МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia»

Виконавець: Олександра КИРИЛЕНКО
(підпис)

Керівник: Віталій КУРУШКІН
(підпис)

Нормоконтролер: Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Кириленко Олександри Романівни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia»
затверджена наказом ректора від «29» березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: БСМ, протокол ZigBee, програмний пакет Castalia.
4. Зміст пояснювальної записки: вступ, актуальність використання БСМ, моделювання БСМ, методи моделювання на базі протоколу ZigBee з використанням програмного пакету Castalia.
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: :енергоспоживання вузлів, зображення роботи вузла.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	АНАЛІЗ БЕЗДРОТОВОЇ ТЕХНОЛОГІЇ ZigBee.	26.05.2023-29.05.2023	Виконано
4	АНАЛІЗ ФУНКЦІОНАЛЬНОГО ВУЗЛА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ.	30.05.2023-07.06.2023	Виконано
5	МОДЕЛЮВАННЯ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ ZigBee ЗА ДОПОМОГОЮ ПРОГРАМНОГО ПАКЕТУ Castalia.	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Олександра КИРИЛЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia» містить _57__ сторінок, _4__ рисунків, _0__ таблиці, _15__ використаних джерел.

Ключові слова: моделювання, бездротова сенсорна мережа, протокол ZigBee, програмний пакет Castalia, мережеві технології, моделювання бездротових мереж, симуляція бездротових мереж, топологія, ZigBee, БСМ, сенсорна мережа, аналіз, бездротовоі технології, області використання, радіомодуль, безпека.

Об’єкт дослідження – є бездротова сенсорна мережа, яка складається з вузлів, що обмінюються даними за допомогою протоколу ZigBee.

Предмет дослідження – процес моделювання цієї мережі з використанням програмного пакету Castalia.

Мета кваліфікаційної роботи – метою кваліфікаційної роботи є вивчення поширених і розробка адаптивних алгоритмів передачі даних у безпровідних сенсорних мережах.

Метод дослідження – при вирішенні комплексу завдань використовувались такі методи: теорія інформації та кодування, методи теорії чисел, методи завадостійкого кодування даних при розробці модулярних коректуючих кодів і методу мережного кодування, методи побудови розподілених комп’ютерних систем та принципи інтелекту при розробці концепції побудови безпровідних сенсорних мереж на основі колективного інтелекту, теорія та методи передачі даних.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

Умовні позначення:

- МП - мікропроцесор;
- МК - мікроконтролер;
- ПЗ - програмне забезпечення;
- ОС - операційна система;
- API - інтерфейс програмування додатків;
- GUI - графічний інтерфейс користувача;
- IDE - інтегроване середовище розробки;
- RAM - оперативна пам'ять;
- ROM - постійна пам'ять;
- UART - універсальний асинхронний приймач-передавач;
- USB - універсальна послідовна шина.

Перелік скорочень:

WSN, БСМ- бездротова сенсорна мережа;

- AODV - Ad-hoc On-demand Distance Vector Routing Protocol (протокол маршрутизації на основі вектора відстаней);
- API - Application Programming Interface (інтерфейс програмування додатків);
- CC2420 - 2.4 GHz ZigBee / IEEE 802.15.4 RF Transceiver (радіопередавач для бездротових мереж);
- CPU - Central Processing Unit (центральний процесор);
- CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance (протокол доступу до каналу з перевіркою несучої та уникненням колізій);
- IDE - Integrated Development Environment (інтегроване середовище розробки);
- IEEE - Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки);
- MAC - Media Access Control (контроль доступу до мережевого середовища);

- MCU - Microcontroller Unit (мікроконтролер);

- MSP430 - Ultra-Low Power Microcontroller from Texas Instruments (мікроконтролер від компанії Texas Instruments);

- NS-2 - Network Simulator 2 (симулятор мереж);

- OS - Operating System (операційна система);

- PHY - Physical Layer (фізичний рівень мережі);

- RAM - Random Access Memory (оперативна пам'ять);

- ROM - Read Only Memory (постійна пам'ять);

- RSSI - Received Signal Strength Indicator (індикатор сили отриманого сигналу);

- SDK - Software Development Kit (набір засобів для розробки програмного забезпечення);

- UART - Universal Asynchronous Receiver/Transmitter (універсальний асинхронний приймач-передавач);

- USB - Universal Serial Bus (універсальна послідовна шина);

- ZigBee - Wireless Communication Standard for Low-Power, Low-Cost, and Mesh Networks (стандарт бездротового зв'язку для мереж з низьким енергоспоживанням, низькою вартістю та мережами типу "мережа-сітка").

ВСТУП

Актуальність теми. Бездротові сенсорні мережі (БСМ) набувають все більшої популярності завдяки своїй здатності моніторити та збирати дані з різних середовищ. Одним з найпоширеніших протоколів для БСМ є ZigBee, який забезпечує низьке енергоспоживання та надійний зв'язок. У зв'язку з цим метою даного дослідження є моделювання бездротової сенсорної мережі на основі протоколу ZigBee з використанням програмного пакету Castalia.

Castalia - це мережевий симулятор з відкритим вихідним кодом, який дозволяє моделювати та імітувати WSN. Він надає повний набір інструментів для моделювання різних аспектів роботи бездротових мереж, включаючи поширення радіохвиль, споживання енергії та мережеві протоколи. За допомогою Castalia можна оцінити продуктивність бездротової сенсорної мережі за різних сценаріїв та умов.

Запропонована модель базуватиметься на протоколі ZigBee, який є стандартом бездротового зв'язку з низьким енергоспоживанням, розробленим для WSN. ZigBee забезпечує надійний зв'язок з низьким енергоспоживанням, що робить його ідеальним вибором для WSN. Модель буде оцінюватися за допомогою різних метрик, таких як коефіцієнт доставки пакетів, наскрізна затримка і споживання енергії.

Отже, метою цього дослідження є моделювання бездротової сенсорної мережі на основі протоколу ZigBee за допомогою програмного пакету Castalia. Запропонована модель буде оцінена за допомогою різних метрик для оцінки її продуктивності за різних сценаріїв та умов.

Мета і завдання дослідження. Метою є дослідження можливостей та ефективності використання бездротових сенсорних мереж на базі протоколу ZigBee.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Огляд літератури з питань бездротових сенсорних мереж, протоколу ZigBee та програмного пакету Castalia.

2. Аналіз можливостей та обмежень протоколу ZigBee для застосування у бездротових сенсорних мережах.

3. Розробка моделі бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia.

Об'єктом дослідження – є бездротова сенсорна мережа, яка складається з вузлів, що обмінюються даними за допомогою протоколу ZigBee.

Предметом дослідження – процес моделювання цієї мережі з використанням програмного пакету Castalia.

Методи досліджень. Теорія інформації та кодування, методи теорії чисел, методи завадостійкого кодування даних при розробці модулярних коректуючих кодів і методу мережного кодування, методи побудови розподілених комп'ютерних систем та принципи інтелекту при розробці концепції побудови безпровідних сенсорних мереж на основі колективного інтелекту, теорія та методи передачі даних.

Практичне значення отриманих результатів.

Отримані результати моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia можуть мати практичне значення для розробки та впровадження подібних мереж у різних галузях, таких як промисловість, медицина, автоматизація будинків та інші.

Зокрема, результати дослідження можуть допомогти в проектуванні оптимальної топології мережі, визначенні оптимальних параметрів передачі даних та енергоспоживання сенсорних вузлів, а також в оцінці продуктивності мережі при різних умовах експлуатації.

Крім того, результати дослідження можуть бути корисними для покращення якості обслуговування та забезпечення безпеки передачі даних у бездротових сенсорних мережах.

Таким чином, отримані результати моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia можуть мати значення для розробки та впровадження подібних мереж у різних галузях.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
АНАЛІЗ БЕЗДРОТОВОЇ ТЕХНОЛОГІЇ ZigBee.

1.1. Архітектура стека ZigBee

Будь-який стандарт,будьто інтерфейс для передачі даних або бездротовий зв'язок,створюється для вирішення конкретного завдання. Наприклад, WiFi забезпечує зв'язок на середні відстані з відносно високою швидкістю передачі даних. Хоча передача відео та аудіо також можлива, WiFi призначений для пристроїв, які підключають бездротові пристрої до корпоративних мереж та Інтернету. Стандарт Bluetooth також призначений для передачі даних на короткі відстані; Bluetooth має значну перевагу в швидкості над WiFi і підходить для потокової передачі аудіо та відео між компонентами домашнього кінотеатру, наприклад. zigBee Основне завдання, яке вирішує ZigBee - передача невеликих обсягів даних на середні відстані. Особливість завдання ZigBee полягає в тому, що приймально-передавальні пристрої цього стандарту повинні мати мінімальне енергоспоживання. За допомогою IEEE 802.15.4 і ZigBee не можна передавати високоякісне потокове аудіо і відео з високою роздільною здатністю. відео високої роздільної здатності, але просунуті схеми моніторингу та управління можуть бути реалізовані практично в будь-якій області.

Документ IEEE 802.15.4 описує частоти, функції та інші параметри мережі, в той час як документ ZigBee описує процеси управління мережею, параметри безпеки та ключові концепції сумісності і профілі пристроїв.Особливістю мереж IEEE 802.15.4-2006 є те, що в них можуть бути реалізовані практично всі протоколи, включаючи стільникові.

Стек протоколів ZigBee побудований на принципах ієрархічної семирівневої моделі протоколів передачі даних у відкритих системах OSI (Open System Interconnection). Стек включає в себе рівень стандарту IEEE 802.15.4, який відповідає за реалізацію каналу зв'язку, а також прикладний мережевий рівень і рівень підтримки додатків, визначені в специфікації ZigBee Alliance.

Архітектура IEEE 802.15.4 визначає ряд рівнів, призначених для спрощення стандарту. Кожен рівень відповідає за частину стандарту і надає послуги для рівня, розташованого вище.Інтерфейси між рівнями визначають логічні взаємозв'язки, описані в стандарті.

IEEE Std 802.15. 4 визначає специфікації для фізичного (PHY) і середнього (MAC) рівнів доступу для низькошвидкісних бездротових середовищ з використанням портативних ручних пристроїв, з максимальною відстанню доступу POS (Personal Operating Space) в 10 метрів. При нижчих швидкостях передачі передбачається, що можна працювати на більших відстанях (<100 м).

Фізичний рівень стека

Фізичний рівень PHY надає два типи послуг: інформаційну послугу PHY і послугу управління, яка взаємодіє зі службою PLME (Physical Layer Management Entity) (яка називається PLME-SAP) точки доступу SAP. Інформаційна послуга PHY дозволяє передавати блок даних протоколу PPDU (Protocol Data Unit) блок даних протоколу PPDU (Protocol Data Unit) може передаватися і прийматися бездротовим способом.

Стандарт визначає наступні швидкості передачі даних: 250 кбіт/с, 100 кбіт/с, 40 кбіт/с, 20 кбіт/с. Радіоприймач приймає і передає дані на фізичному рівні PHY, визначаючи використовуваний діапазон частот, тип модуляції, максимальну швидкість і кількість каналів: діапазон 2,4 ГГц O-QPSK (16 каналів, 250 Кбіт/с), BPSK (подвійна фазова маніпуляція) на частотах 915 МГц (10 каналів, 40 Кбіт/с) і 868 МГц (1 канал, 20 Кбіт/с). Рівень PHY запускає/зупиняє приймач, визначає енергію прийнятого сигналу в робочому каналі, вибирає фізичний частотний канал, вказує на якість зв'язку при прийомі пакетів даних, оцінює вільні канали для реалізації протоколу CSMA-CA (протокол множинного доступу з керуванням несучою та уникненням колізій). Важливо розуміти, що стандарт 802.15.4 - це фізичне радіо (мікросхема радіоприймача), а ZigBee - це логічна мережа та програмний стек, який забезпечує функції безпеки та маршрутизації.

