режим передачі. Крім того, щоб дати пристроям достатньо часу на обробку отриманих даних, в стандарті визначені мінімальні затримки, які слідують після кадру підтвердження:

— для кадрів довжиною до 18 байт включно - 18 символьних періодів;

— для кадрів довжиною понад 18 байт - 40 символьних періодів.

Як правило, ці затримки охоплюються при підготовці до передачі чергового кадру даних.

Використовуючи наведені вище розрахунки, визначимо ефективну швидкість передачі по стандарту 802.15.4:

Таблиця 3.3 - Часові витрати

Дія	Час (в мс)
CSMA/CA	2,368 мс
Передача кадра	4,256 мс
Затримка після передачі	0,192 мс
Передача підтвердження	0,352 мс
Загальний час (Ту)	7,168 мс

Ефективна швидкість: $\frac{V}{T_{\Sigma}} = \frac{114 \cdot 8}{7{,}168 \cdot 10^{-3}} = 127$ Кбіт / с.

3.4 Розрахунок енергоспоживання і часу роботи

Енергоспоживання - один з ключових питань для сенсорних мереж, так як пристрої живляться в основному від батарейок.

Інформація про споживання енергії в різних режимах взята з технічного опису мікроконтролерів компанії Jennic, що виробляє готові модулі по стандарту 802.15.4.

Таблиця 3.4 - Енергоспоживання мікроконтролера фірми Jennic.

Режим	Споживання струму, мА
Активний	12
Режим сну	0,003
Передача	125
Прийом	45

Таблиця 3.4 показує, що сенсор в базовому (активному) режимі споживає приблизно в кілька тисяч разів більше енергії, ніж в режимі сну. Відправлення повідомлень збільшує енергоспоживання в порівнянні з базовим режимом. Цілком природно, що співвідношення між показниками може відрізнятися для різних виробників. Але в будь-якому випадку очевидно те, що сплячий режим вимагає найменшої кількості енергії.

Час активності пристрою за один раз складає 16мс. 3мс витрачається на передачу зібраних даних і стільки ж витрачається на їх прийом. Час підготовки до передачі даних становить приблизно 2 мс. Таким чином, один цикл складає 24мс.

Тепер необхідно розрахувати скільки разів в секунду буде пристрій працювати в активному режимі, в режимі прийому і в режимі передачі: 1000/24 = 41 разів. Час, що залишився 16мс пристрій буде збирати дані для передачі.

У стандарті 802.15.4 зазначено максимальну швидкість передачі даних 250 Кбіт / с. Реальна швидкість, яка була розрахована вище, дещо менше, оскільки кадри мають певний формат, що включає в себе адреси приймача і передавача і деякі інші поля. Зробимо розрахунок для обох швидкостей.

Мікроконтролер може занурюватися в режим сну, при якому струм споживання є мінімальним. Даний режим застосовується в сенсорах для більш тривалого терміну служби батареї, а, отже, і великим часом роботи пристрою, однак, в нашому випадку, пристрій не

може переходити в режим сну при роботі на прийом, передачу і при формуванні даних. Тому розрахунки будуть проводитися виходячи з цих трьох режимів.

Розрахуємо середнє споживання струму за час t = 1с. Воно дорівнюватиме:

$$I_{\text{ср}} = \frac{0{,}016 \cdot 12 \cdot 42 + 0{,}003 \cdot 125 \cdot 41 + 0{,}003 \cdot 45 \cdot 41 + 0{,}002 \cdot 12 \cdot 41}{1} = 29{,}96 \text{ мА} \qquad (3.3)$$

Припустимо, для живлення сенсорної плати використовуються дві батарейки АА. Ємність кожної батарейки приблизно дорівнює 2122 мАг. Тоді пристрій буде працювати протягом: $t_p = \frac{2 \cdot 2122}{29{,}96} = 141$ годину або 5 днів і 21 годину.

Для розрахованої швидкості отримуємо:

$$I_{\text{ср}} = \frac{0{,}016 \cdot 12 \cdot 33 + 0{,}006 \cdot 125 \cdot 33 + 0{,}006 \cdot 45 \cdot 33 + 0{,}002 \cdot 12 \cdot 33 + 0{,}01 \cdot 12}{1} = 40{,}91 \text{ мА} \quad (3.4)$$

$t_p = \frac{2 \cdot 2122}{40{,}91} = 103$ години або 4 дня і 7 годин.

Неважко помітити, що основна енергія витрачається при передачі даних. Якщо зробити можливість відходу пристрою в сплячий режим, то, відповідно, отриманий час роботи tp буде значно більшим.

Якщо порівняти час роботи даного пристрою з часом роботи аналогів, то неважко помітити, що воно значно перевищує його, і тому система, побудована з таких пристроїв, може стати конкурентоспроможною на ринку радіозв'язку.

Були розглянуті різні стандарти малопотужних бездротових мереж. Найбільш перспективним є стандарт IEEE802.15.4-2006. Виходячи з специфікацій даного стандарту була визначена ефективна швидкість передачі даних, споживання струму і час роботи пристроїв при заявленій і розрахованої швидкостях передачі даних.

4 ОГЛЯД ЗАСОБІВ МОДЕЛЮВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

У цьому розділі розглянуто шість основних інструментів моделювання, що використовуються в БСМ: NS-2, TOSSIM, Emstar, Castalia, J-Sim, ATEMU, і проаналізовані переваги і недоліки кожного інструменту моделювання.

Система NS-2 розроблена в 1989 році, використовується в якості симулятора реальної мережі. NS-2 є дискретно-подієвим симулятором, побудований в об'єктно-орієнтованому стилі. Розроблений на мові C ++. Працює на операційній системі Linux. Може використовуватися як для дротових, так і для бездротових мереж. Це система з відкритим вихідним кодом.

Переваги, по-перше, як неспецифічний для БСМ симулятор, NS-2 може підтримувати значний спектр протоколів у всіх шарах. Наприклад, спеціальні та конкретні протоколи БСМ надаються NS-2. По-друге, модель відкритого вихідного коду економить витрати на моделювання, і електронні документи дозволяють користувачам легко змінювати і покращувати систему.

Проте, цей симулятор має деякі обмеження. По-перше, люди, які хочуть використовувати цей симулятор мають бути знайомі з написанням програм на скриптових мовах. По-друге, іноді використання NS-2 є більш складним і трудомістким, ніж інших систем моделювання. По-третє, NS-2 забезпечує погану графічну підтримку, без графічного інтерфейсу користувача (GUI).

Система TOSSIM є емулятором, спеціально призначеним для БСМ, що працюють на TinyOS, який поширюється з відкритим вихідним кодом. Розроблено в 2003 році. Написаний на мові Python і C ++. Працює в операційній системі Linux. TOSSIM також поширюється в вихідному коді.

До переваг відноситься швидкість емуляції. Крім того, TOSSIM має графічний інтерфейс, TinyViz, що дуже зручно для того, щоб взаємодіяти з електронними пристроями, оскільки вона забезпечує зображення замість тексту команд.

Крім того, TOSSIM є дуже простим, але потужним емулятором для БСМ. Кожен вузол може бути оцінений в ідеальних умовах передачі, і за допомогою цього емулятора можна досліджувати приховані проблеми. Може підтримувати тисячі вузлів. Проте цей емулятор має деякі обмеження. По-перше, TOSSIM призначений для моделювання поведінки і застосування TinyOS, і він не призначений для імітації показників інших нових протоколів. Тому TOSSIM не може правильно моделювати питання енергоспоживання в БСМ; можна використовувати PowerTOSSIM, інший симулятор TinyOS. По-друге, кожен

вузол повинен працювати на Nesc коді - мовою програмування, який управляється подіями на основі компонентів і реалізований на TinyOS. По-третє, TOSSIM розроблений спеціально для моделювання тільки вузлів.

Система Emstar є емулятором, спеціально призначеним для БСМ. Побудований на мові С. Працює на операційній системі Linux. Цей емулятор підтримує розвинені можливості по роботі з апаратними датчиками.

До переваг відноситься, по-перше, модульна модель програмування. Вона дозволяє користувачам запускати кожен модуль окремо без шкоди для повторного використання програмного забезпечення. Emstar має графічний інтерфейс, який може бути дуже корисним для користувачів, для управління електронними пристроями. Проте, цей емулятор містить деякі недоліки. Наприклад, він не може підтримувати велику кількість вузлів і датчиків і обмежену масштабованість в результаті. Крім того, Emstar може працювати тільки в режимі реального часу.

Castalia є подієво-дискретним симулятором. Написаний на C ++. Castalia поширюється по некомерційної ліцензії для використання в навчальних закладах або некомерційних дослідницьких організаціях, а також під комерційною ліцензією. Цей симулятор подделжівает написання модулів користувачем. Працює в операційній системі Linux, Unix-подібних операційних системах. Castalia є популярною системою моделювання БСМ. Більшість вихідного коду может бути доступно в початковому вигляді.

До переваг відноситься те що, по-перше, Castalia забезпечує потужні засоби трасування та налагодження. Підтримуються широкі можливості роботи з радіоканалом, підтримує багато MAC протоколи. Крім того, Castalia може імітувати проблеми енергоспоживання в БСМ. Проте, існують деякі обмеження. Наприклад, кількість доступних протоколів не є достатньо великим.

Система J-SimSim є дискретно-подієвим симулятором. Написаний на Java. Є графічний інтерфейс. Поширюється в вихідному коді. Зазвичай використовується в фізіології і галузі біомедицини, але також може бути використаний для моделювання БСМ. Крім того, J-Sim може імітувати процеси в реальному часі.

Переваги, по-перше, в моделі J-Sim є можливість повторного використання і взаємозамінності компонентів. По-друге, J-Sim містить велику кількість протоколів. По-третє, J-Sim надає графічний інтерфейс, який може допомогти користувачам відстежувати і налагоджувати програми. По-четверте, в порівнянні з NS-2 J-Sim може імітувати велике число вузлів датчиків, близько 500 і J-Sim може заощадити багато оперативної пам'яті. Проте, цей симулятор має деякі обмеження. Час виконання набагато більше, ніж у NS-2. Оскільки J-Sim спочатку не призначені для моделювання БСМ.

Система ATEMU. Побудований на C; заточений під платформу MICA. ATEMU надає графічний інтерфейс. Працює в операційних системах Solaris і Linux. Поширюється в вихідному коді. Переваги, по-перше, ATEMU може імітувати кілька датчиків на вузлі. По-друге, ATEMU має велику бібліотеку готових пристроїв. По-третє, ATEMU може забезпечити дуже високий рівень деталізації емуляції БСМ. По-четверте, графічний інтерфейс може допомогти користувачам в налагодженні і моніторингу реалізації моделі. Проте, цей емулятор також має деякі обмеження. Наприклад, хоча ATEMU може дати високу точність результатів, час моделювання набагато довше, ніж інших інструментів моделювання. Крім того, ATEMU має менше функцій для моделювання маршрутизації.

Розглянуто шість основних систем імітаційного моделювання БСМ: NS-2, TOSSIM, Emstar, Castalia, J-Sim, ATEMU. Результати сравнівненія їх достоїнств і недоліків наведені в таблиці 4.1. Вибір системи варто проводити в залежності від цілей дослідження, вибираючи більш ефективну для конкретного випадку.

Таблиця 4.1 - Порівняння шести основних систем моделювання БСМ

Система	Дискретно-подієва система, інакше заснована на трассировці	Графічний інтерфейс користувача	Поширюється в вихідному коді	Спеціально призначений для БСМ, інакше загальний	Особливості
NS-2	Так	Ні	Так	Ні	1) не більше 100 вузлів, 2) не може імітувати проблеми пропускної здатності або споживання електроенергії в БСМ
TOSSIM	Так	Так	Так	Так	1) близько тисячі вузлів, 2) тільки однорідні додатки
Emstar	Ні	Так	Так	Так	1) не підтримує велику кількість вузлів, 2) працює тільки в режимі реального часу і тільки вузли MICA2
Castalia	Так	Так	Некомерційна і комерційна ліцензія	Так	1) підтримка протоколів MAC, 2) симуляція споживаної потужності і канали, 3) розширена емуляція радіоканалу

Продовження таблиці 4.1

Система	Дискретно-подієва система, інакше заснована на трассировці	Графічний інтерфейс користувача	Поширюється в вихідному коді	Спеціально призначений для БСМ, інакше загальний	Особливості
J-Sim	Так	Так	Так	Ні	1) може імітувати велику кількість вузлів датчиків, близько 500, 2) може імітувати радіоканали і споживану потужність, 3) час його роботи набагато більше
ATEMU	Так	Так	Так	Так	1) може емулювати різні вузли в однорідних мережах або гетерогенних мережах, 2) симуляція споживаної потужності і радіоканалів, 3) час моделювання набагато довше

У зв'язку з великими можливостями моделювання (в тому числі радіоканалу) в подальшому будемо використовувати систему Castalia.

Castalia є системою моделювання для бездротових сенсорних мереж і взагалі мереж малопотужних вбудованих пристроїв. Вона заснована на платформі OMNeT ++ [2,3] і може бути використана дослідниками і розробниками, які хочуть випробувати свої алгоритми і / або протоколи в реалістичній середовищі бездротового каналу з розширеною радіо моделлю, з реалістичною поведінкою вузла. Castalia також може бути використана для оцінки різних характеристик платформи для конкретних додатків, так як вона дуже гнучка в налаштуванні і може імітувати широкий діапазон платформ. Основними рисами Castalia є [3]:

1. Удосконалена модель каналу на основі емпіричних даних вимірювань:

— модель системи враховує втрати в каналі передачі даних, а не просто з'єднань між вузлами;

— комплексна модель для зміни втрат в каналі;

— повністю підтримує рухливість вузлів;

— перешкоди враховуються вже на рівні сигналу, а не у вигляді окремої функції.

2. Удосконалена модель радіо на основі на реальних малопотужних радіо пристроїв зв'язку:

— ймовірність отримання залежить від SINR, розміру пакета, типу модуляції. Модуляції PSK, FSK підтримуються, призначені для користувача модуляції можуть бути визначені шляхом завдання SNR-BER кривої;

— можуть задаватися кілька рівнів потужності передачі з індивідуальними варіаціями;

— стану з різним енергоспоживанням і затримками перемикання між ними підтримуються;

— реалістичне моделювання RSSI несучої;

— розширене моделювання вимірювальних пристроїв;

— дуже гнучка фізична модель процесу вимірювання;

— підтримка шумів, зсувів і споживання енергії для вимірювального пристрою;

3. MAC протоколи доступні.

4. Призначена для адаптації і розширення.

Що стосується останнього пункту, Castalia була розроблена з самого початку так, що користувачі можуть легко реалізувати / імпортувати свої алгоритми і протоколи в той час як Castalia бере на себе особливості моделювання. Модульність, надійність і швидкість Castalia частково заслуга OMNeT ++, яка лягла в основу Castalia.

Castalia не є орієнтованою на конкретну платформу. Castalia забезпечує загальний надійний і реалістичний спосіб перевірки алгоритму перш, ніж перейти до реалізації на конкретній платформі і використовує OMNeT ++ в якості своєї бази тому передбачається, що у вас є чітке розуміння основних понять OMNeT хоча це і не потрібно, особливо, якщо ви хочете використовувати Castalia без створення власних протоколів / додатків. Заснований на поняттях модулів і повідомлень. Простий модуль є основною одиницею виконання. Він приймає повідомлення від інших модулів або безпосередньо і в Відповідно до повідомлення виконує частину коду. Цей код може зберігати стан, яке змінюється при прийомі повідомлень і може відправити нові повідомлення. Є також складові модулі. Складовий модуль - просто спосіб побудови простих і / або інших композитних модулів.

Вузли не з'єднуються один з одним безпосередньо, а через модуль бездротового каналу. Стрілки вказують на те передачу повідомлень від одного модуля до іншого. Коли вузол має пакет для відправки, то він переходить в бездротовоий канал, який потім вирішує які вузли повинні отримувати пакет. Вузли також пов'язані через фізичні процеси, які вони контролюють. Для кожного фізичного процесу є один модуль. Вузли взаємодіють з

фізичним процесом в просторі і часі (шляхом відправки повідомлення на відповідний модуль), щоб отримати показники датчиків. Там може бути кілька фізичних процесів, що представляють кілька датчиків.

Модуль вузла є складовим. Суцільні стрілки означають передачу повідомлень і пунктирні стрілки означають просто викликаються функції. Наприклад, більшість з модулів викликають функції менеджера ресурсів, щоб сигналізувати, що енергія витрачена. Castalia пропонує підтримку для створення призначених для користувача протоколів і додатків, визначаючи відповідні абстрактні класи. Всі існуючі модулі добре настроюється за багатьма параметрами.

Опис модулів здійснюється з використанням мови OMNeT ++ NED. За допомогою цієї мови можна легко визначити модулі, тобто визначити ім'я модуля, параметри модуля і модуля інтерфейсу і можливу структуру підмодуля (якщо це композитний модуль). Сам код модуля пишеться на мові C ++.

5 АНАЛІЗ ПРАЦЕЗДАТНОСТІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

В даному розділі описуються моделі надійності для бездротової сенсорної мережі. Проводиться дослідження в системі Castalia.

5.1 Модель надійності бездротової сенсорної мережі

Найбільшого поширення останнім часом отримали бездротові сенсорні мережі, параметри яких регламентуються стандартом IEEE 802.15.4.

Технології побудови бездротових сенсорних мереж визначають їх переваги перед іншими рішеннями в області моніторингу: автономність вузлів, можливість їх розміщення у важкодоступних місцях, мале енергоспоживання, здатність до самоорганізації. До недоліків можна віднести їх меншу надійність, під якою розуміється ймовірність безпомилкової і своєчасної доставки результатів вимірювань на мережеві шлюзи для подальшої обробки.

Надійність бездротових сенсорних мереж визначається багатьма факторами, найбільш істотними з яких є: надійність апаратного і програмного забезпечення вузлів, область розгортання мережі, взаємне розташування вузлів, період регламентного обслуговування мережі, інтенсивність збору і передачі інформації кінцевими вузлами (вузли, оснащені сенсорами і здійснюють вимірювання), розмір переданих пакетів інформації.

Підхід до оцінювання надійності заснований на поданні функціонування бездротової сенсорної мережі як марковського процесу [16,23], і передбачає використання математичної моделі надійності передачі даних між двома вузлами такої мережі, яка, в свою чергу, являє собою композицію моделей надійності вузлів, комунікацій між ними і механізму їх доступу до середовища.

5.2 Модель надійності передачі пакета даних між двома вузлами.

Дана модель може бути описана виразом, кількісно визначаючим ймовірність p_{ij} успішної передачі пакету від і вузла бездротової сенсорної мережі j.

Тут і далі передбачається, що відправка пакетів і вузлом в процесі роботи мережі утворює найпростіший потік подій з інтенсивністю Λ_{oi}, а прийом пакетів цим же вузлом -

найпростіший потік з інтенсивністю Λ_{Ii}, де Ii - безліч вузлів, які можуть передати пакет до адреси і вузла; O_i - безліч вузлів, яким може бути переданий пакет від і (рис.5.1).

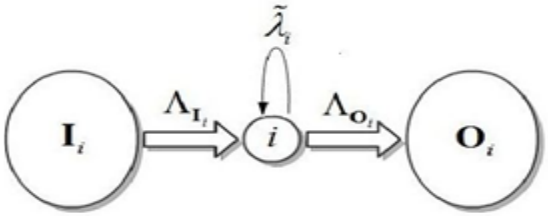


Рисунок 5.1 - Потоки подій на і-му вузлі мережі

Величиною Λ_i на малюнку 5.1 позначена інтенсивність потоку подій, відповідних безуспішним спробам передачі пакетним вузлом. Цю величину можна визначити наступним чином [21]:

$$\tilde{\lambda_i} = \sum_{j \in O_i} (\bar{n}_{ij} - 1)\lambda_{ij} \tag{5.1}$$

де n_{ij} - математичне очікування кількості спроб передачі пакета від і -го вузла j -му, необхідне для успішного його прийому:

$$\bar{n}_{ij} = \sum_{x=1}^{+\infty} x \cdot P_{ij}^{(1)} \left(1 - P_{ij}^{(1)}\right)^{x-1} = \frac{1}{P_{ij}^{(1)}} \tag{5.2}$$

де $p_{ij}^{(1)}$- ймовірність передачі пакета з першої спроби від і вузла j; λ_{ij} - інтенсивність передачі пакетів від і вузла мережі j.