Радіообладнання працює на одному з неліцензованих частотних діапазонів:

868-868.6 МГц (наприклад, для Європи)

902-928 МГц (для Північної Америки)

2400-2483.5 МГц (для решти світу)

Можливості MAC-рівня:

64-розрядна адресація IEEE, 16-розрядна адресація в локальній мережі (теоретична максимальна кількість пристроїв у мережі - 264, проста мережа з 16-розрядною адресацією в локальній мережі налічує понад 65 тисяч (216) пристроїв).

Метод адресації.

Ідентифікація: Ідентифікатор мережі + ідентифікатор обладнання (протокол Star);

Ідентифікатор відправника/одержувача (однорангова передача);

Автоматичний вхід/вихід з мережі/напівавтоматична організація мережі;

Формат пакету мережевих повідомлень ZigBee; максимальне корисне навантаження пакета даних - 104 байти даних; максимальна довжина кадру - 127 байт;

Рівень безпеки.

Вільний доступ до мережі;

Список контролю доступу;

Таймер для виявлення затримок при передачі та актуальності пакетів даних;

Шифрування 128-бітовим симетричним ключем AES;

Механізми доступу до мережі, розподіл часу та гарантовані часові інтервали; доступ до каналів за протоколом CSMA-CA;

Підтримка мережевих протоколів, включаючи протоколи "точка-точка", "зірка", багатостільникові та кластерні протоколи;

Сповіщення про прибуття пакетів даних, підтвердження отримання (ACK) та 16-бітовий контроль помилок (CRC);

Пакетний/потоковий режим передачі

1.2. Топологія ZigBee

Стандарт IEEE 802.15.4 - це основа для більш високорівневих протоколів (ZigBee, 6loWPAN, DigiMesh тощо). Він дозволяє реалізовувати за допомогою програмних надбудов на мережевому рівні та вище будь-яку з топологій.

Протокол ZigBee дозволяє створювати сенсорні мережі, що самоорганізуються і самовідновлюються; завдяки вбудованому програмному забезпеченню, пристрої ZigBee можуть знаходити один одного і формувати мережу при включенні, також у разі збою в одному з вузлів може бути створений новий маршрут і відправлені повідомлення.

Мережа ZigBee складається з трьох типів логічних пристроїв: ZigBee-контролер, ZigBee-маршрутизатор і кінцеві точки ZigBee Функція ZigBee-координатора полягає в частковому переключенні каналів і пошуку вільних каналів для формування мережі, У мережі ZigBee може існувати тільки один контролер. Функції маршрутизатора ZigBee - передача пакетів, маршрутизація і буферизація даних для сплячих кінцевих вузлів; кінцеві точки ZigBee виконують тільки прикладні функції (збір інформації та управління віддаленими об'єктами) і не беруть участі в передачі.

Протокол ZigBee можна використовувати не тільки для реалізації простих з'єднань типу "точка-точка" і "зірка", але і для побудови складних мереж з деревоподібною і комірчастою структурою. Надійна дальність передачі бездротового сигналу вузлів мережі ZigBee, Залежно від багатьох факторів (особливо чутливості приймача і потужності передавача), відстань між вузлами мережі ZigBee може становити в середньому 100 м на відкритому повітрі і десятки метрів в приміщенні. Неможливість переведення контролерів і маршрутизаторів у сплячий режим є перешкодою для створення повністю автономних сенсорних мереж.

Трафік сенсорної мережі може передаватися через телекомунікаційні мережі загального користування.

Отже, сенсорні мережі характеризуються наступними особливостями:

-Здатність до самокорекції та самоорганізації,

-Здатність передавати інформацію на великі відстані з низькою потужністю передачі (шляхом ретрансляції),

-Низька вартість вузла та малі розміри,

-Низьке енергоспоживання і можливість живлення від вбудованого джерела живлення,

-Простота в установці, відсутність необхідності прокладати кабелі (завдяки повністю бездротовій технології та роботі від батареї),

-Така мережа може бути створена без додаткових робіт на існуючих експлуатаційних об'єктах,

-Можливість керувати інфраструктурою за допомогою планшетного ПК,

-Низькі витрати на обслуговування.

При проектуванні та побудові сенсорної мережі необхідно враховувати різні аспекти, в тому числі вирішення науково-технічних завдань, пов'язаних з різними галузями інформаційно-телекомунікаційних технологій.

1.3. Надійність

Zigbee - це технологія бездротових мереж, що використовується для забезпечення зв'язку між різними пристроями. Технологія була розроблена з метою створення надійних і ефективних мереж, які можуть працювати в різних умовах і середовищах.

Згідно з даними, Zigbee використовує надійну технологію, яка може працювати в різних умовах і середовищах. Однак, як і у випадку з будь-якою технологією, у неї можуть бути обмеження і недоліки: Для максимізації продуктивності та ефективності вимірювань на основі Zigbee необхідно враховувати ряд факторів, включаючи діапазон сигналу, перетворення в сигнальні шляхи і кількість підключених сигналів.

Однією з ключових переваг Zigbee є його низьке енергоспоживання, що дозволяє адаптувати батареї для тривалої безперервної роботи. Zigbee також

пропонує високий рівень безпеки, забезпечуючи аутентифікацію та шифрування інформації для більш глибокого захисту.

Ще однією перевагою Zigbee є його ефективність. Ця технологія дозволяє пристроям довше працювати від батарей за рахунок використання низького енергоспоживання. Крім того, Zigbee має вбудовану систему керування живленням, яка дозволяє ефективно використовувати енергію та економити заряд батареї.

Незважаючи на всі ці переваги, Zigbee також має недоліки. Одним з них є обмежена швидкість передачі даних у порівнянні з іншими бездротовими технологіями, такими як Wi-Fi та Bluetooth. Мережі Zigbee також можуть бути менш масштабованими, ніж інші технології.

Загалом, Zigbee - це надійна технологія, яка підходить для використання в різних сферах. Вона має низьке енергоспоживання, високий рівень сигналу і широке покриття. Однак, перш ніж використовувати Zigbee, слід ретельно оцінити всі переваги і недоліки цієї технології.

1.4. Безпека

Мережі ZigBee характеризуються гарантованою стійкістю до перешкод, багатопроменевих завмирань і різних помилок і збоїв при передачі даних. До цього слід додати не тільки гарантовану, але й безпечну передачу, що важливо для багатьох критично важливих додатків. Легко уявити наслідки несанкціонованого втручання в системи управління технологічними процесами і безпеки. У той же час, для менш критичних застосувань повинна бути можливість знизити ціну обладнання за рахунок зниження вимог до безпеки. Саме такий підхід застосовано в моделі безпеки ZigBee: основним механізмом забезпечення конфіденційності в мережі ZigBee є забезпечення належного захисту всіх ключових даних. Основою безпеки є довіра, яка необхідна як на початковому етапі генерації ключів, так і при обробці інформації, пов'язаної з безпекою. Це означає, що дані повинні обмінюватися тільки між довіреними сторонами. Ця концепція послідовно пронизує всю ієрархію обміну даними.

Специфікація ZigBee визначає безпеку на рівнях NWK і APS і базується на базовій структурі безпеки, визначеній в стандарті IEEE 802.15.4. Комутатор є основою архітектури безпеки ZigBee. Їх захист є надзвичайно важливим, і ключі ніколи не повинні передаватися незахищеними каналами. Короткочасний (і єдиний) виняток з цього правила відбувається, коли до мережі додається раніше неналаштований пристрій: У специфікації ZigBee зазначено, що мережа, створена в конкретній ситуації, може бути фізично доступною для зовнішніх пристроїв, а конкретне робоче середовище може бути непередбачуваним. Крім того, різні додатки, що працюють одночасно і використовують для зв'язку один і той же трансивер, повинні взаємно довіряти один одному. З міркувань вартості ця модель не забезпечує брандмауер між об'єктами додатків. У стеку протоколів різні рівні не розділені криптографічно, тому політики доступу є обов'язковими і повинні бути розроблені належним чином. Відкрита модель довіри всередині пристрою дозволяє розділити ключі, що, серед іншого, знижує потенційну вартість пристрою. Однак рівень, який створює фреймворк, відповідає за його безпеку. Якщо існує ризик появи зловмисного пристрою, все корисне навантаження на рівні, який його створює, має бути зашифроване, щоб несанкціонований трафік міг бути негайно заблокований. Винятком є, як уже згадувалося, передача мережевого ключа на новий підключений пристрій для забезпечення єдиного рівня мережевої безпеки для цього пристрою.

Архітектура безпеки

Система безпеки ZigBee заснована на 128-бітному алгоритмі AES. Служби безпеки ZigBee, визначені в специфікації ZigBee, визначають генерацію ключів, управління пристроями і захист даних. Ключ може бути пов'язаний з мережею (і використовуватися ZigBee і MAC-підрівнем) або каналом зв'язку. Ключі можуть бути отримані шляхом попереднього встановлення, узгодження або передачі. Встановлення ключа каналу зв'язку базується на використанні головного ключа, який контролює відповідність ключів каналу зв'язку. Перший майстер-ключ повинен бути отриманий в безпечному середовищі (передача або попередня інсталяція), оскільки від нього залежить безпека всієї мережі. Майстер-ключі та

ключі каналів видимі лише на рівні програми. Різні сервіси використовують різні варіації ключів каналів зв'язку, щоб уникнути витоку та ризиків безпеки.Розподіл ключів - одна з найважливіших функцій мережевої безпеки. У захищеній мережі виділяється спеціальний пристрій - центр управління безпекою, від якого інші пристрої покладаються на розподіл ключів безпеки. В ідеалі, всі пристрої в мережі повинні мати адресу центру управління безпекою і перший попередньо встановлений майстер-ключ. Програми без особливих вимог до безпеки можуть використовувати мережеві ключі, які центр керування безпекою надсилає незахищеним каналом під час передачі. У такий спосіб центр керування безпекою захищає мережевий ключ і забезпечує безпеку "точка-точка". Пристрій приймає лише повідомлення, зашифровані за допомогою ключа, наданого центром управління безпекою, за винятком першого головного ключа.

Мережевий рівень керує маршрутизацією, обробляє вхідні повідомлення і може надсилати запити. Кадр-відправник використовує відповідний комутатор каналу зв'язку згідно з маршрутизацією, якщо такий є, або мережевий комутатор для захисту корисного навантаження від зовнішніх пристроїв.

Прикладний рівень генерує ключі та надає транспортні послуги як об'єкту пристрою (ZDO), так і додатку. Сповіщення можуть надходити від самого пристрою (наприклад, проста зміна статусу) або від центру управління безпекою (сповіщення про те, що певний пристрій було видалено з мережі). Цей рівень також маршрутизує запити пристроїв та оновлення мережевих ключів від центру керування безпекою до всіх пристроїв.Об'єкт пристрою ZDO підтримує політики безпеки пристроїв.

Центр управління безпекою. Важливим елементом концепції безпеки ZigBee є центр управління безпекою.На етапі формування або реконфігурації мережі центр управління безпекою дозволяє або забороняє новим пристроям приєднуватися до мережі.Центр управління безпекою може періодично оновлювати ключ мережі і переходити на новий ключ. Спочатку він транслює новий ключ, який зашифровано старим мережевим ключем. Потім він сповіщає всі пристрої про перехід на новий ключ.

Центр керування безпекою - це, як правило, координатор мережі, який працює за сумісництвом, але може бути і окремим пристроєм.

Центр керування виконує такі функції для забезпечення безпеки

а) Автентифікація пристроїв, які хочуть приєднатися до мережі,

б) управління та розгортання мережевих комутаторів; і

в) забезпечення безпечного зв'язку між пристроями.

Основні типи

ZigBee використовує три типи ключів для управління безпекою

а) Майстер-комутатори

б) мережевий комутатор

в) перемикач з'єднання.

Головний ключ.

Цей ключ не використовується для шифрування; він використовується як секретний код, яким обмінюються два пристрої, коли вони виконують процедуру генерації ключа зв'язку. Майстер-ключ, згенерований центром управління безпекою, називається майстер-ключем центру безпеки, а інші ключі - майстер-ключами на рівні додатків.

Мережевий ключ.

Це ключ для безпеки на рівні мережі; кожен пристрій у мережі ZigBee має мережевий ключ. Високозахищені мережеві ключі повинні передаватися тільки в зашифрованому вигляді через радіоканал. Стандартні мережеві ключі можна надсилати зашифрованими або незашифрованими.

Ключі каналу зв'язку.

Ці ключі забезпечують безпечну одноадресну передачу повідомлень між двома пристроями на рівні програми.

Стандартний режим безпеки

У стандартному режимі безпеки списки пристроїв, головні ключі, ключі каналів і мережеві ключі можна зберігати в Центрі керування безпекою або на самому пристрої. Однак Центр керування безпекою відповідає за збереження стандартних мережевих ключів і контролює політику допуску до мережі. У цьому

режимі вимоги до пам'яті Центру керування безпекою значно нижчі, ніж у режимі підвищеної безпеки.

Режим підвищеного рівня безпеки

У режимі підвищеного рівня безпеки центр керування безпекою зберігає списки пристроїв, головні ключі, ключі зв'язку та мережеві ключі, необхідні для оновлення мережевих ключів, а також для контролю та застосування політик доступу до мережі. У цьому режимі обсяг пам'яті, необхідний центру керування безпекою, швидко зростає зі збільшенням кількості пристроїв у мережі.

Zigbee - це незворотний протокол, який можна використовувати для захисту користувачів від різних додатків IoT (Інтернету речей). Інформація, яку необхідно передати, може містити конфіденційну інформацію, наприклад, конкретні дані та інформацію про безпеку, а безпека Zigbee необхідна для їхньої автентифікації та захисту від несанкціонованого доступу.

Одним з основних способів захисту Zigbee є шифрування даних. Кожен пристрій в мережі має власний ключ шифрування, який використовується для захисту передачі даних. Крім того, Zigbee може покладатися на автентифікацію на реальному пристрої, якщо він може перевірити, що він надходить легітимно.

Одним із способів забезпечення однорангової безпеки Zigbee є контроль доступу до мережевих ресурсів. Зловмисникам, які є авторизованими користувачами, можна дозволити доступ до даних, що передаються через сайт.

Zigbee також виграє при дистанційних атаках і може блокувати атаки на різні місця.

Для однорангової безпеки Zigbee аутентифікується за допомогою таких засобів, як перевірка цілісності даних і захист від атак однорангових інфекцій. Переміщення, які не можуть бути видалені з місця передачі і мають фізичний доступ до пристрою перехоплення.

1.5. Області використання БСМ

Бездротові сенсорні мережі (БСМ) - це мережі розподілених, невеликих, автономних пристроїв, які використовуються для вимірювання, обробки і передачі даних, пов'язаних з фізичними параметрами і процесами навколишнього середовища. Сьогодні WSN стали можливими завдяки прогресу в мікроелектроніці та дослідженням на перетині вимірювання, обчислень і бездротового зв'язку.

1) Схеми.

2) Зменшення енергоспоживання

- Розвиток мікроелектромеханічних систем (МЕМС);
- Мініатюризація та зниження вартості;
- Використання відновлюваних джерел енергії.

3) Обробка інформації

- Обчислювальна потужність;
- Вбудоване програмне забезпечення;
- Обробка даних на вузлах;
- Методи спільної обробки даних;

4) Мережеві технології

- Самоконфігурація.
- Масштабованість
- Динамічна топологія
- Управління топологією;
- Гібридні мережі
- Розподілена маршрутизація та планування;

5) Бездротовий зв'язок

- Багатоінтервальна маршрутизація

6) Енергоефективність

- Короткі робочі цикли
- Ефективний контроль доступу
- Зв'язок в єдиному частотному полі.

Бездротовий сенсорний вузол складається з шести основних компонентів: сенсорного блоку, аналого-цифрового перетворювача (АЦП), процесора, пам'яті, радіомодуля та джерела живлення. Блок обробки даних, що складається з процесора і пам'яті, є найважливішим компонентом бездротового сенсорного вузла; саме блок обробки даних приймає дані від АЦП, виконує арифметичні і логічні операції, зберігає отримані дані і передає їх на радіомодуль. Дослідженнями та розробкою апаратного та програмного забезпечення для WSN займаються відомі університети та найбільші виробники електроніки, такі як Intel, IBM, Texas Instruments, Microchip, Freescale, NXP та Atmel. На сьогоднішній день успішно завершені проекти з розробки та застосування WSN в різних сферах діяльності, таких як технічний та екологічний моніторинг, системи точного землеробства та цифрові зоопарки. У той же час, розвиток WSN стикається з низкою проблем, особливо пов'язаних зі збоями в передачі даних, обмеженими апаратно-обчислювальними ресурсами та електроживленням. Бездротові сенсорні мережі можуть збирати інформацію про стан фізичного середовища, забезпечувати просту обробку зібраних даних і передавати їх на віддалений сервер. Для задач моніторингу в БСМ здебільшого використовують топологію кластерного дерева. У цій топології сусідні вузли на шляху до базової станції є як джерелами інформації, так і ретрансляторами даних з інших вузлів. В принципі, базова станція передає дані через бездротові канали зв'язку (WiFi, GSM, супутник) на віддалений сервер, підключений до мережі Інтернет. На сучасному етапі основою для розвитку BSM є стандарт IEEE 802.15.4 і стек протоколів ZigBee. Стандарт був розроблений альянсом компаній, серед яких Invensys, Inc.

Стек протоколів ZigBee побудований на принципах ієрархічної семирівневої моделі протоколів передачі даних Open System Interconnection (OSI) і Open System OSI (Open System Interconnection). Стек включає в себе рівень IEEE 802.15.4, що відповідає за реалізацію каналу зв'язку, програмний мережевий рівень, визначений специфікацією ZigBee Alliance, і рівень підтримки додатків. На фізичному рівні сенсорної мережі передача даних здійснюється відповідно до стандарту IEEE

802.15.4. В якості середовища передачі даних використовуються радіоканали або відкриті інфрачервоні канали.

Стандарт IEEE 802.15.4 (ZigBee) передбачає роботу в трьох частотних діапазонах:

Один канал в діапазоні 868,0 - 868,6 МГц (для Європи);

10 каналів у діапазоні 902 - 928 МГц (центральна частота діапазону 2 МГц);

16 каналів у діапазоні 2450 МГц (центральна частота 5 МГц).

Однією з головних потреб до вузлів BSM є забезпечення заданих функцій при мінімальному споживанні струму. Це забезпечує тривалий час роботи від автономного джерела живлення. Одним з основних джерел енергоспоживання вузла є радіоприймач. Тому існує нагальна потреба у зменшенні енергоспоживання під час передачі даних.

До бездротових вузлів пред'являються наступні вимоги:

- Мінімальні розміри та вага; - Мінімальне енергоспоживання
- мінімальне енергоспоживання;
- Робота з великою кількістю вузлів в обмеженому просторі; і
- Автономність і робота без технічного обслуговування; і
- Здатність адаптуватися до навколишнього середовища;
- Низькі виробничі витрати.

Розроблено класифікацію БСМ, яка охоплює технологію передачі, середовище передачі, тип вузла, тип джерела живлення, область розгортання та область застосування. Технологія передачі Середовищем передачі, що використовується в WSN, є бездротові канали, бездротові оптичні канали і канали з магнітним наведенням. Середовище передачі даних. Залежно від середовища передачі даних розрізняють наземні, підземні та підводні БСМ. Наземні WSN характеризуються великою кількістю недорогих вузлів (від сотень до тисяч), які передають дані на базову станцію. Оскільки джерела живлення обмежені і часто не підлягають заміні, сенсорні вузли можуть використовувати відновлювані джерела енергії, такі як сонячні батареї.

Вони використовують поновлювані джерела енергії, такі як сонячні батареї. Для економії енергії вузли використовують багатохопову маршрутизацію. Підземні WSN складаються з масиву сенсорних вузлів, розміщених під землею або в обмеженому просторі, наприклад, в печерах, шахтах і метро. Основна відмінність між підземними і наземними WSN полягає в середовищі передачі даних, яке характеризується високим рівнем загасання і втрат сигналу, що необхідно враховувати при розробці протоколів передачі даних. Підводні WSN складаються з датчиків, розміщених під водою для моніторингу моря або океану. Підводні мережі використовують акустичні хвилі і тому страждають від обмежень пропускної здатності, довгих затримок поширення і згасання сигналу. Підводні вузли повинні бути здатні адаптуватися до екстремальних умов навколишнього середовища в океані. Підводні WSN використовуються для моніторингу забруднення, сейсмічного моніторингу, моніторингу обладнання та підводної робототехніки. Мобільні WSN Вузли в мобільних WSN можуть рухатися і взаємодіяти з фізичним середовищем. При розробці БСМ з мобільними вузлами можуть виникати проблеми з локалізацією вузлів, маршрутизацією і контролем мобільних вузлів, підтримкою зв'язності мережі, мінімізацією енергоспоживання в русі і розробкою протоколів динамічної маршрутизації. При розробці протоколів маршрутизації необхідно враховувати швидкість, з якою рухається вузол, і максимальну відстань, на яку можуть змінюватися координати вузла. Застосування бездротових сенсорних мереж Залежно від застосування, в БСМ можуть використовуватися різні типи датчиків, такі як датчики температури, вологості, руху, тиску, стану ґрунту, шуму, диму, хімічного складу (речовин, повітря), наявності або відсутності певних типів об'єктів, визначення швидкості, напрямку і розміру об'єктів, аудіо- та відеоданих і т.д. Основними сферами застосування БСМ є екологічний і технічний моніторинг, точне землеробство, охорона здоров'я, "розумні" будинки і системи безпеки.

Екологія.

В екологічних додатках WSN використовують для відстеження пересування птахів,

Для моніторингу пересування дрібних тварин і комах;

Моніторинг стану навколишнього середовища;

екологічних умов, що впливають на врожай і поголів'я худоби;

Точне землеробство;

Біологічний моніторинг;

Моніторинг забруднення навколишнього середовища: повітря, водних ресурсів (включаючи океани), виявлення лісових пожеж; метеорологічні або геофізичні дослідження;

Медичні послуги: фізіологічний моніторинг (частота серцевих скорочень, кров'яний тиск, температура, частота дихання, рівень стресу та інші життєво важливі показники); невідкладна допомога; моніторинг поведінки людей похилого віку; моніторинг персоналу та пацієнтів у лікарнях. Фізіологічні дані, зібрані сенсорною мережею, можуть зберігатися протягом тривалого часу і використовуватися для медичних досліджень.