Таким чином, можна записати:

$$\tilde{\lambda_i} = \sum_{j \in O_i} \frac{\lambda_{ij}}{P_{ij}^{(1)}} \tag{5.3}$$

Алгоритм розрахунку ймовірності p_{ij} заснований на одному з можливих принципів роботи механізму маршрутизації в бездротових сенсорних мережах [16]. Нехай на кожному і-му вузлі є обмежена таблиця маршрутизації (визначальна безліч O_i сусідніх з і вузлів, яким їм може бути переданий пакет даних). Записи в цій таблиці ранжовані за перевагою

використання кожного напряму при передачі пакета. Для кожного нового пакета, що надходить на і вузол і потребує подальшої ретрансляції, робиться максимум N_a спроб його передачі j вузлу з безлічі O_i, вказаною першим в таблиці маршрутизації і -го. Якщо всі спроби виявилися невдалими, то з безлічі O_i вибирається j + 1 вузол, відповідний наступному запису в таблиці маршрутизації, і і вузол намагається передати пакет йому, і т.д. Пакет, який до вступу на і вузол наступного пакета не вдалося передати жодному з вузлів, зазначених в таблиці, видаляється з системи (втрачається).

Ємність таблиці маршрутизації, яка визначає потужність безлічі O_i для і -го вузла, як і максимальна кількість повторних спроб передачі N_a не регламентуються стандартами і при побудові мережі можуть бути обрані довільно.

Таким чином, вираз для розрахунку P_{ij} може бути записано таким чином:

$$p_{ij} = Q_j \sum_{k=1}^{N_a} P^{(k)} P_w^{(k)}(\tau_j) \tag{5.4}$$

де Q_j- ймовірність непередання і вузлом пакета тих вузлів, які знаходяться вище j в його таблиці маршрутизації:

$$Q_j = \begin{cases} 1, j = 1 \\ \prod_{z=1}^{j-1}(1 - p_{iz}), j > 1 \end{cases}, j = 1 \dots |O_i| \tag{5.5}$$

N_a - максимальна кількість невдалих спроб передачі пакета одному вузлу; $P^{(k)}$ - ймовірність передачі пакета з k спроби:

$$P^{(k)} = \left(1 - P^{(1)}\right)^{k-1} P^{(1)}, k = 1 \dots N_a \tag{5.6}$$

де $P^{(1)}$ - ймовірність передачі пакета з першої спроби:

$$P^{(1)} = P_{d_j} P_{c_{ij}} \left(1 - P_{h_j}\right) \tag{5.7}$$

де P_{dj} - ймовірність працездатності (надійність) j вузла бездротової сенсорної мережі; P_{cij} - надійність комунікації між вузлами, що визначається параметрами радіоканалу; P_{hj} – ймовірність колізії, обумовленої ефектом «прихованого вузла» [29].

$P_w^{(k)}(\tau_j)$- ймовірність того, що вузол зможе здійснити k спроб передачі пакета за час τ_j. Ця ймовірність визначається механізмом конкурентного доступу до середовища, що використовуються в бездротових сенсорних мережах і регламентованим стандартом IEEE 802.15.4 [11].

Очевидно, що успішна передача пакета може бути здійснена тільки при виконанні умови [23]:

$$\sum_{z=1}^{k} T_{w_z} + kT_L \leq \tau_j \tag{5.8}$$

де T_{wz} - час очікування вузлом початку передачі перед здійсненням z спроби з k можливих, обумовлений конкурентним доступом до середовища;

T_L - час, що витрачається вузлом безпосередньо на процес передачі (прийому) пакета фіксованої довжини L_p байт, $T_L = \frac{L^p}{R}$, де R - швидкість передачі даних, байт / сек;

τ_j - період часу, протягом якого можлива передача чергового пакета і вузлом на адресу j. Величина τ_j різна для кожного j вузла з безлічі O_i (таблиці маршрутизації і вузла) і визначається на основі інтенсивності потоків прийому і передачі пакетів на і вузлі, довжини пакетів, допустимої кількості спроб передачі і середнього часу очікування вузлом можливості виходу в ефір:

$$\tau_j = T_s - (j-1)(\bar{T}_w + T_L)N_a, j \in O_i \tag{5.9}$$

де T_s - середнє значення часу, який може бути витрачено і вузлом на передачу одного з пакетів потоку, що ретранслюються їм:

$$T_s = \frac{1}{\Lambda_{O_i}} - T_L \tag{5.10}$$

де Λ_{oi} - інтенсивність передачі пакетів і -им вузлом на адресу вузлів з безлічі O_i; T_w - середнє значення часу очікування вузлом початку передачі пакету.

Таким чином, вираз для визначення ймовірності можна записати у вигляді:

$$P_w^{(k)}(\tau_j) = P\left(\sum_{k=1}^{k} T_{w_z} \leq \tau_j - kT_L\right) \tag{5.11}$$

де права частина являє собою функцію розподілу сумарного часу очікування вузлом початку передачі, обумовленого конкурентним доступом до середовища, для k спроб.

Далі буде розглянуто опис математичних моделей, які кількісно визначають ймовірності P_{dj}, P_{cij}, P_{hj}, $P_w^k(\tau_j)$.

5.3 Модель надійності вузла

Визначимо регламент обслуговування мережі як регулярний з періодом Tserv контроль і заміну несправних вузлів. Обмеження на надійність вузлів бездротової сенсорної мережі обумовлено розрядом їх батареї в процесі роботи мережі, а також можливістю випадкового виходу їх з ладу, викликаного відмовою апаратного або програмного забезпечення, зовнішніми впливами і т.д. [20,21,23]

Запишемо вираз для визначення ймовірності працездатності j вузла на заданий момент часу t у вигляді [16]:

$$P_{d_j}(t) = \left(1 - Q_{d_j}^{(rnd)}(t)\right) P_{d_j}^{(bat)}(t) \tag{5.12}$$

де $Q_{dj}^{(rnd)}$- ймовірність випадкових відмов j вузла, закон розподілу яких можна в першому наближенні прийняти експоненціальним [21]:

$$Q_{d_j}^{(rnd)} = 1 - e^{-\lambda_f t} \tag{5.13}$$

де λ_f - інтенсивність випадкових відмов. Ця величина вибирається, виходячи з емпіричних міркувань, на основі статистики відмов вузлів в функціонуючих мережах;

$P_{dj}^{(bat)}(t)$- ймовірність працездатності джерела живлення (батареї) вузла. Для опису надійності джерела живлення приймемо спрощену модель, що припускає його рівномірний розряд протягом часу T_{dcj}. Основне споживання енергії вузлом відбувається при активній роботі його приймача або передавача, тому час розряду батареї буде обернено пропорційно довжині пакетів і сукупної інтенсивності їх прийому/передачі $\Lambda_{\Sigma j}$, розрахованої з урахуванням невдалих спроб:

$$T_{dcj} = \frac{T_{dc}^{nom}}{\Lambda_{\Sigma j}\, T_L} \tag{5.14}$$

де $\bar{T}_{dc}^{(nom)}$ - середній час безперервної роботи вузла до розряду батареї при прийомі /передачі даних з максимально можливою щільністю, T_L - час трансляції пакета;

$$\Lambda_{\Sigma_j} = \Lambda_{I_j} + \Lambda_{O_j} + \tilde{\lambda}_j + \sum_{q \in I_j} \tilde{\lambda}_j^{(q)} \tag{5.15}$$

$\tilde{\lambda}_j^{(q)}$ - інтенсивність потоку подій безуспішних передач пакета q вузлом до адреси j вузла, її величина може бути отримана:

$$\tilde{\lambda}_j^{(q)} = \left(\bar{n}_{qj} - 1\right)\lambda_{qj} \tag{5.16}$$

Будемо вважати, що після закінчення часу T_{dcj} з моменту заміни батареї вузол втрачає працездатність з ймовірністю 1. Заміна розряджених батарей вузлів здійснюється з періодичністю Tserv (одночасно для всіх вузлів) [16]. Таким чином, для величини $P_{d_j}^{(bat)}(t)$ можна записати:

$$P_{d_j}^{(bat)}(t) = \begin{cases} 1 \mid \boldsymbol{T_{serv}}\, a \le t \le \left(\boldsymbol{T_{serv}}\, a + T_{dc_j}\right) \\ 0 \mid \left(\boldsymbol{T_{serv}}\, a + T_{dc_j}\right) \le t \le \boldsymbol{T_{serv}}\,(a + b + 1) \end{cases} \tag{5.17}$$

де a - кількість минулих періодів регламентних робіт з початку роботи мережі до останньої заміни джерела живлення, b - кількість повних періодів регламентних робіт, що пройшли з моменту заміни джерела живлення до відмови вузла.

5.4 Модель надійності комунікації між вузлами

У зв'язку з особливостями експлуатації бездротових сенсорних мереж мають місце втрати пакетів через наявність шумів, викликаних як іншими пристроями в конкуруючому діапазоні, так і наявністю власних ехосигналів. Імовірність успішної передачі повідомлення довжиною $L_[$ байт від і вузла j можна визначити з співвідношення: $P_{cij} = (Psij)^{2Lp}$, де P_{sij} - ймовірність безпомилкового прийому символу даних. Залежність P_{sij} від ймовірності бітової помилки може бути отримана шляхом інтерполяції розрахункових значень для діапазону частот в 2.45 ГГц [16], де використовується надлишкове кодування відповідно до стандарту IEEE 802.15.4 [11]:

де P_{bij}- ймовірність бітової помилки, яка може бути визначена з наступного співвідношення:

$$P_{bij} = 2Q\left(\sqrt{\frac{2E_b}{N_0}}\right)\left[1 - Q\left(\sqrt{\frac{2E_b}{N_0}}\right)\right] \tag{5.18}$$

де E_b - енергія біта трансляції, дорівнює добутку потужності на приймальні антени j вузла P_{rx} і тривалості трансляції біта T_b, що визначається швидкістю передачі даних [16];

N_0 - спектральна щільність шумів (її позитивна частина) на приймальній антені j -го вузла, складається не тільки з власних теплових шумів приймача і шумів інших джерел випромінювання (BlueTooth, Wi-Fi, GSM і ін.), але ще й суми луна сигналів [27]; Q(x) - гаусів інтеграл помилок:

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{u^2}{2}}du \tag{5.19}$$

Відношення $\frac{E_b}{N_0}$ можна показати як: $\frac{E_b}{N_0} = T_b W \frac{E_{rx}}{E_N} = \frac{E_{rx}}{E_N} \cdot \frac{W}{R}$, де E_{rx} - амплітуда сигналу, E_N - амплітуда шуму, W - ширина частотної смуги, R - швидкість передачі даних. При W = 5МГц і R = 250Кб/с $\frac{W}{R} = 20$ [16].

Амплітуда сигналу E_{Rx} визначається з наступного співвідношення:

$$E_{RX} = \sqrt{P_{RX} R_{ant}}, \tag{5.20}$$

де R_{ant} - опір антени (50 Ом) [24].