Вони можуть бути використані для медичних досліджень.

Розумний будинок З розвитком технології розумного будинку бездротові вузли будуть інтегровані в побутову техніку, таку як пилососи, мікрохвильові печі, холодильники, люстри, мультиварки і кавомашини. Це дозволяє пристроям спілкуватися один з одним і з зовнішніми мережами через Інтернет або супутник. Системи технічного спостереження БСМ ефективно використовуються в системах технічного спостереження, особливо в моніторингу мостів, нафтових танкерів і газопроводів, будівель і споруд в сейсмонебезпечних зонах, а також в системах обліку енергії для особистого і промислового використання.

Системи безпеки BSM використовуються в системах особистої та промислової безпеки, таких як контроль периметра, виявлення вторгнень та віддалений моніторинг. Запропонований метод базується на технології бездротових сенсорних мереж і дозволяє швидко модифікувати світлофори для організації "зелених коридорів" для транспортних засобів спеціального призначення. Транспортні засоби спеціального призначення оснащуються радіокеруванням з запрограмованим кодом доступу. Коли транспортний засіб потрапляє в зону дії (0,1-1,0 км) радіомодуля, встановленого в світлофорі, відбувається передача коду доступу, і світлофор

переходить в режим "Увага" (жовтий миготливий колір) за певним алгоритмом. При віддаленні від зони зв'язку світлофор переходить у звичайний режим роботи. Щоб унеможливити несанкціонований доступ до керування світлофором, усі команди передаються в зашифрованому вигляді. Для захисту команд використовується 128-бітний алгоритм шифрування AES та модифікована схема стрибкоподібної зміни частоти. Радіомодулі, встановлені на одному перехресті, об'єднані в мережу для коректного обміну сигналами світлофорів у зоні перехрестя. Мережа організована за топологією "зірка" або "сітка" на основі ZigBee-модулів одного типу маршрутизатора. Модулі ZigBee, розміщені в світлофорах, мають функцію документування, яка зберігає час і код пристрою, що керує світлофором, у флеш-пам'яті. При необхідності дані з флеш-пам'яті можна зчитати через бездротовий інтерфейс. Якщо підключені відеосенсори, мережа може бути використана для моніторингу дорожнього руху. Такий підхід до організації "зеленого коридору" підвищує швидкість і безпеку проїзду транспортних засобів спеціального призначення через регульовані перехрестя, а також зменшує необхідність зупинки світлофора на тривалий час.

1.6. ZigBee радіо модулі (JN5139, XBee PRO, Texas Instruments)

ZigBee є бездротовою технологією, що може бути використана для зменшення кількості операцій з низькою швидкістю передачі даних та низьким споживанням енергії. ZigBee радіомодуль обирається для створення бездротових мереж у різноманітних промислових та побутових застоях, таких як автоматизація будинку, системи контролю доступу, моніторинг середовища тощо.

Радіомодуль ZigBee працює на частотах 2,4 ГГц, 868 МГц або 915 МГц і може передавати дані на відстані до 100 метрів у прямому напрямку. Вони можуть низько підтримувати енергію, що дає змогу використовувати їх в автономному режимі на батареях, що протягують три години.

Радіомодуль ZigBee може використовувати вбудований протокол протоколу ZigBee, який дає змогу створювати нешкідливі з'єднання з високим рівнем безпеки

та надійності. Крім того, радіомодуль ZigBee підтримує меншу топологію "дзеркало", "дерево" і "меш", що дає змогу створювати меншу кількість різних складів і розмірів.

Один із виробників радіомодулів ZigBee від компанії Digi International, яка пропонує широкий асортимент модулів для різних цілей. Іншими перевіреними виробниками є XBee від компаній MaxStream та JN516x від NXP Semiconductors.

Узагальчи, радіомодуль ZigBee - це бездротова технологія з низькою швидкістю передавання даних і низьким споживанням енергії, як використовується для створення бездротових мереж у різних промислових і побутових застоях. Ви можете використовувати вбудований протокол ZigBee, який дає змогу створювати безпечні та надземні мережі з невеликим запасом і швидкістю.

ZigBee радіомодуль JN5139 - це низькопотужний радіочастотний модуль, що використовується для захисту бездротової ланки на відстані до 500 метрів у промислових і побутових умовах. Розробник цього модуля - компанія NXP Semiconductors.

JN5139

JN5139 має вбудований процесор ARM7 з тактовою частотою 32 МГц, а також радіочастотний блок, що підтримує роботу в діапазоні 2,4 ГГц і 784/868/915 МГц. Модуль може використовувати стандартну бездротову мережу ZigBee Pro і може працювати в режимі маршрутизатора або координатора.JN5139 підтримує безпечне шифрування AES-128 і механічний обмін ключами. Крім того, модуль великого об'єму промислового та цифрового ШІМ-контролера, що дає змогу керувати електродвигунами та іншими приладами.Встановлення радіомодуля ZigBee JN5139 можна розпізнавати в багатьох галузях, таких як автоматизація будівель, промисловий контроль, системи безпеки та багато в інших.

XBee PRO

ZigBee радіомодуль XBee PRO - це бездробильні радіомодулі, як перевірена технологія ZigBee для передачі даних. Компанія Digi International працює в різних конфігураціях, перемикаючи різні частоти діапазонів, потужність передач і типи антен.Модуль XBee PRO може мати багатофункціональні функції, що включають

менш жорстку маршрутизацію, без необхідності заважати і забезпечувати енергетичне постачання. Також можна використовувати різні типи з'єднань, такі як UART, SPI та I2C.Ці модулі можуть бути збережені для безвідмовних передач даних у різних точках, таких як системи автоматизації виробництва, системи контролю доступу та системи моніторингу середовища.

Один із головних перетворювачів радіомодуля ZigBee XBee PRO має найнижчий рівень енергоспоживання, що дає змогу допускати їхнє використання в батарейних пристроях із постійним терміном служби. Крім того, вони можуть мати високу надбавку і можуть працювати в різних умовах середовища.Завантажуваний, ZigBee радіомодуль XBee PRO - цей бездротовий радіомодуль, який можна під'єднати до радіостанції для передавання даних у різних джерелах із низьким рівнем споживання енергії та високою надійністю.

Texas Instruments

ZigBee радіомодуль Texas Instruments - це бездонний радіомодуль, який підтримує протокол ZigBee для передачі даних на відстані до 100 метрів. Ці модулі були вироблені компанією Texas Instruments, і вони можуть бути побудовані для виробництва бездротових заходів з контролем за енергопостачанням.

Основною перевагою ZigBee радіомодулів Texas Instruments є їхнє низьке енергоспоживання. Це дозволяє їм працювати на батарейках протягом тривалого часу, що робить їх ідеальними для застосування в бездротових сенсорних мережах. Крім того, цей модуль може мати низьку вартість і може бути легко інтегрований з більш низькими частотами.Texas Instruments пропонує широкий спектр ZigBee-радіомодулів, які можуть бути затребувані в будь-якій бездроновій мірі. Наклад, CC30 є найбільш популярним серед популярних модифікацій, який може використовуватися в різних цілях, наприклад, для виконання різних замін. Крім того, Texas Instruments пропонує радіомодулі ZigBee з різними інтерфейсами, оснащеними UART, USB і Ethernet.Використовувані, радіомодулі ZigBee Texas Instruments з ефективними та надійними компонентами для забезпечення бездріжджового енергоспоживання, а також контролю споживання енергії.

Висновки до розділу

У першому розділі кваліфікаційної роботи було проведено аналіз бездротової технології ZigBee. Було досліджено основні характеристики технології, такі як швидкість передачі даних, надійність, безпека, області використання та інші. Також було проаналізовано переваги та недоліки використання ZigBee у порівнянні з іншими бездротовими технологіями.

За результатами аналізу можна зробити висновок, що технологія ZigBee є ефективною для використання в мережах з низькою швидкістю передачі даних та обмеженими ресурсами енергопостачання. Вона також є популярною у застосуваннях Інтернету речей (IoT), таких як датчики, контролери тощо.

Проте, необхідно враховувати недоліки технології, такі як обмежена дальність зв'язку та низька швидкість передачі даних порівняно з іншими бездротовими технологіями. Також, використання ZigBee може бути обмеженим у випадках, коли потрібна висока точність передачі даних.

У цілому, аналіз бездротової технології ZigBee показав, що вона є ефективною для використання у застосуваннях IoT та мережах з низькою швидкістю передачі даних та обмеженими ресурсами енергопостачання.

РОЗДІЛ 2.
АНАЛІЗ ФУНКЦІОНАЛЬНОГО ВУЗЛА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ.

2.1. Аналіз функціонування вузла бездротової сенсорної мережі

Вузол бездротової сенсорної мережі (WSN) - це автономний пристрій, який може відчувати, обробляти і передавати дані бездротовим способом. Вузли WSN - це, як правило, невеликі, малопотужні пристрої, які можуть бути розгорнуті у великій кількості, щоб сформувати мережу, яка може відстежувати фізичні або екологічні умови в реальному часі. У цьому всебічному аналізі ми детально розглянемо функціонування вузла бездротової сенсорної мережі.

Основними компонентами вузла WSN є сенсорний блок, блок обробки, блок зв'язку та блок живлення. Сенсорний блок складається з одного або декількох датчиків, які можуть вимірювати фізичні параметри або параметри навколишнього середовища, такі як температура, вологість, інтенсивність світла, тиск тощо. Обробний блок обробляє дані, отримані від сенсорного блоку, і виконує необхідні обчислення. Блок зв'язку відповідає за бездротову передачу оброблених даних на інші вузли або базові станції. Блок живлення забезпечує вузол енергією для його функціонування. Функціонування вузла WSN можна розділити на три етапи: етап зондування, етап обробки та етап комунікації.

На етапі зчитування датчик(и) у вузлі визначають фізичний параметр(и) або параметр(и) навколишнього середовища і перетворюють їх в електричні сигнали. Потім ці сигнали надсилаються до блоку обробки для подальшого аналізу.

На етапі обробки блок обробки виконує необхідні обчислення над отриманими даними. Це може включати фільтрацію, усереднення, згладжування або інші методи обробки сигналів для видалення шуму або вилучення релевантної інформації з необроблених даних.

На етапі зв'язку оброблені дані передаються бездротовим способом на інші вузли або базові станції за допомогою радіочастотних (РЧ) протоколів зв'язку, таких

як Zigbee, Bluetooth Low Energy (BLE), Wi-Fi або стільникові мережі. Протокол зв'язку, що використовується, залежить від таких факторів, як відстань між вузлами, вимоги до швидкості передачі даних, обмеження енергоспоживання та топологія мережі.Вузли WSN можуть бути розгорнуті в різних сферах застосування, таких як моніторинг навколишнього середовища, моніторинг охорони здоров'я, промислова автоматизація, розумні будинки/будівлі/міста, моніторинг сільського господарства та багато інших. Розгортання вузлів WSN вимагає ретельного врахування таких факторів, як розміщення вузлів, топологія мережі, енергоспоживання, маршрутизація даних і безпека.Отже, вузол WSN – це. автономний пристрій, який може сприймати, обробляти та передавати дані бездротовим способом. Його функціонування включає в себе три етапи: зондування, обробку та передачу даних. Вузли WSN мають різні застосування і вимагають ретельного підходу під час розгортання.

2.2. Розрахунок часу роботи вузла

Формула для розрахунку часу роботи вузла залежить від декількох факторів, таких як час обробки, час очікування, час передачі та час відновлення. Основна формула для розрахунку часу роботи вузла складається з суми цих факторів:

Час роботи вузла = Час обробки + Час очікування + Час передачі + Час відновлення

Час обробки - це час, необхідний для виконання завдання вузлом. Цей час може бути розрахований на основі складності завдання та швидкості обробки.

Час очікування - це час, протягом якого завдання перебуває у черзі на обробку. Цей час може бути розрахований на основі кількості завдань у черзі та середнього часу обробки.

Час передачі - це час, необхідний для передачі даних до та з вузла. Цей час може бути розрахований на основі швидкості передачі даних та обсягу даних.

Час відновлення - це час, необхідний для відновлення вузла після збою або перерви. Цей час може бути розрахований на основі середнього часу відновлення та частоти збоїв.

Точна формула для розрахунку часу роботи вузла може бути складною, оскільки залежить від багатьох факторів, які можуть змінюватися з часом.Не існує єдиної точної формули для розрахунку часу безвідмовної роботи вузла, оскільки цей час залежить від багатьох факторів, таких як тип вузла, обчислювальна потужність і кількість запитів, отриманих вузлом.

Однак, для розрахунку середнього часу, необхідного вузлу для обслуговування запиту, можна використовувати наступну формулу:

$$T = (N / X) + S$$

(1.1)

В даній формулі :

T - час роботи вузла,

N - кількість запитів, отриманих вузлами

X - пропускна здатність вузла (кількість запитів, які вузол може обробити за одиницю часу)

S - середній час, необхідний вузлу для обробки одного запиту.

Ця формула дає загальне уявлення про час безвідмовної роботи вузла, але для отримання більш точних результатів можна використовувати інші методи розрахунку.

Для розрахунку часу безвідмовної роботи вузла можна використовувати закон Кірхгофа. Закон Кірхгофа - це математична формула, яка дозволяє знайти значення струму або напруги в кожному вузлі електричної мережі. Ці правила базуються на законі збереження енергії та законі Ома.

Щоб розрахувати час роботи вузла, потрібно знати значення струму, що протікає через цей вузол, і опір інших вузлів, підключених до нього. Використовуючи закон Кірхгофа, ми можемо написати одночасне лінійне рівняння, що описує зв'язки між вузлами електричної мережі. Розв'язання цього одночасного рівняння дозволяє визначити значення струму в кожному вузлі.

Перший закон Кірхгофа.

У кожному вузлі електричного кола алгебраїчна сума значень струмів, які об'єднуються в цьому вузлі, дорівнює нулю, або алгебраїчна сума струмів, що вливаються у вузол електричного кола, дорівнює алгебраїчній сумі струмів, що витікають з цього вузла.

Перший закон описує зв'язок між сумою струмів, що вливаються у вузол електричного кола (додатні струми), і сумою струмів, що витікають з цього вузла (від'ємні струми). Згідно з цим законом, алгебраїчна сума струмів, що збігаються в будь-якій точці вітки провідника, дорівнює нулю (1):

$$\sum_k I_k = 0.$$

(1)

Перший закон Кірхгофа є наслідком закону збереження заряду. Він відповідає рівнянню неперервності для струмів, неперервно розподілених у просторі.

Другий закон Кірхгофа.

Для будь-якого дроту в замкненому контурі алгебраїчна сума електрорушійної сили дорівнює алгебраїчній сумі добутків сили струму в кожній ділянці контуру на опір цієї ділянки з урахуванням внутрішнього опору джерела струму.

Математично другий закон Кірхгофа записується наступним чином (2):

$$\sum_i \mathcal{E}_i = \sum_k I_k R_k.$$

(2)

Застосування.

Якщо послідовно застосувати закон Кірхгофа до всіх вузлів і контурів складної електричної мережі, можна скласти повний набір одночасних рівнянь для визначення струмів у кожній ділянці.

Щоб розрахувати ланцюг, спочатку намалюйте схему електричного кола і довільно позначте стрілкою напрямок струму в кожній ділянці. Потім виберіть замкнутий контур і перетніть його в довільно обраному напрямку. Якщо стрілка, що

вказує на напрямок струму, вказує на напрямок обходу, то добуток відповідного струму і опору береться зі знаком мінус.

Якщо обхід проходить від негативного полюса до позитивного полюса джерела струму, то ЕРС записується зі знаком плюс, в іншому випадку - зі знаком мінус. Отримана система рівнянь використовується для визначення густини струму. Той факт, що густина струму від'ємна, означає, що напрямок струму на цій ділянці насправді (довільно) протилежний напрямку, обраному на початку розв'язку, але не впливає на швидкість або точність чисельного розв'язку.

Нехай електричне коло складається з двох джерел напруги і трьох резисторів.

Згідно з першим законом:

$$i_1 - i_2 - i_3 = 0$$

Застосовуючи другий закон до замкненого кола s1, отримаємо:

$$-R_2 i_2 + \mathcal{E}_1 - R_1 i_1 = 0$$

Застосовуючи другий закон до замкненого контуру s2:

$$-R_3 i_3 - \mathcal{E}_2 - \mathcal{E}_1 + R_2 i_2 = 0$$

Отримаємо систему лінійних рівнянь:

$$\begin{cases} i_1 - i_2 - i_3 & = 0 \\ -R_2 i_2 + \mathcal{E}_1 - R_1 i_1 & = 0 \\ -R_3 i_3 - \mathcal{E}_2 - \mathcal{E}_1 + R_2 i_2 & = 0 \end{cases}$$

Котра еквівалентна:

$$\begin{cases} i_1 + (-i_2) + (-i_3) & = 0 \\ R_1 i_1 + R_2 i_2 + 0 i_3 & = \mathcal{E}_1 \\ 0 i_1 + R_2 i_2 - R_3 i_3 & = \mathcal{E}_1 + \mathcal{E}_2 \end{cases}$$

Іншими словами, закон Кірхгофа можна використовувати для розрахунку часу роботи вузлів електричної мережі.

2.3. Розрахунок часу життя кінцевого пристрою

Для розрахунку часу життя кінцевого пристрою необхідно враховувати кілька факторів, таких як тип пристрою, його використання та умови зберігання.

Один з основних факторів, який впливає на час життя пристрою - це тип батареї, якою він оснащений. Батареї мають обмежену кількість циклів заряду-розряду, після яких їх потрібно замінити. Таким чином, час життя кінцевого пристрою може бути обмеженим кількістю циклів заряду-розряду батареї.

Іншим фактором є використання пристрою. Чим більше часу ви проводите на своєму пристрої, тим швидше вона зношується і може потребувати ремонту або заміни.

Також важливо враховувати умови зберігання пристрою. Висока температура, вологість або механічні пошкодження можуть призвести до зниження часу життя пристрою.

Для розрахунку часу роботи сенсорного вузла на базі протоколу Zigbee необхідно враховувати кілька факторів, таких як тип використовуваного вузла, його енергоспоживання, тип батареї та її ємність, а також інтенсивність використання мережі.

Зазвичай, сенсорні вузли на базі протоколу Zigbee мають низьке енергоспоживання та можуть працювати на одній батареї протягом декількох місяців або навіть року. Залежно від типу використовуваного сенсора та його параметрів, час роботи може коливатися від кількох місяців до кількох років.

Одним з ключових факторів, який впливає на час роботи сенсорного вузла на базі протоколу Zigbee, є інтенсивність використання мережі. Якщо сенсорний вузол використовується в мережі з високою інтенсивністю трафіку, то це може призвести до скорочення часу роботи батареї. Однак, якщо мережа має низьку інтенсивність трафіку, то це дозволяє сенсорному вузлу працювати на одній батареї протягом довгого часу.

Також важливо враховувати тип батареї та її ємність. Наприклад, батареї типу CR2032 мають ємність близько 200 мА * год, тоді як батареї типу AA можуть мати ємність до 3000 мА * год. Це означає, що сенсорний вузол з батареєю CR2032 буде працювати менше, ніж сенсорний вузол з батареєю типу AA.

Отже, для розрахунку часу роботи сенсорного вузла на базі протоколу Zigbee необхідно враховувати тип використовуваного вузла, його енергоспоживання, тип батареї та її ємність, а також інтенсивність використання мережі.

2.4. Спосіб продовження роботи мережі за допомогою алгоритму

Перспективність і актуальність використання технології бездротових сенсорних мереж (БСМ) для виконання завдань моніторингу та управління в таких галузях, таких як автоматизація підприємств, безпека, екологія, надзвичайні ситуації залучили до досліджень провідні наукові центри та лабораторії світу. До основних переваг технології БСМ належить можливість створення самоорганізованих мереж, які використовують дешеві мініатюрні автономні обчислювальні пристрої [1]. Однак існують проблеми, які перешкоджають масовому впровадженню рішень на базі БСМ. Одна з них – це необхідність збільшення часу автономної роботи безпровідної мережі. Оскільки живлення вузлів БСМ здійснюється від батарей обмеженої ємності, то завдання управління витратами енергоресурсу сенсорних вузлів є одним із основних.

Спосіб продовження роботи мережі за допомогою алгоритму.

В сучасному світі комп'ютерні мережі є невід'ємною частиною багатьох організацій та підприємств. Проте, якщо мережа перестає працювати, це може призвести до серйозних наслідків, таких як втрата даних або зупинка роботи всього підприємства. Тому важливо мати ефективний спосіб продовження роботи мережі в разі виникнення неполадок.

Один з таких способів - це використання алгоритму, який дозволяє продовжувати роботу мережі навіть у разі виникнення проблем. Основна ідея

полягає в тому, що якщо один з пристроїв у мережі перестає працювати, інші пристрої можуть автоматично прийняти на себе його функції.

Існують різні алгоритми, які можуть бути використані для продовження роботи мережі. Один з них - це алгоритм "Spanning Tree Protocol" (STP). Цей алгоритм дозволяє уникнути петель у мережі, що можуть призвести до збоїв. STP визначає найкоротший шлях до кореневого моста та блокує всі інші шляхи, що приводять до петель.

Інший алгоритм - це "Virtual Router Redundancy Protocol" (VRRP). Цей алгоритм дозволяє створювати віртуальний IP-адресу, яка може бути використана як захисний механізм у разі виникнення проблем з основним маршрутизатором. Коли основний маршрутизатор перестає працювати, віртуальна IP-адреса автоматично перенаправляється на резервний маршрутизатор.

Також існують алгоритми, які дозволяють автоматично перенаправляти трафік на інші пристрої у разі виникнення проблем. Один з них - це "Hot Standby Router Protocol" (HSRP). Цей алгоритм дозволяє створювати віртуальний IP-адресу, яка може бути використана як захисний механізм у разі виникнення проблем з основним маршрутизатором. Коли основний маршрутизатор перестає працювати, віртуальна IP-адреса автоматично перенаправляється на резервний маршрутизатор.

Усі ці алгоритми дозволяють продовжувати роботу мережі навіть у разі виникнення проблем. Вони дозволяють забезпечити безперебійну роботу мережі та запобігти втратам даних та зупинці роботи підприємства.