Так як сигнал, з яким синхронізується вузол - це, як правило, прямий (найбільш потужний) сигнал для умови прямої видимості і квазі-сферичності діаграми спрямованості антени, його потужність можна визначити з відомого співвідношення [16]:

де P_{rx}, P_{tx} - потужності прийнятого і випромінюваного сигналу відповідно, d - відстань між вузлами, λ - довжина хвилі (0,125m ≈), K - коефіцієнт посилення каналу зв'язку (0.8 ≈).

Амплітуда шуму E_N є випадковою величиною, і може бути описана розподілом Релея [29], щільність розподілу якого має вигляд:

$$\mathrm{p}(E_N) = \frac{En}{\sigma_r^2} e^{-\frac{E_N^2}{2\sigma_r^2}} \tag{5.21}$$

де параметр цього розподілу $\sigma_r = \sqrt{\frac{E_0 N}{2}}$, залежить від E_0

E_0 - середньої амплітуди шумового сигналу, і N - числа когерентно підсумовуючих сигналів на приймачі. У нульовому наближенні середня амплітуда і число когерентно підсумовуючих променів залежить від розмірів приміщення і його захараченості предметами, що становлять собою «дзеркала» для радіосигналів. Таким чином, приміщення, в якому функціонує сенсорна мережа, може бути охарактеризоване параметром σ_r, який вибирається за допомогою методики, описаної в [16].

5.5 Дослідження надійності передачі пакета даних між двома вузлами в системі Castalia

Розглянемо на практиці надійність передачі пакета даних між двома вузлами. Для простоти розгляду надійності передачі пакета між двома вузлами будемо розглядати бездротову сенсорну мережу з дев'яти вузлів. Будемо вважати, що вузли розташовані в просторі на одній площині в області розміру 30м на 30м. Розташовані по сітці.

Для задання параметрів моделювання в системі Castalia використовуються конфігураційні файли [3] (зазвичай такий файл прийнято називати omnetpp.ini), розташовуватися такий файл повинен в папці даного моделювання (у нас interNodes), яка в свою чергу повинна знаходитися в папці Simulations системи Castalia. Повний текст приведений в додатку А.

Для задання даної просторової конфігурації використовуються параметри: SN.field_x = 30, SN.field_y = 30, SN.numNodes = 9, SN.deployment = "3x3"

Час моделювання задаємо в 100с. (Параметр sim-time-limit = 100s), варто зазначити, що моделювання в системі Castalia відбувається не в реальному часі, тобто реальний час проведення експерименту буде не 100с.

Як вже зазначалося, система Castalia має модульну структуру, так що користувач може створювати власні модулі при необхідності (помістивши їх вихідний код в спеціально призначені для цього папки і проводячи перекомпіляцію системи).

Для моделювання надійності передачі пакета даних між двома вузлами розроблений модуль програми InterNodes, представлений файлами interNodes.ned, interNodes.h, interNodes.cc. Вихідний код приведений в додатку А.

Кожен вузол з інтервалом 100 мс (в додатку заведений відповідний таймер) відправляє повідомлення на широкомовні адреса (рівномірний потік повідомлень утворюється), всього відправляє 100 таких повідомлень.

При цьому у кожного вузла заведена таблиця сусідів, що має структуру. Де id - ідентифікатор вузла, timesRx - кількість пакетів прийшли від нього.

При отриманні повідомлення від вузла, лічильник повідомлень для нього інкрементується (нарощується). Після закінчення моделювання інформація за отриманими повідомленнями заноситься в вихідні дані, щоб їх можна було проаналізувати.

В налаштуваннях моделювання вказуємо додаток (параметр SN.node [*]. ApplicationName = "interNodes")

Відзначимо, що для ідеалізації комунікаційного середовища між вузлами відключимо параметри, що відповідають за перешкоди каналу (параметр SN.wirelessChannel.sigma = 0).

Система Castalia дозволяє у файлі з параметрами моделювання задавати різні конфігурації (різнитися будуть значеннями параметрів). Кожна конфігурація задається секцією, які поділяються ім'ям секції в квадратних дужках. Конфігурація General (задається [General]) є обов'язковою.

Для запуску моделювання використовується команда Castalia. На рисунку 5.2 представлений запуск моделювання з конфігурацією General і висновком в файл res.txt. Як видно, моделювання не зайняло багато часу.

Рисунок 5.2 - Запуск моделювання в системі Castalia

Для обробки даних і отримання результатів в системі Castalia використовується команда CastaliaResults. На рисунку 5.2 виводиться загальна інформація про зібрані в ході моделювання даних, збережених у файлі res.txt. Кожен модуль системи може збирати різні дані. У нашому модулі Application збирали дані про отримані пакетах від сусідів і записували як Packets received. Величина Dimensions характеризує скільки вузлів і дані якої розмірності писали.

На рисунку 5.3 показано, що в середньому кожен вузол отримав 88 пакетів. Таким чином видно, що в ідеальних умовах комунікаційного середовища не всі пакети були отримані, тобто можемо говорити про надійність зв'язку між вузлами з певною ймовірністю.

Рисунок 5.3 - Висновок загальних відомостей про результати моделювання в системі Castalia

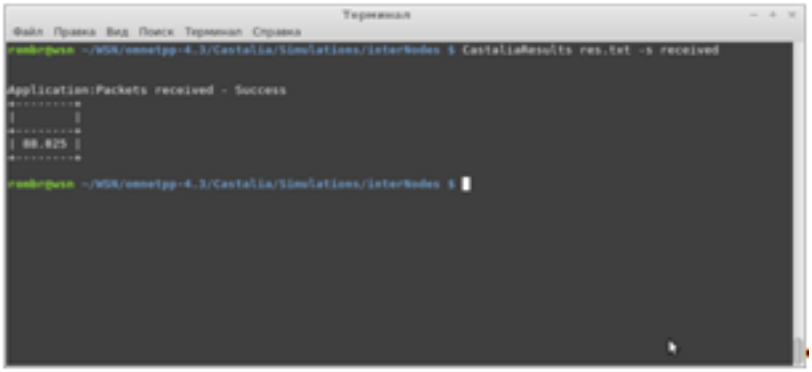


Рисунок 5.4 - Середнє число пакетів отриманих кожним вузлом

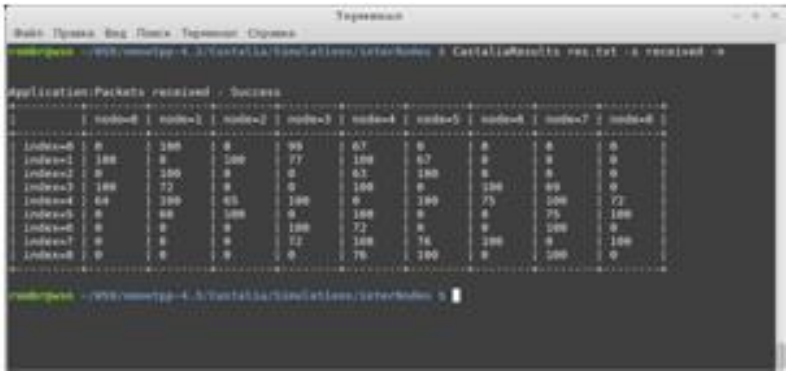


Рисунок 5.5 - Число пакетів отриманих кожним вузлом

На рисунку 5.5 показано скільки пакетів отримав кожен вузол від інших. Стовпці представляють вузли, а рядки записи з таблиць сусідів, дані якої були записані в висновок після закінчення моделювання.

Послідовно проводячи моделювання можна помітити, що результати його будуть відрізнятися, що обумовлено випадковим характером багатьох чинників. Можна повторювати багаторазово моделювання для зниження похибки. Система Castalia дозволяє

проводити повтор моделювання заданий число раз з допомогу опції -n <число повторень>. При цьому результати беруться середні.

Провівши наше моделювання сто раз, на рисунку 5.6 видно, що в цілому отримані дані практично ідентичні тим, що були отримані без багаторазового повторення. Тому докладніше розглянемо перші.

Кожен стовпець являє собою вузол, а рядки відповідають числу пакетів, отриманих від конкретного вузла. Наприклад, видно, що третій вузол отримав від другого вузла 100 пакетів, від п'ятого вузла 65 пакетів, від шостого вузла 100 пакетів і нічого не отримав від інших вузлів.

Так як кожен вузол відправив по 100 пакетів, можемо говорити про ці числа спрощено як ймовірності доставки повідомлень між вузлами.

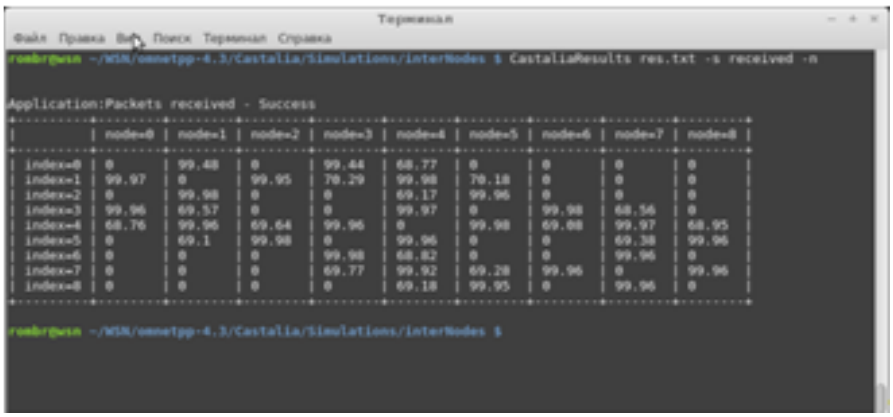


Рисунок 5.6 - Кількість пакетів отриманих вузлами при стократному повторенні моделювання

Дана таблиця може бути інтерпретована як матриця суміжності з вагами.

Таким чином, розглянута модель надійності передачі пакетів між двома вузлами в середовищі без перешкод.

5.6 Вплив перешкод на надійність комунікаційного середовища між двома вузлами в системі Castalia

Розглянемо тепер випадок, коли є проблеми із перешкодами.

Перешкодою називається стороннє обурення, що діє в системі передачі і перешкоджає правильному прийому сигналів [24,29].

Джерела перешкод можуть перебувати як зовні, так і всередині самої системи передачі. Прикладами зовнішніх перешкод можуть служити предмети, що перешкоджають проходженню сигналу, атмосферні явища; приклади внутрішніх - збої пристрою.