Для вирішення завдання максимізації часу життя сенсорної мережі запропоновано новий енергозбе рігаючий метод моніторингу цілей у зонах спостереження сенсорів БСМ. Для визначення маршрутів передачі зібраної інформації за сесіями спостере- ження запропоновано два нові види метрик, які враховують поточний (залишковий) запас енергії вузліві надійність безпровідних з'єднань. Перша метрика може бути використана окремо для вирішення завдань пошуку оптимальних маршрутів. У цій метриці застосовуються функції вартості переходу, в яких враховується інформація про якість зв'язку. Друга метрика в поєднанні з першою додатково вра- ховує залишкові запаси енергії вузлів для динамічного балансування

мережевого навантаження між ними. Розроблені метрики можуть бути успішно використані в БСМ із надлишковою кількістю вузлів під час стеження за цілями моніторингу для вирішення завдання збільшення часу життя мережі.

2.5. Спосіб розподіленого балансування трафіку в БСМ

Спосіб розподіленого балансування трафіку в БСМ полягає у розподілі навантаження між декількома серверами з метою забезпечення оптимальної продуктивності та надійності мережевих додатків. Цей метод передбачає використання спеціального програмного забезпечення, яке автоматично розподіляє трафік між серверами на основі певних алгоритмів. Розподілене балансування трафіку є важливою задачею в бездротових сенсорних мережах (WSN), оскільки вони зазвичай мають обмежені ресурси, такі як енергія, пропускна здатність та обчислювальна потужність. Це означає, що необхідно ефективно керувати ресурсами, щоб забезпечити максимальну продуктивність та продовжити тривалість роботи мережі.

Одним з найбільш поширених методів розподіленого балансування трафіку є метод Round Robin, який полягає у послідовному розподілі запитів між серверами. Іншими популярними методами є Least Connections, Weighted Round Robin та IP Hash.

Метод Least Connections використовується для розподілу трафіку на основі кількості активних з'єднань на кожному сервері. Сервер з меншою кількістю активних з'єднань отримує більше запитів.

Метод Weighted Round Robin дозволяє встановлювати вагу для кожного сервера, що впливає на його пріоритет при розподілі трафіку. Сервер з більшою вагою отримує більше запитів.

Метод IP Hash використовується для розподілу трафіку на основі IP-адреси клієнта. Кожен запит направляється на сервер, який визначається за допомогою хеш-функції, яка обчислюється на основі IP-адреси клієнта.

Один з методів розподіленого балансування трафіку - це метод використання маршрутних протоколів, таких як AODV (Ad-hoc On-demand Distance Vector) та DSR (Dynamic Source Routing). Ці протоколи дозволяють визначати оптимальний шлях для передачі даних в мережі. Крім того, вони можуть бути налаштовані для балансування навантаження на різних шляхах, що дозволяє зменшити перевантаження на окремих вузлах мережі.

Інший метод - це використання протоколів маршрутизації, які базуються на стані мережі, таких як OLSR (Optimized Link State Routing) та TBRPF (Topology Broadcast based on Reverse-Path Forwarding). Ці протоколи дозволяють визначати стан кожного вузла мережі та використовувати цю інформацію для балансування навантаження на різних шляхах.

Також можна використовувати методи, які базуються на розподілі навантаження на різних рівнях мережі. Наприклад, можна використовувати механізми балансування навантаження на рівні маршрутизатора або на рівні додатку. На рівні маршрутизатора можна використовувати методи, такі як Equal-Cost Multi-Path (ECMP), що дозволяє розподіляти трафік між різними шляхами з однаковою пропускною здатністю. На рівні додатку можна використовувати методи, такі як Round Robin або Weighted Round Robin, що дозволяють розподіляти трафік між різними вузлами мережі залежно від їх потужності.

Узагальнюючи, існує кілька методів розподіленого балансування трафіку в бездротових сенсорних мережах. Вибір конкретного методу залежить від характеристик мережі та вимог до продуктивності.

Висновки до розділу

Здійснюючи аналіз функціонального вузла бездротової сенсорної мережі, було виявлено, що такий вузол складається з декількох компонентів, які взаємодіють між собою. Основними компонентами є сенсорні вузли, які забезпечують збір і передачу даних, трансмітери, які передають дані до базової станції, та базова станція, яка обробляє отриману інформацію та забезпечує її передачу на сервер.

Одним з головних завдань функціонального вузла бездротової сенсорної мережі є забезпечення надійності та ефективності передачі даних. Для цього необхідно

правильно планувати розташування сенсорних вузлів та трансмітерів, а також використовувати оптимальні протоколи передачі даних.

Крім того, важливим аспектом є забезпечення безпеки передачі даних. Для цього можуть використовуватися різноманітні методи шифрування та аутентифікації даних.

Отже, аналіз функціонального вузла бездротової сенсорної мережі є важливим етапом у проектуванні та розгортанні таких мереж. Врахування особливостей компонентів та їх взаємодії дозволяє забезпечити надійну та ефективну роботу мережі.

РОЗДІЛ 3.
МОДЕЛЮВАННЯ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ ZigBee ЗА ДОПОМОГОЮ ПРОГРАМНОГО ПАКЕТУ Castalia.

3.1. Симулятор

Castalia - це симулятор мережі з низьким енергоспоживанням. Унікальність цього симулятора полягає в тому, що команда розробників взялася реалізувати не лише модель на рівні передачі даних, а й модель фізичних процесів, зібраних у вузлах. В результаті бездротові датчики пов'язані між собою не лише бездротовими каналами зв'язку, а й фізичними процесами, які вимірюють їхні параметри. Перевага моделі Castalia полягає в тому, що команда розробників від самого початку поставила собі за мету змоделювати всі аспекти роботи бездротової сенсорної мережі.

Вихідний код є відкритим і, що найважливіше, середовище моделювання, на якому він базується, також є відкритим і вільно поширюється для некомерційного використання.

Система Castalia

Castalia - це керований подіями дискретно-часовий симулятор, написаний на C++. Castalia розповсюджується під некомерційною ліцензією та комерційною ліцензією для використання в навчальних закладах та некомерційних дослідницьких організаціях. Симулятор підтримує написані користувачем модулі і працює на Linux та Unix-подібних операційних системах. Castalia - це універсальна система моделювання BSS. Більшість вихідного коду може бути доступною в оригінальній формі.

Переваги та недоліки

Перш за все, Castalia надає потужні інструменти для моніторингу та налагодження. Вона також підтримує широкий спектр операцій з радіоканалами і підтримує багато MAC-протоколів. Крім того, Castalia може імітувати проблеми зі споживанням енергії в BSS.

Однак, існують деякі обмеження. Наприклад, кількість доступних протоколів недостатньо велика.

Ми будемо продовжувати використовувати систему Castalia через її великі можливості моделювання (особливо в радіоканалі).

Castalia - це система моделювання на основі платформи OMNeT++ для бездротових сенсорних мереж (БСМ) та мереж малопотужних вбудованих пристроїв в цілому, з розширеними радіомоделями, радіоканалами з реалістичною поведінкою вузлів. Він може бути використаний дослідниками та розробниками, які хочуть протестувати алгоритми та протоколи в реальних умовах. Castalia також легко конфігурується і може імітувати широкий спектр платформ, а отже, може використовуватися для характеристики різних платформ для конкретних застосувань.

Основними характеристиками Castalia є-

1.Удосконалена модель каналу, заснована на емпіричних даних вимірювань:

- Модель системи враховує втрату зв'язку між вузлами, а також втрату каналів передачі даних;

- Комплексна модель мінливості втрат в каналах;

- Повна підтримка мобільності вузлів;

- Перешкоди оцінюються на рівні прийнятого сигналу, а не як окрема функція.

2.Вдосконалені радіомоделі на основі реальних малопотужних пристроїв бездротового зв'язку:

- Ймовірність прийому залежить від SINR, розміру пакета і схеми модуляції; Підтримується PSK і FSK модуляція; Користувацька модуляція може бути визначена шляхом вказівки кривих SNR-BER;

- Кілька рівнів потужності передачі можуть бути налаштовані індивідуально;

- Підтримує різні стани енергоспоживання та затримки переходу між станами;

- Реалістичне моделювання несучої RSSI

3.Розширене моделювання вимірювального пристрою:

- Гнучке фізичне моделювання процесу вимірювання;

- Підтримка шуму, зміщення та енергоспоживання лічильника.

4.Доступний протокол MAC.

5.Призначений для адаптації та розширення.

Нарешті, Castalia розроблена з нуля, так що користувачі можуть легко впроваджувати/імпортувати свої власні алгоритми і протоколи, а Castalia піклується про моделювання; модульність, надійність і швидкість Castalia частково обумовлені OMNeT++.

3.2. Налаштування початкових параметрів мережі

Для налаштування початкових параметрів мережі необхідно виконати наступні кроки:

1. Визначити IP-адресу маршрутизатора та підключитися до нього за допомогою програми для налаштування мережевого обладнання, такої як PuTTY або Tera Term.

2. Увійти до конфігураційного режиму маршрутизатора, використовуючи логін та пароль адміністратора.

3. Налаштувати основні параметри мережі, такі як IP-адресу, маску підмережі та шлюз за замовчуванням.

4. Налаштувати DNS-сервери, щоб забезпечити правильне розподілення доменних імен.

5. Налаштувати безпеку мережі, включаючи налаштування брандмауера та функції шифрування.

6. Зберегти налаштування та перезавантажити маршрутизатор для застосування змін.

Таким чином, налаштування початкових параметрів мережі досить просте, але потребує певних знань та навичок.

Для налаштування початкових параметрів мережі на базі протоколу Zigbee необхідно виконати наступні кроки:

1. Встановити координатор мережі Zigbee. Це може бути здійснено за допомогою спеціального пристрою, наприклад, координатора USB Zigbee.

2. Налаштувати параметри мережі. Для цього можна використовувати програмне забезпечення, що постачається з координатором або ж іншими програмами для роботи з мережами Zigbee. В параметрах мережі визначаються такі значення, як ідентифікатор мережі, канал радіочастоти, швидкість передачі даних та інші.

3. Додати до мережі новий пристрій Zigbee. Для цього необхідно виконати певну послідовність дій, що залежить від типу пристрою та його виробника. Зазвичай ця послідовність детально описана в інструкції користувача пристрою.

4. Налаштувати параметри пристрою. Це може бути здійснено за допомогою програмного забезпечення, що постачається з пристроєм або ж іншими програмами для роботи з мережами Zigbee. В параметрах пристрою визначаються такі значення, як ідентифікатор пристрою, тип пристрою, швидкість передачі даних та інші.

5. Перевірити налагоджену мережу та пристрій. Для цього можна використовувати спеціальні програми для моніторингу мереж Zigbee або ж використовувати функції самого пристрою.

У разі виникнення проблем з налаштуванням мережі Zigbee рекомендується звернутися до документації виробника або до фахівців з питань налаштування мереж.

Щоб налаштувати початкові параметри мережі на основі протоколу ZigBee за допомогою програмного пакету Castalia, ви можете виконати наступні кроки:

1. Встановіть Castalia: По-перше, вам потрібно завантажити та встановити програмний пакет Castalia на вашу систему. Ви можете знайти останню версію Castalia на її офіційному сайті.