Величина перешкод в системі Castalia задається параметром SN.wirelessChannel.sigma, а сама величина перешкод розраховується за формулою [3]:

$$PL(d) = PL(d_0) + 10 \cdot \eta \cdot \log\left(\frac{d}{d_0}\right) + X_\sigma \qquad (5.22)$$

де, PL(d) втрати передачі на відстань dd, PL (d_0) є відомим значенням втрати на початковому відстані $d_0 d_0$, ηη - показник втрат, і X_σ є випадковою величиною зі стандартним відхиленням σσ. Саме за допомогою неї в системі можна змінювати величину перешкод.

Для розгляду впливу перешкод визначили в налаштуваннях моделювання конфігурацію varySigma, при якій буде запущено моделювання (рис 5.7) з варіацією цього параметра (SN.wirelessChannel.sigma = $ {Sigma = 0,1,3,5})

На рисунку 5.7 видно, що зі збільшенням параметра sigma ймовірність доставки пакета зменшується, а значить і надійність, проте ж різкого зростання зниження надійності немає.

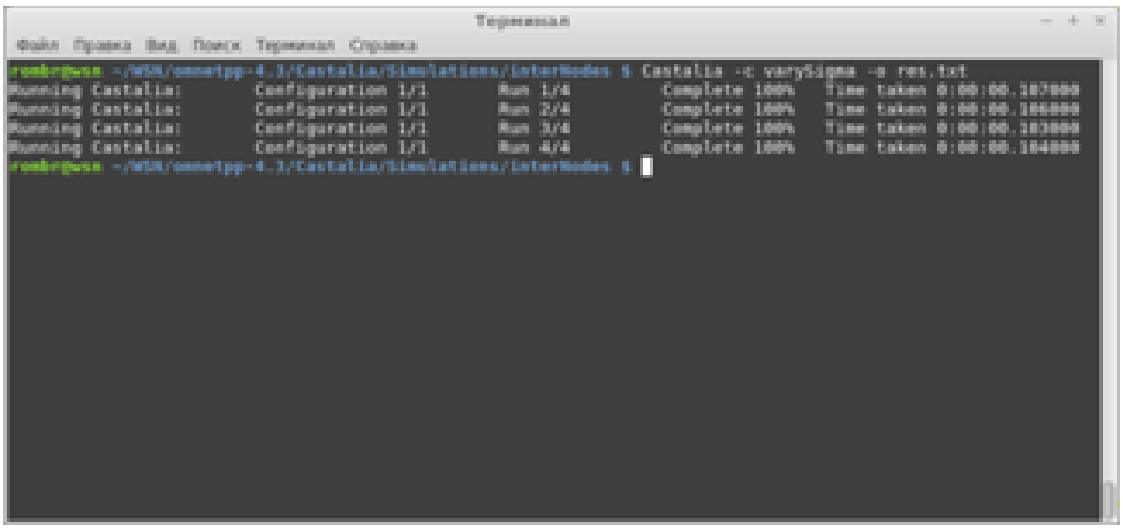


Рисунок 5.7 - Моделювання з варіаціями рівня перешкод

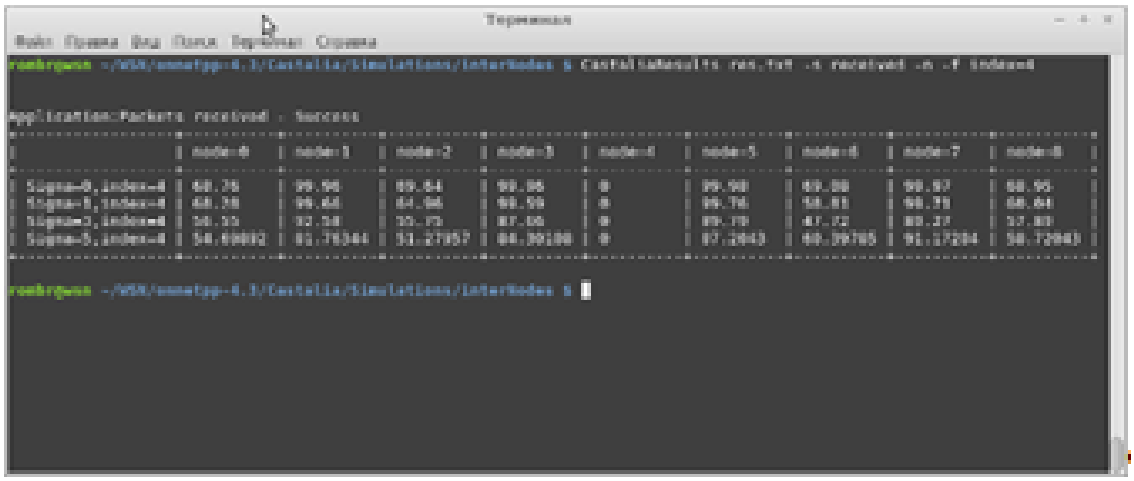


Рисунок 5.8 - Кількість пакетів, отриманих при різних рівнях перешкод

Для візуалізації отриманих даних в системі Castalia є команда CastaliaPlot, яка дозволяє будувати різні візуальні представлення (графіки, діаграми і т. Д.) З даних, що були отримані командою CastaliaResults [3] (рис.5.9).

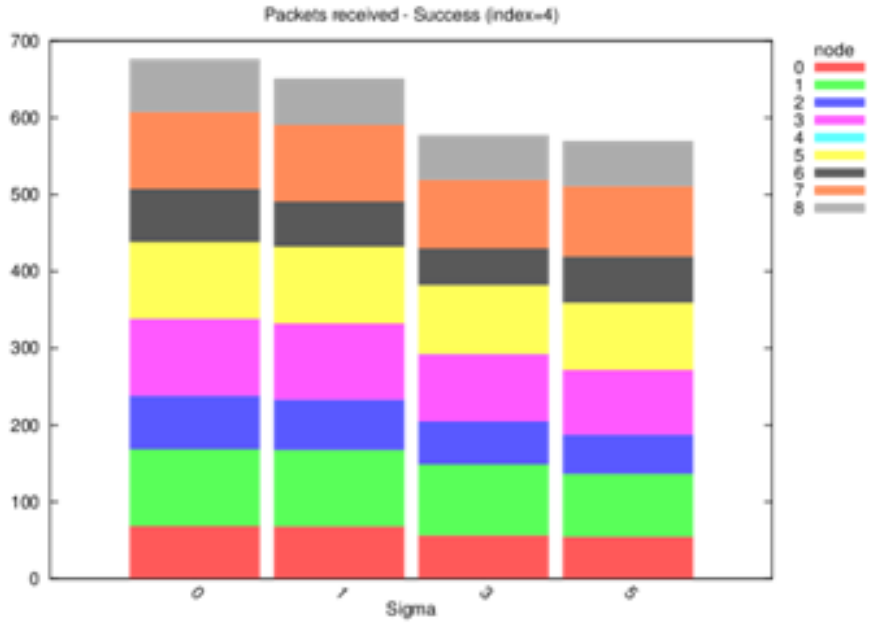


Рисунок 5.9 - Вплив перешкод на число отриманих пакетів

На рисунку 5.9 представлена діаграма, що ілюструє скільки пакетів, отримав п'ятий вузол від інших, де Sigma - параметр, який відповідає за рівень перешкод; node - вузли, пронумеровані від 0 до 8 і позначені різними кольорами; число на осі ординат відповідає загальному числу отриманих повідомлень п'ятим вузлом, кожен кольоровий сегмент показує скільки пакетів отримано від відповідного кольору вузла. Видно, що при відсутності перешкод було отримано близько семисот пакетів. Із зростанням величини перешкод починаючи з 3 видно, що число отриманих пакетів не значно падає, тобто можемо

говорити, що надійність тут вже не залежить від рівня перешкод, що може бути обумовлено хорошим протоколом канального рівня.

5.7 Впливи потужності радіо-модуля на надійність комунікаційного середовища між двома вузлами в системі Castalia

Розглянемо вплив потужності радіо-модуля при передачі повідомлень.

Для розгляду впливу потужності радіо-модуля визначили в налаштуваннях моделювання конфігурацію varyTxPower, при якій буде запущено моделювання з варіацією цього параметра (SN.node [*]. Communication.Radio.TxOutputPower = $ {TXpower = "0dBm", "- 1dBm", "-3dBm", "- 5dBm"})

На рисунку 5.10 представлена діаграма, що ілюструє скільки пакетів отримав п'ятий вузол від інших. Де TXpower - параметр, який відповідає за рівень потужності радіо-модуля; node - вузли, пронумеровані від 0 до 8 і позначені різними кольорами; число на осі ординат відповідає загальному числу отриманих повідомлень п'ятим вузлом, кожен кольоровий сегмент показує скільки пакетів отримано від відповідного кольору вузла. Видно, що при рівні потужності в -5dBm було отримано близько семисот пакетів. Із зростанням величини потужності, починаючи з -3dBm видно, що число отриманих пакетів зросла до восьмисот і стабільно, тобто можемо говорити, що надійність тут вже не залежить від рівня потужності радіо-модуля.

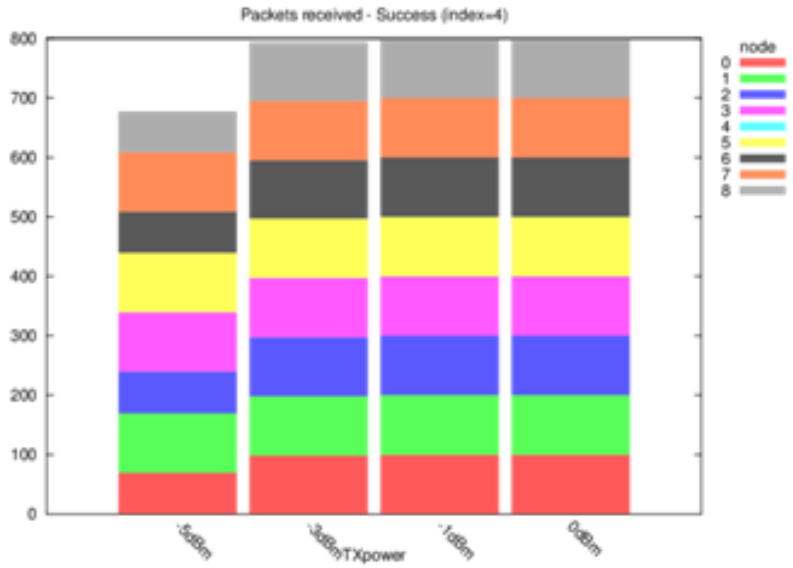


Рисунок 5.10 - Вплив рівня потужності радіо-модуля на число отриманих пакетів

5.8 Дослідження надійності збору інформації мережею в системі Castalia

Для простоти розгляду надійності збору інформації мережею будемо розглядати бездротову сенсорну мережу з 36 вузлів. Будемо вважати, що вузли розташовані в просторі на одній площині в області розміру 100м на 100м. Розташовані по сітці.

Для завдання параметрів моделювання в системі Castalia використовуються конфігураційні файли (зазвичай такий файл прийнято називати omnetpp.ini), розташовуватися такий файл повинен в папці даного моделювання (у нас reliabilityFullNet), яка в свою чергу повинна знаходитися в папці Simulations системи Castalia. Повний текст приведений в додатку Б.

Для завдання даної просторової конфігурації використовуються параметри: SN.field_x = 100, SN.field_y = 100, SN.numNodes = 36, SN.deployment = "6x6".

Час моделювання задаємо в 600с (параметр sim-time-limit = 600s). Варто зазначити, що моделювання в системі Castalia відбувається не в реальному часі, тобто реальний час проведення експерименту буде не 600 с.

Говорячи про збір даних бездротовою сенсорною мережею, маємо на увазі, що один з вузлів мережі є шлюзом між БСМ і зовнішніми системами, куди потрапляють зібрані дані. Нехай шлюзом буде четвертий вузол (параметр SN.node .Application.isSink = true).

Для того щоб збирати дані необхідна модель функціонування вузла, для цього був розроблений модуль програми DataToSink, представлений файлами DataToSink.ned, DataToSink.h, DataToSink.cc. Вихідний код приведений в додатку Б.

Раз в одну секунду (для цього в модулі визначено відповідний таймер) запускається процедура для збору даних з сенсора. При цих діях пишеться також інформація для трасування. Дана процедура знімає дані з сенсора (для цього є спеціальні функції) і формує пакет даних, який потім відправляє на шлюз (адреса шлюзу завжди міститься в спеціальній константі SINK_NETWORK_ADDRESS).

З іншого боку, якщо вузол отримує пакет даних і при цьому є шлюзом, то інформація про це заноситься в вихідні дані, щоб їх можна було проаналізувати.

В налаштуваннях моделювання вказуємо додаток (параметр SN.node [*]. ApplicationName = "DataToSink").

Для того, щоб інформація від вузлів йшла до шлюзу був розроблений модуль простий маршрутизації MultipathRingsRouting, представлений файлами MultipathRingsRouting.ned, MultipathRingsRouting.h, MultipathRingsRouting.cc. Вихідний код приведений в додатку Б.

Алгоритм складається з двох фаз, які поділяються типом пакета:

— Перша фаза. Встановлення рівнів. Для цього шлюз шле в канал пакет з типом MPRINGS_TOPOLOGY_SETUP_PACKET. Вузол, отримуючи такий пакет, якщо його власний рівень не встановлений, ставить рівень на одиницю більше, запам'ятовує як свій рівень і передає пакет далі. Аналогічно інші вузли. Таким чином, навколо шлюзу формуються «кільця рівнів».

— Друга фаза. Власне обмін даними. При відправці повідомлення від вузла в пакеті записується рівень цього вузла. При отриманні пакету з типом NETWORK_LAYER_PACKET, якщо рівень вузла менше рівня пакета, то пакет передається далі, поки не досягне шлюзу. Інакше, якщо рівень вузла більше або дорівнює рівню пакета, то такий пакет ігнорується (як неправильний напрямок). Загалом, даний алгоритм допомагає підвищити ефективність доставки даних до шлюзу і знизити навантаження на мережу.

В налаштуваннях моделювання вказуємо протокол маршрутизації (параметр SN.node [*]. Communication.RoutingProtocolName = "MultipathRingsRouting").

Надійність БСМ визначається надійністю обміну пакетами між вузлами. Тут під надійністю збору інформації мережею будемо розуміти надійність отримання пакетів шлюзом і розглядаємо можливість отримання пакетів.

Використовуючи раніше розглянутий апарат і запустивши моделювання с конфігурацією General, отримали дані, на основі яких побудований графік на рисунку 5.11. Тут видно інформація, про доставку пакетів до четвертого вузла (шлюзу). По осі абсцис стан доставки, а по осі ординат їх ймовірності. Видно, що стани Failed превалюють, а Received становлять приблизно близько 0,3. На перший погляд це може здатися поганим результатом, однак в силу специфіки інформації, що збирається і інших чинників, таких як довга автономна робота мережі, цілком прийнятно.

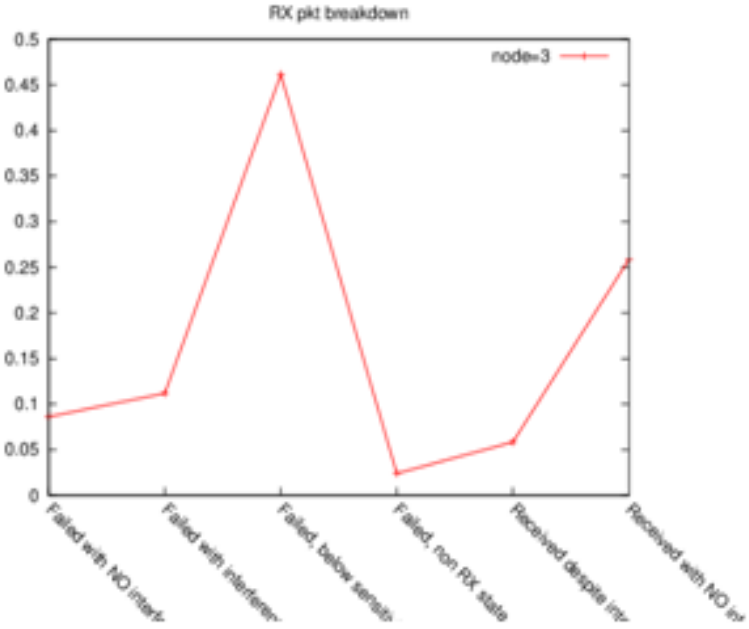
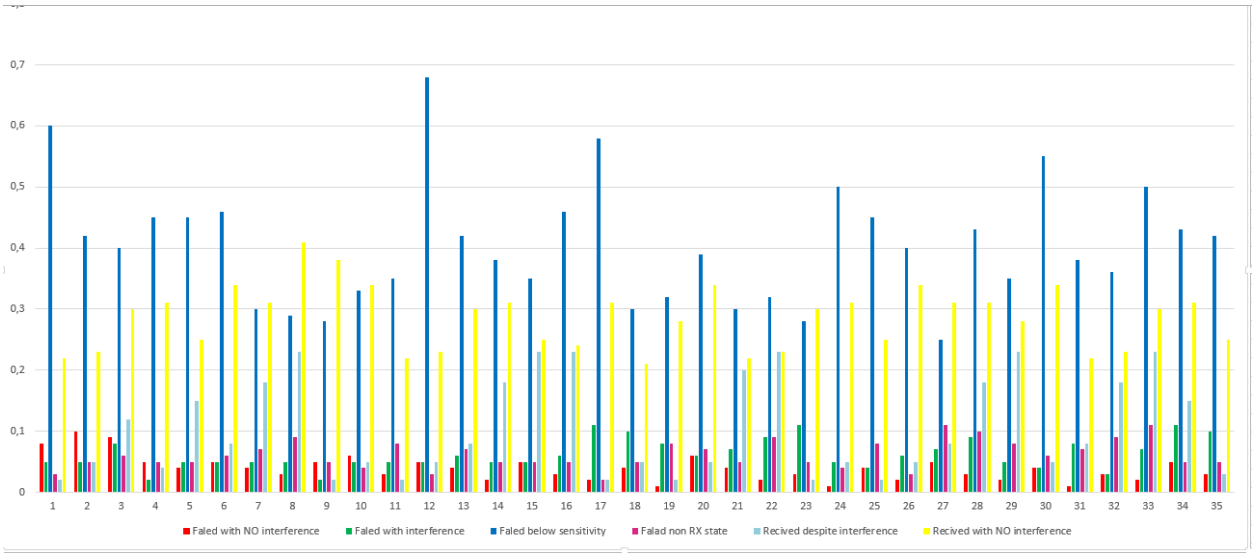


Рисунок 5.11 - Кількість пакетів, отриманих шлюзом

На рисунку 5.12 відображена інформація про можливості доставки повідомлень для всіх вузлів мережі. По осі абсцис номера вузлів, по осі ординат ймовірності, а кольорами позначені стани пакетів. Звідси видно, що найбільша надійність доставки пакетів 0,5 виявляється для вузла 27. Що може послужити причиною використовувати в якості шлюзу саме такі вузли.



Малюнок 5.12 – Інформація про отримані пакети для вісх вузлів

5.9 Вплив перешкод на надійність збору інформації мережею в системі Castalia

Для розгляду впливу перешкод на мережу визначили в налаштуваннях моделювання конфігурацію varySigma, при якій буде запущено моделювання з варіацією цього параметра (SN.wirelessChannel.sigma = $ {Sigma = 0,1,3,5}).

На рисунках 5.13-5.16 показано як змінюється надійність доставки пакетів в залежності від рівня перешкод. По осі абсцис номера вузлів, по осі ординат ймовірності, а кольорами позначені стани пакетів. Помітна тенденція, що зі зростанням рівня перешкод зростає ймовірність доставки пакетів. Це може бути обумовлено хорошими алгоритмами канального рівня.