2. Налаштуйте сценарій моделювання: Після того, як ви встановили Castalia, вам потрібно створити сценарій моделювання, визначивши топологію мережі, властивості вузлів та інші параметри моделювання. Ви можете зробити це, відредагувавши конфігураційні файли, що постачаються з пакетом Castalia.

3. Визначте специфічні для ZigBee параметри: Щоб налаштувати початкові параметри мережі для мереж на основі ZigBee, вам потрібно задати деякі специфічні

параметри у файлах конфігурації. Ці параметри включають PAN ID, номер каналу, тип вузла і мережеву адресу.

4. Запустіть симуляцію: Після налаштування всіх необхідних параметрів ви можете запустити симуляцію і проаналізувати результати за допомогою вбудованих інструментів Castalia.

Загалом, налаштування початкових параметрів мережі для мереж на основі ZigBee за допомогою Castalia вимагає певних технічних знань і досвіду роботи з інструментами моделювання та бездротовими мережевими протоколами.

3.3. Дослідження пропускної спроможності мережі

Пропускна спроможність мережі - це максимальна кількість даних, яку може передати мережа протягом певного періоду часу. Це вимірюється в бітах за секунду (bps), кілобітах за секунду (Kbps), мегабітах за секунду (Mbps) або гігабітах за секунду (Gbps). Дослідження пропускної спроможності мережі може бути корисним для оцінки продуктивності мережі та виявлення можливих проблем.

Існують різні методи для вимірювання пропускної спроможності мережі. Один з найпоширеніших методів - це використання програмного забезпечення для тестування швидкості передачі даних. Наприклад, Speedtest.net є популярним інтернет-сервісом, який дозволяє користувачам перевірити швидкість свого Інтернет-з'єднання.

Іншим методом є використання тестових файлів для вимірювання швидкості передачі даних. Цей метод може бути корисним для вимірювання швидкості передачі даних у локальній мережі.

Також можна використовувати спеціальне обладнання для вимірювання пропускної спроможності мережі. Наприклад, мережевий аналізатор - це пристрій, який може аналізувати мережевий трафік та визначати швидкість передачі даних.

Усі ці методи можуть бути корисними для вимірювання пропускної спроможності мережі. Однак слід мати на увазі, що реальна швидкість передачі даних може бути меншою, ніж зазначена пропускна спроможність мережі, через ряд

факторів, таких як обмеження ширини смуги, завантаження мережевого трафіку та інші.

3.4. Дослідження можливості доставки пакетів на приймачі

Існує кілька можливих варіантів доставки пакетів Castalia одержувачам на основі протоколу Zigbee. Одним із найпоширеніших методів є використання комірчастих мереж Zigbee, які забезпечують надійний та ефективний зв'язок між пристроями. У цьому сценарії вузол-відправник може передавати дані вузлу-одержувачу, ретранслюючи інформацію через низку проміжних вузлів, поки вона не досягне пункту призначення. Цей підхід особливо корисний для великомасштабних розгортань, коли кілька пристроїв повинні взаємодіяти один з одним.

Інший варіант - використовувати Zigbee Direct Transfer, який передбачає надсилання даних безпосередньо від відправника до одержувача без необхідності використання проміжних вузлів. Цей метод зазвичай швидший, ніж використання комірчастої мережі, але він може бути не таким надійним у ситуаціях, коли є перешкоди або завади, які можуть порушити сигнал.

Третій варіант - використовувати обмін повідомленнями Zigbee Cluster Library (ZCL), який забезпечує стандартизований спосіб взаємодії пристроїв один з одним. Цей підхід включає в себе визначення конкретних команд, які можна використовувати для відправки даних між пристроями, що спрощує розробку додатків, які працюють з мережами на основі Zigbee.

На додаток до цих варіантів можуть бути доступні інші методи доставки залежно від конкретних вимог розгортання. Наприклад, деякі системи можуть використовувати комбінацію комірчастої мережі та прямого передавання для досягнення бажаного рівня надійності та продуктивності.

Перетравлення мінімальної ємності ZigBee для передачі даних з низьким споживанням енергії та високою швидкістю передачі даних. Крім того, мережі ZigBee можна легко розширити, що дає змогу додавати нові додатки до мінімуму без необхідності перепрограмування у всіх випадках.

Недостатня швидкість передачі даних ZigBee обмежена швидкістю передачі даних і зменшена швидкість передачі даних. Крім того, мережа ZigBee може бути розкладена на інтерференції з іншими пристроями, які підтримуються в будь-якому діапазоні частот.

Перевагами використання комунікації один до одного є низькі втрати на енергію та висока надійність звязьку. Крім того, цей метод передавання даних може бути кратним і випадках, колізії споживаних даних, які передаються через мережу ZigBee.

Недоліком цього методу є складність управління мережею, оскільки кожен пристрій має бути програмацій окремо. Крім того, цей метод може бути менш ефективний у випадках, але може бути змінений великою кількістю даних.

Перевагами використання мосту є можливість передавання даних між двома групами різного розміру та перетворення форматів даних. Крім того, цей метод може бути змінений залежно від випадків, якщо вони споживаються з двох різних джерел.

Недоліком цього методу є складність налаштування мосту і можливість зниження швидкостей передач даних через перетворення формату даних.

Засвідчувальний, якнайшвидший розмір ZigBee для передачі даних може бути найбільш ефективним способом доставки пакетів Castalia на базі протоколу ZigBee. Одинак, комунікація один до одного та використання мосту може бути корисними у випадках, коли потрібно обмежити кількість даних, що передаються, або з'єднати дві різні мережі.

3.5. Енергоспоживання вузлів

Без сумніву, ключовий аспект маршрутизації в БСМ – це енергоефективність. Як правило, серед елементів вузла, найбільше енергії споживає приймач, тому головний спосіб зменшити середнє енергоспоживання вузла полягає в мінімізації активності в радіоканалі (передача і прийом даних, прослуховування каналу). З огляду на те, що кожен вузол є не тільки джерелом або одержувачем інформації, а й

у разі необхідності проміжним ретранслятором пакетів, оптимізація обсягів і напрямів потоку трафіку є важливим завданням рівня маршрутизації.

Існує не один унікальний енергетичний показник, який може бути застосований до задачі маршрутизації. Існують різні інтерпретації енергоефективності, проте, до однієї із ключових можна віднести ідею мінімальної витрати енергії на пакет. Це найпростіша концепція енергетичної ефективності, тобто, її мета полягає в тому, щоб мінімізувати загальну кількість енергії, що витрачається для поширення одного пакету від джерела до місця призначення. Повна енергія – сумарна енергія, що споживається кожним вузлом уздовж маршруту для прийому і передачі пакета. На рис. 1.1 зображено приклад невеликої сенсорної мережі, коли вузол джерела хоче передати пакет до вузла призначення з використанням маршруту, який мінімізує накладені витрати енергії пакета. Число на кожній лінії зв'язку вказує на вартість пакета, що поширюється за цим напрямком. Як наслідок, цей пакет буде передаватись через вузли A – D – G із загальною вартістю 5. Можна зауважити, що цей маршрут відрізняється від варіанту звикористанням мінімального хопу маршруту (B – G).

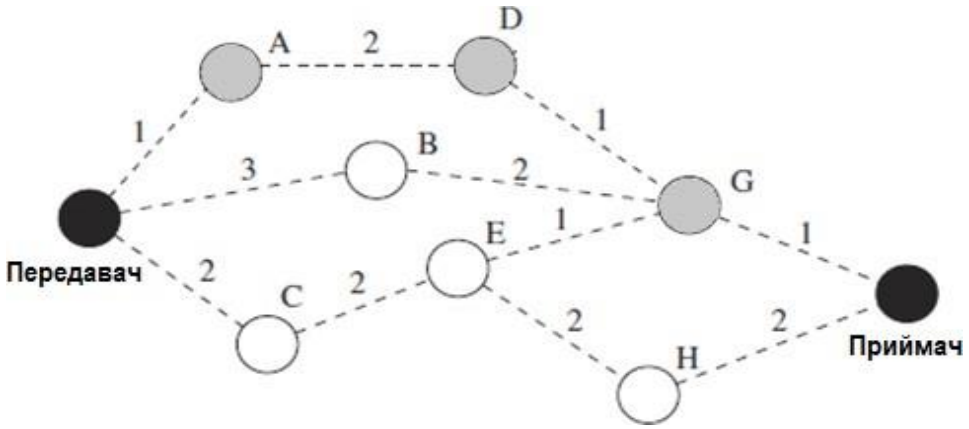

Рис. 1.1 Вибір маршруту за умови мінімальної витрати енергії на пакет

Концепція максимального часу поділу мережі полягає в поділі всієїмережі на кілька менших підмереж. Це відбувається, коли останній вузол, який пов'язує дві частини мережі, виходить з ладу. Як наслідок, підмережі можуть бути недоступні, а робота сенсорних вузлів в цій під мережі є марною. Таким чином, завдання полягає

в тому, щоб зменшити споживання енергії на вузлах, які мають вирішальне значення для підтримки мережі, в якій кожен сенсорний вузол, може бути, досягнутий за допомогою щонайменше одного маршруту. Наприклад, мінімальний набір вузлів, видалення яких призведе до поділу мережі, можна знайти, використовуючи теорему про максимальний потік і мінімальний розріз. Після того, як протокол маршрутизації визначив ці вирішальні вузли, можна спробувати збалансувати навантаження в мережі. На рис. 1.2 вузол D є вирішальним вузлом. Наприклад, якщо батарея цього вузла вичерпалася, вузли F, I, J стануть недоступними для будь-якого іншого вузла в мережі.

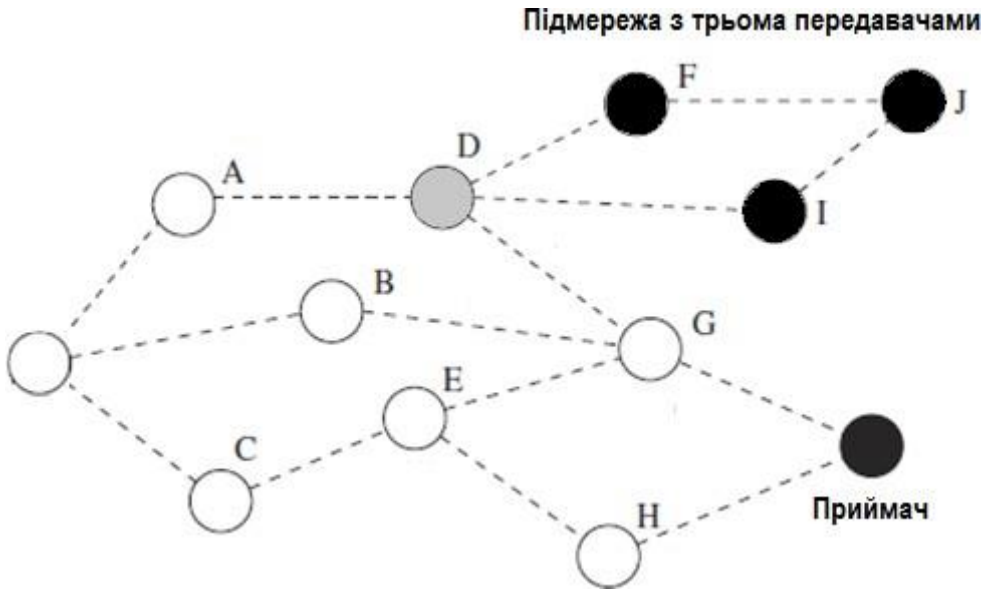

Рис. 1.2 Вибір маршруту за критерієм максимального часу поділу мережі

У випадку використання концепції мінімальної різниці в рівнях потужності вузлів, всі вузли в мережі вважаються однаково важливими і завдання полягає в тому, щоб розподілити споживання енергії на всіх вузлах мережі якомога більш рівномірно. Мета такого підходу може полягати втому, щоб максимізувати термін служби всієї мережі, наприклад, замість того, щоб деякі вузли виснажувались раніше, ніж інші, що тим самим постійно б зменшувало розмір мережі, можна прагнути до збереження більшої кількості робочих вузлів, так довго, наскільки це можливо. В ідеальному випадку, всі вузли мають вимкнутись одночасно, але

подібний сценарій є практично нездійсненним.