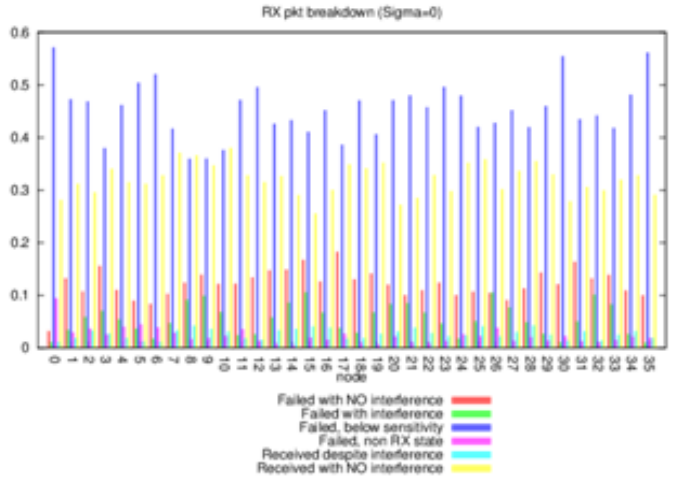


Рисунок 5.13 - Кількість пакетів при Sigma 0

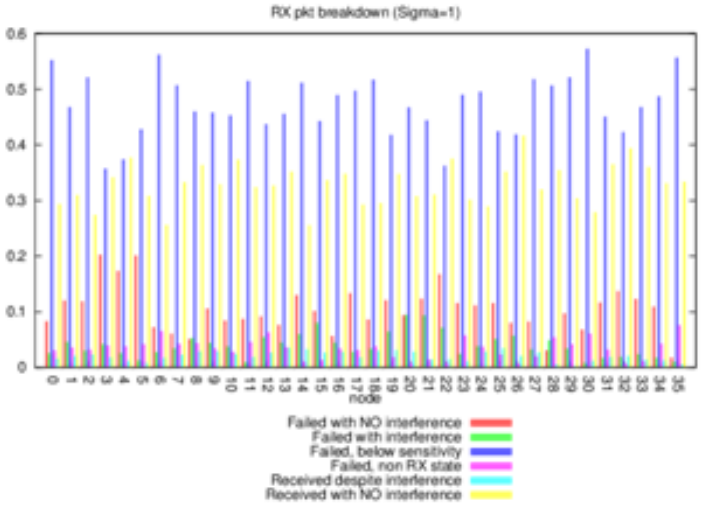


Рисунок 5.14 - Кількість пакетів при Sigma 1

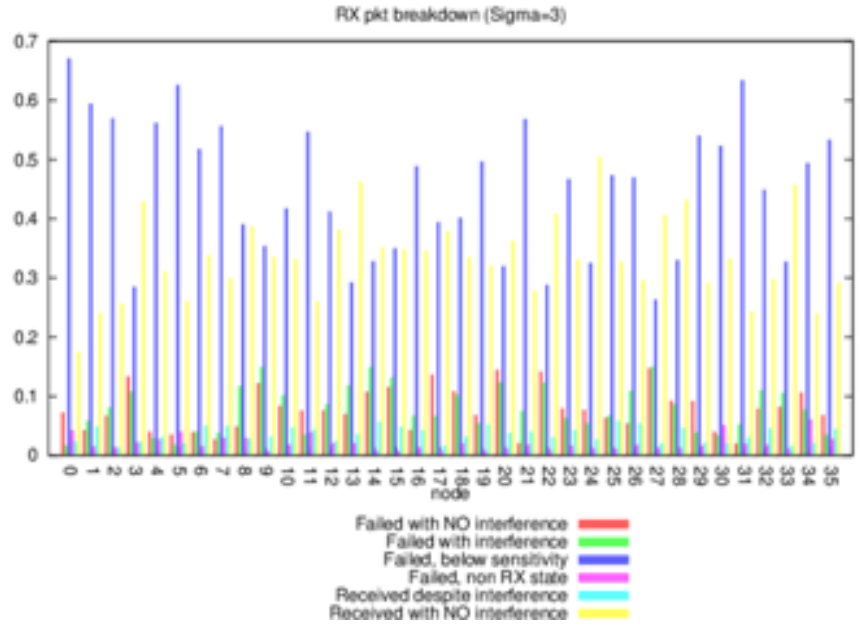


Рисунок 5.15 - Кількість пакетів при Sigma 3

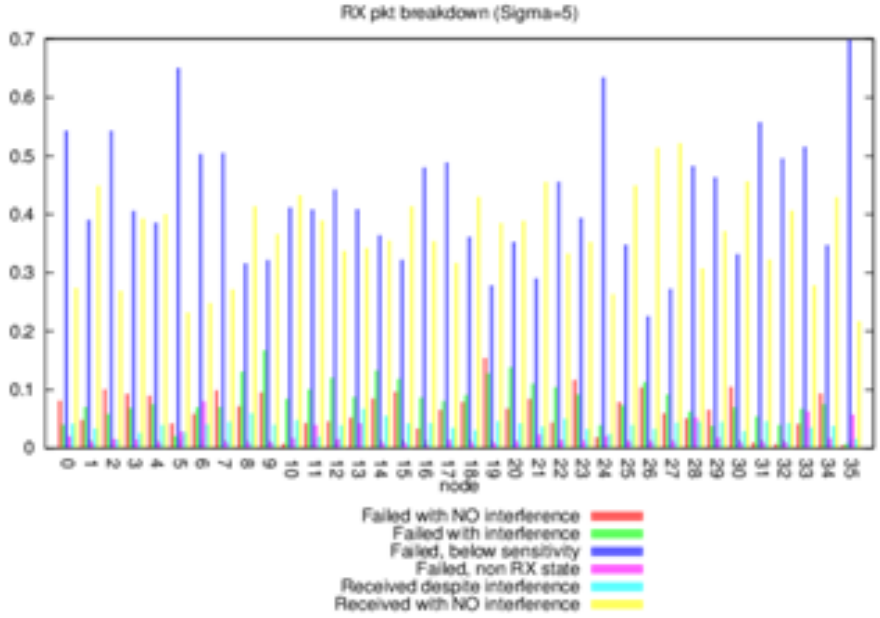


Рисунок 5.16 - Кількість пакетів при Sigma 5

ВИСНОВОК

Технологія Internet of Things - IoT (Інтернет речей) передбачає використання вбудованих мережевих пристроїв, так званих Smart (розумних) об'єктів, в навколишні нас речі. Можна привести багато прикладів подібних пристроїв: мобільні телефони, персональні пристрої охорони здоров'я, пристрої домашньої і промислової автоматизації, системи обліку та моніторингу навколишнього середовища і т.п. Поряд з цим перспективне використання даної технології в міському господарстві полягає в створенні міської бездротової Mesh - мережі для забезпечення оперативного зв'язку і доступу до різних баз даних спецслужб в разі надзвичайних ситуацій в межах міста (пожежі, дорожньо-транспортні пригоди, всілякі аварійні ситуації і т. п.). При цьому в місті на невеликій відстані один від одного (припустимо, на стовпах вуличного освітлення) встановлюються активні приймально-передавальні модулі - Mesh-портали, які в разі надзвичайної ситуації дозволяють працівникам спецслужб підключатися до них і виходити в інформаційну мережу.

Можна констатувати, що в даний час відбувається поступовий перехід від «Інтернету людей» до «Інтернету речей» - IoT. В основі технології IoT лежить принцип побудови бездротових сенсорних мереж на базі сучасних малопотужних ZigBee модулів. Точна кількість вузлів мережі, тобто розмір мережі, реалізованої на принципах технології Internet of Things, на сьогоднішній день важко оцінити, так як зростання даних мереж не залежить від кількості користувачів в них. Передбачається, що ця складова скоро перевищить решту мережі Інтернет за розміром і буде продовжувати рости швидкими темпами. Довгостроковий потенційний розмір IoT зараз оцінюється трильйонами пристроїв.

Створення та ефективне використання такого роду систем передбачає розвиток методів їх моделювання. Існує кілька досить ефективних систем моделювання сенсорних мереж. Однак при проектуванні реальних мереж велику роль відіграє правильний вибір конкретної моделює системи. Серед засобів імітаційного моделювання бездротових сенсорних мереж на базі стандарту IEEE 802.15.4-2006 найбільшого поширення набули наступні системи: NS-2 - об'єктно-орієнтоване середовище імітаційного моделювання дискретних подій і станів з відкритим вихідним кодом; OPNET Modeler - потужне середовище імітаційного моделювання дискретних подій і станів; OMNET ++ - середовище імітаційного моделювання дискретних подій і станів з відкритим вихідним кодом, заснована на компонентах ZigBee.

Основна область застосування всіх цих систем - моделювання мереж передачі даних, IT систем і бізнес процесів. Був проведений порівняльний аналіз зазначених симуляторів, який показав, що в умовах некомерційного застосування засобу моделювання використання програмного комплексу OPNET Modeler представляється досить проблематичним через його дорожнечу. Звичайно, існує безкоштовна ознайомча версія OPNET Modeler Academic Edition, однак з огляду на те, що дана версія дещо спрощена і скорочена її використання в реальних умовах є не завжди прийнятним. Інший симулятор, Network Simulator NS-2, також не підходить через невідповідність специфікації модулів ZigBee, на яких базуються структури, реалізовані за технологією Internet of Things. Нарешті, аналіз ще одного програмного комплексу OMNET ++ в ролі симулятора сенсорних ZigBee- мереж показав, що на сьогодні він є найкращим варіантом.

На основі проведених досліджень зроблені наступні висновки:

— при оцінці надійності передачі пакета даних між двома вузлами зі збільшенням рівня перешкод до певного значення сильного падіння надійності не відбувається;

— надійність зв'язку між вузлами залежить від топології;

— рівень потужності сигналу не впливає суттєво на надійність;

— при оцінці надійності збору інформації мережею для розглянутої мережі коливання надійності не настільки істотні при різних рівнях перешкод, що може бути обумовлено хорошими алгоритмами канального рівня.

У даній роботі були розглянуті математичні методи оцінки надійності бездротових сенсорних мереж, виконано огляд і аналіз програмних продуктів, призначених для імітаційного моделювання таких мереж. На підставі аналізу та відповідно до поставлених цілей роботи була обрана система моделювання Castalia, для якої були розроблені модулі, що дозволяють виконати моделювання впливу перешкод і потужності передачі радіосигналу на надійність передачі пакета даних між двома вузлами і надійність збору інформації бездротової сенсорної мережею. Результати моделювання представлені у вигляді таблиць, графіків і діаграм.

ПЕРЕЛІК ДЖЕРЕЛ

1. Castalia Installation Guide [Электронный ресурс] / Castalia: URL: http://castalia.research.nicta.com.au/pdfs/Castalia%20-%20Installation.pdf

2. Castalia official site [Электронный ресурс] / Castalia: URL: http://castalia.research.nicta.com.au/

3. Castalia User's manual [Электронный ресурс] / Castalia: URL: http://castalia.research.nicta.com.au/pdfs/Castalia%20-%20User%20Manual.pdf

4. Chandra T.D., Toueg S. Unreliable failure detectors for reliable distributed systems. // J. ACM. 1996. V. 43. P. 225-267.

5. Delporte-Gallet C., Devismes S., Fauconnier H. Stabilizing leader election in partial synchronous systems with crash failures. // J. Parallel Distrib. Comput. − 2010. − 70. − P. 45 − 58.

6. E. Egea-Lpez, J. Vales-Alonso, A. S. Martnez-Sala, P. Pavn-Mario, J. Garca-Haro Simulation Tools for Wireless Sensor Networks // Summer Simulation Multiconference - SPECTS 2005 // − 2005. − P. 2 − 9.

7. Ezio Biglieri Coding for Wireless Channels (Information Technology: Transmission, Processing and Storage) −2005. − P. 428.

8. Fei Yu A Survey of Wireless Sensor Network Simulation Tools URL: http://www1.cse.wustl.edu/~jain/cse567−11/ftp/sensor/index.html

9. Fischer M.J., Lynch N.A., Paterson M.S. Impossibility of distributed consensus with one faulty process. // J. ACM. 1985. V 32. P. 374-382.

10. Garay J.A., Perry K.J. A continuum of failure models for distributed computing. // Proc. 6nd Int. Workshop on Distributed Algorithms (Haifa, 1992) / S. Zaks, A. Segall (eds.). P. 153-156.

11. IEEE Standards 802.15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). − IEEE Computer Society, 2003.

12. Luis Javier Garca Villalba , Ana Lucila Sandoval Orozco, Alicia Trivio Cabrera, Cludia Jacy Barenco Abbas Routing Protocols in Wireless Sensor Networks // Sensors // − 2009 − 9 − P. 399-421.

13. Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. // J. ACM. 1984. V. 27. P. 228-234.

14. Roya N., Gub T., Das S.K. Supporting pervasive computing applications with active context fusion and semantic context delivery. // Pervasive and Mobile Computing − 2010. − 6. − P. 21-42.

15. Zhang M., Chan M.C., Ananda A.L. Connectivity monitoring in wireless sensor networks. // Pervasive and Mobile Computing − 2010. − 6. − P. 112-127.

16. Акимов Е.В., Кузнецов М.Н. Вероятностные математические модели для оценки надежности беспроводных сенсорных сетей // Электронный журнал «Труды МАИ». Выпуск № 40// URL: http://www.mai.ru/science/trudy/

17. Ахо А., Хопкрофт Д., Ульман Д. Структуры данных и алгоритмы /А. Ахо − М.: Вильямс, 2000. − 384 с.

18. Гейер Д.Ж. Беспроводные сети. Первый шаг. // Пер. с англ. / Д.Ж. Гейер − М.: Вильямс, 2005. − 192 с.

19. Нечаев Д.Ю., Чекмарев Ю.В. Надежность информационных систем/Д.Ю. Нечаев − М.: ДМК Пресс, 2012. − 64 с.

20. Острейковский В.А. Теория надежности / В.А Острейковский М.: Высшая школа, 2000. − 464 с.

21. Острейковский В.А. Теория надежности. Учебник для вузов / В.А Острейковский − М.: Высшая школа, 2003. − 457 с.

22. Половко А.М., Гуров С. В. Основы теории надежности / А.М. Половко − СПб.: БХВ-Петербург 2006. − 560 с.

23. Смелянский Р. Л. Компьютерные сети. В 2 томах. Том 1. Системы передачи данных / Р.Л Смелянский − М.: Академия, 2011. − 304 с.

24. Тель Ж. Введение в распределенные алгоритмы. Пер. с англ. В. А. Захарова. / Ж. Тель − М.: МЦНМО, 2009. − 616 с.

25. Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. / И.А Ушаков − М.: Радио и связь 1991. − 132 с.

26. Хьюз К., Хьюз Т. Параллельное и распределенное программирование на C++. Пер. с англ. / К. Хьюз − М.: Издательский дом Вильямс, 2004. − 672 с.

27. Шахнович И.А. Современные технологии беспроводной связи. /И.А Шахнович − М.: Техносфера, 2006. − 288 с.

28. Шубин В.И. Беспроводные сети передачи данных / В.И. Шубин, О. С. Красильникова. − М.: Вузовская книга, 2012. − 104 с.

29. Эндрюс Г.Р. Основы многопоточного, параллельного и распределенного программирования / Г.Р. Эндрюс // Пер. с англ. − М.: Издательский дом Вильямс, 2003. − 512 с.

30. Вабищевич А. Н. Определение положения в пространстве элементов бес проводной сенсорной сети с помощью инерциальных сенсоров / А.Н. Вабищевич // Тезисы докладов научно-технической конференции студентов, аспирантов и молодых специалистов МИЭМ’2010. − М.: МИЭМ, 2010. − С. 151-152.

31. Васильев Ф. П. Численные методы решения экстремальных задач: Учеб. пособие для вузов. − 2-е изд., перераб. и доп. / Ф.П Васильев − М.: Наука, 1988. 552 с.

32. Вишневский В. М. Широкополосные беспроводные сети передачи информации / В.М. Вишневский − М.: Техносфера, 2005. 592 с.

33. Гекк М. В., Истомин Т. Е., Файзулхаков Я. Р., Чечендаев А. В. Адаптивный алгоритм быстрой доставки сообщений по выделенным направлениям для беспроводных сетей датчиков / М.В. Гекк // Вестник молодых ученых "Ломоносов". Выпуск III. 2006. С. 55–60.

34. Ефремов В. В., Маркман Г. З. "Энергосбережение"и "энергоэффективность": уточнение понятий, система сбалансированных показателей энергоэффективности / В.В. Ефимов // Известия Томского политехнического университета. 2007. Т. 311, No 4. С. 146–148.

35. Ефремов С. Г. Разработка системы активного беспроводного сбора данных в интралогистике (номер государственной регистрации НИОКР01200961253).

36. Жданов В. С. Проблемы и задачи проектирования беспроводных сенсорных сетей // Информационные, сетевые и телекоммуникационные технологии: сборник научных трудов, под ред. проф. д.т.н. Жданова В.С. 2009. С. 8–21.

37. Иванов Е. В. Определение координат в беспроводных сенсорных сетях: дис. ... канд. техн. наук: 05.12.13. 2008. 149 с.

38. Комаров М. М. Разработка и исследование метода энергетической балансировки беспроводной стационарной сенсорной сети с автономными источниками питания: дис. ... канд. техн. наук: 05.12.13. 2012. 125 с.

39. Комаров М. М., Восков Л. С. Позиционирование датчиков беспроводной сети как способ энергосбережения // Датчики и системы. 2012. Т. 1. С. 34–38.

40. Курпатов Р. О. Исследование и разработка энергоэффективного метода локализации элементов беспроводных сенсорных сетей: дис. ... канд. техн. наук: 05.12.13. М., 2011. 126 с.

41. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 4-е издание, 2010. 943 с.

42. Юркин В. Ю., Мохсени Т. И. Иерархические подходы к самоорганизации в беспроводных широкополосных сенсорных сетях на основе хаотических радиоимпульсов // Труды МФТИ. 2012. Т. 4, No 3. С. 151–161.

43. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z0231-05 - 21.12.2017 р.

44. Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України (НАПБ Б.02.005-2003) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z1148-03 - 21.12.2017 р.

45. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.6.042.-99) [Електронний ресурс] / Законы Украины - Режим доступу: www.URL: http://uazakon.com/documents/date_42/pg_ikcfxj.htm - 22.12.2017 р.

46. Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98) [Електронний ресурс] / Педрада - Режим доступу: www.URL: http://zakon.pedrada.com.ua/regulations/10637/478672/ - 22.12.2017 р.

47. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою (НАПБ Б.03.002-2007) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/32980/doc-НАПБ_Б.03.002.-2007 - 23.12.2017 р.

48. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.6.042-99) [Електронний ресурс] / UAinfo - Режим доступу: www.URL: http://ua-info.biz/legal/basetp/ua-zmptae.htm - 23.12.2017 р.

49. Санітарні норми виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.6.037-99) [Електронний ресурс] / Нормативно-директивні документи МОЗ України - Режим доступу: www.URL: http://mozdocs.kiev.ua/view.php?id=1789 - 23.12.2017 р.

50. Про затвердження Положення про розробку інструкцій з охорони праці (ДНАОП 0.00-4.15-98) [Електронний ресурс] / Законодавство України – Режим доступу: www.URL: http://zakon2.rada.gov.ua/laws/show/z0226-98 - 23.12.2017 р.

51. Про затвердження Правил охорони праці під час експлуатації електронно-обчислювальних машин (НПАОП 0.00-1.28-10) [Електронний ресурс] / Законодавство України – Режим доступу: www.URL: http://zakon2.rada.gov.ua/laws/show/z0293-10 - 23.12.2017 р.

52. Природне і штучне освітлення (ДБН В.2.5-28:2015) [Електронний ресурс] / Державні будівельні норми України – Режим доступу: www.URL: http://dbn.at.ua/load/normativy/dbn/dbn_v_2_5_28_2015/1-1-0-1188 - 23.12.2017 р.

53. Державні санітарні правила і норми (ДСанПіН 2.2.7.029) [Електронний ресурс] / LIGA:ZAKON – Режим доступу: www.URL: http://search.ligazakon.ua/l_doc2.nsf/link1/MOZ4153.html - 25.12.2017 р.

54. Державні санітарні норми виробничої загальної та локальної вібрації (ДСН 3.3.6.039-99) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/31680/doc-%D0%94%D0%A1%D0%9D_3.3.6.039-99 - 25.12.2017 р.

55. ССБТ. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля (ГОСТ 12.1.006-84) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/42235/doc-%D0%93%D0%9E%D0%A1%D0%A2_12.1.006-84 - 26.12.2017 р.

56. Электробезопасность. Защитное заземление. Зануление (ГОСТ 12.1.030-81) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/2128/doc-%D0%93%D0%9E%D0%A1%D0%A2_12.1.030-81 - 26.12.2017 р.

57. Нормы качества электрической энергии в системах электроснабжения общего назначения (ГОСТ 13109-97) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/42313/doc-%D0%93%D0%9E%D0%A1%D0%A2_13109-97 - 26.12.2017 р.

58. Правила безпечної експлуатації електроустановок споживачів (НПАОП 40.1-1.21-98) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/2029/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_40.1-1.21-98 - 27.12.2017 р.

59. Опалення, вентиляція та кондиціювання (ДБН В.2.5-67:2013) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/32609/doc-%D0%94%D0%91%D0%9D_%D0%92.2.5-67_2013 - 27.12.2017 р.

60. Общие санитарно-гигиенические требования к воздуху рабочей зоны (ГОСТ 12.1.005-88) [Електронний ресурс] / document.UA - Режим доступу: www.URL: http://document.ua/ssbt_-obshie-sanitarno-gigienicheskie-trebovanija-k-vozduhu--nor3205.html - 26.12.2017 р.

61. ССБТ. Пожаровзырвоопасность веществ и материалов (ГОСТ 12.1.044-89) [Електронний ресурс] / STROYNOTE строительный портал - Режим доступу: www.URL: http://www.stroynote.com.ua/construction-regulations/document-1611.html - 27.12.2017 р.