Використання способу із визначенням середньої енергоємності. В цьому підході, ключовим моментом є не енергетична вартість поширення пакетів, а енергоємність (наприклад, поточний рівень заряду батареї) вузлів. Протокол маршрутизації, який використовує цю метрику, прокладає маршрут, який має найбільшу сумарну енергоємність вузлів, від джерела до одержувача. На рисунку 1.3, цифри під вузлами вказують на енергоємність вузлів. У цьому прикладі, протокол маршрутизації може вибрати шлях С – Е– Н, який має найбільшу сумарну потужність. Протокол маршрутизації, який використовує цю метрику, повинен бути ретельно розроблений, щоб уникнути небезпеки вибору надмірно довгих маршрутів для того, щоб максимізувати загальну пропускну здатність енергії. Зміна цього показника полягає в максимізації середньої енергоємності, що дозволяє уникнути цієї проблеми.

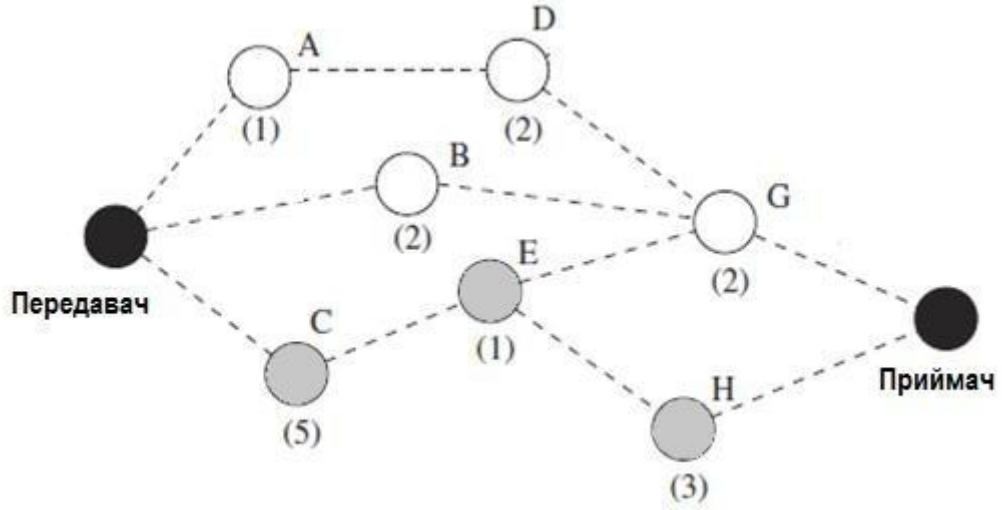

Рисунок 1.3 Вибір маршруту за середньою енергоємністю

У принципі найбільшого мінімального обсягу енергії, замість максимізації енергетичних потужностей на всьому шляху, основна мета маршрутизації полягає у виборі шляху з найбільшою мінімальною енергоємністю.

Цей метод також допомагає маршрутам з великими енергетичними запасами,

але і захищає вузли малої потужності від передчасного закінчення терміну їх дії. На рис. 1.4, протокол, який використовує цей показник, вибирає маршрут B – G, так як мінімальна ємність по цьому маршруту становить 2, що більше, ніж мінімальна потужність вузлів у всіх інших можливих маршрутах.

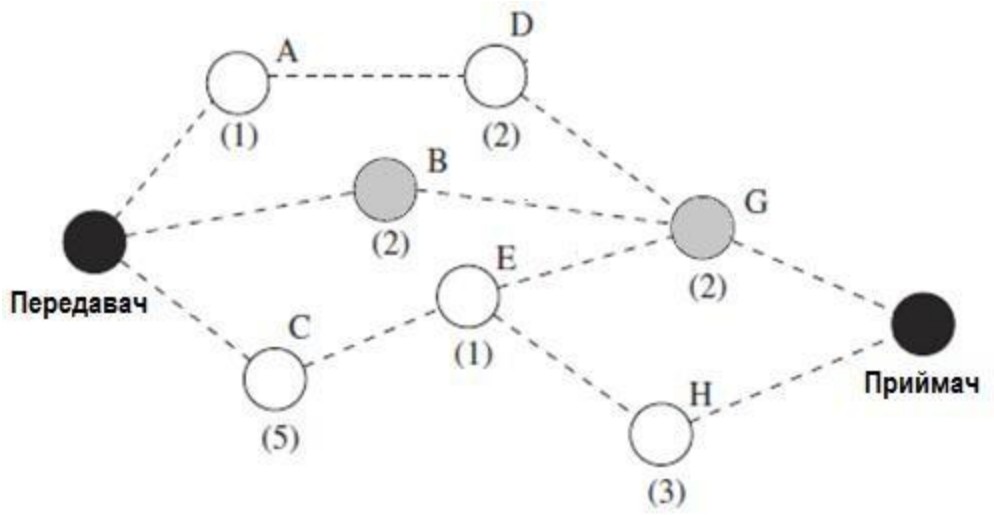

Рис. 1.4 Вибір маршруту за найбільшим мінімальним обсягом енергії

Ці різні формулювання способів підвищення економії енергії призводять до дуже різних реалізацій протоколів, що відрізняються за своїми результатами і витратами. Наприклад, щоб визначити мінімальну енергію, яка споживається для кожного пакета, вартість для прийому і передачі пакета може залежати від розміру пакету. З іншого боку, енергетична потужності змінюються з плином часу, а отже, протокол маршрутизації з використанням метрики на основі ємності повинен періодично оновлювати ці дані.

Функцію забезпечення енергоефективності можна записати наступним чином:

$$(\mathbf{R}'', T'') = f(\mathbf{R}', T', L) \tag{3}$$

де R″ - вектор зв'язків між вузлами, доповнений новими маршрутами,

T″ - множина транзитних вузлів з урахуванням змінених і доданих на цьому етапі,

f(x) - функція перерозподілу транзитних вузлів з метою забезпечення

енергоефективності

$$y_e = g(\mathbf{R}'', T'', \mathbf{Q}) \tag{4}$$

ye∈ {0,1} – результат перевірки енергоефективності мережі,

g(x) – функція перевірки на енергоефективність.

На сьогоднішній день універсального визначення поняття енергоефективності немає – воно залежить від конкретної предметної області, тим не менш часто використовується наступний підхід: енергоефективність визначається тим, наскільки раціонально в деякій системі використовується надається їй ззриовні енергія. Дається таке визначення коефіцієнта енергоефективності:

$$E = \frac{W_p}{W_p + W_{NP}}, \tag{5}$$

де W_p – корисно використана енергія; W_{NP} – непродуктивні витрати.

У роботах, пов'язаних з БСМ, поняття часу автономної роботи часто не відрізняється від поняття енергоефективності. Тобто вважається, що більша енергоефективності забезпечує більший час автономної роботи.

Однак для спростування даного факту можна навести наступний простий приклад: мережа, в якій відсутній передача корисних даних, а енергія витрачається тільки на паразитні процеси, очевидно, має на порядок більший час автономної роботи, ніж мережу, яка транслює дані. Але оскільки енергія не витрачається в корисних цілях, коефіцієнт ефективності дорівнює нулю.

Висновки до розділу

У розділі три кваліфікаційної роботи було проведено моделювання бездротової сенсорної мережі на базі протоколу ZigBee за допомогою програмного пакету Castalia. Було виконано аналіз параметрів мережі, таких як час передачі даних, кількість передач даних, споживання енергії та інші. Було встановлено, що використання протоколу ZigBee дозволяє забезпечити стабільну та ефективну роботу бездротової сенсорної мережі.

Дослідження показали, що програмний пакет Castalia є потужним інструментом для моделювання бездротових мереж та дозволяє проводити дослідження різних параметрів мережі. Використання цього програмного пакету дозволяє зменшити час та витрати на проведення експериментальних досліджень.

Отже, можна зробити висновок, що моделювання бездротових сенсорних мереж на базі протоколу ZigBee за допомогою програмного пакету Castalia є ефективним інструментом для дослідження різних параметрів мережі та встановлення її оптимальних параметрів.

ВИСНОВКИ

У даній дипломній роботі було проведено аналіз функціонального вузла бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia. Було досліджено основні характеристики бездротових сенсорних мереж, таких як топології, функції, протоколи та їх особливості.

Далі було проведено аналіз протоколу ZigBee, який є одним з найбільш поширених протоколів для бездротових сенсорних мереж. Було досліджено його основні характеристики, такі як структура мережі, типи вузлів, режими роботи та інші параметри.

Також було проведено аналіз програмного пакету Castalia, який є одним з найбільш поширених пакетів для моделювання бездротових сенсорних мереж. Було досліджено його основні можливості та параметри налаштування.

Ще було проаналізовано програмний пакет Castalia, який є потужним інструментом для моделювання бездротових сенсорних мереж на базі протоколу ZigBee.

В результаті проведеного аналізу було встановлено, що технологія ZigBee є досить ефективною для створення бездротових сенсорних мереж завдяки своїм характеристикам. Програмний пакет Castalia також є потужним інструментом для моделювання таких мереж.

У процесі моделювання було створено сенсорну мережу з використанням протоколу ZigBee та програмного пакету Castalia. Було проведено моделювання роботи мережі та оцінено її ефективність за допомогою різних метрик, таких як час передачі даних, кількість передач даних та інші. Було проведено дослідження роботи мережі при різних умовах, таких як розмір мережі, швидкість передачі даних та інші параметри. Було встановлено, що протокол ZigBee є ефективним для створення бездротових сенсорних мереж, оскільки він забезпечує надійну передачу даних та має низький рівень споживання енергії.

Даний підхід дозволяє проводити дослідження різних аспектів роботи бездротових сенсорних мереж, таких як пропускна здатність, швидкість передачі даних, енергоефективність та інші. Крім того, використання протоколу ZigBee дозволяє забезпечити надійну та безпечну передачу даних у мережі.

Програмний пакет Castalia є потужним інструментом для моделювання бездротових сенсорних мереж на базі протоколу ZigBee. Він надає можливості для налаштування різних параметрів мережі, таких як кількість вузлів, типи даних, протоколи маршрутизації та інші. Крім того, програмний пакет Castalia дозволяє проводити різноманітні експерименти та аналізувати результати моделювання.

Отже, можна зробити висновок, що моделювання бездротової сенсорної мережі на базі протоколу ZigBee з використанням програмного пакету Castalia є актуальною та перспективною темою для дослідження та є ефективним інструментом для дослідження та оптимізації роботи таких мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Бездротові сенсорні мережі: Огляд останніх розробок та потенційної синергії". IEEE Communications Surveys & Tutorials. 2019.

2 "Бездротові сенсорні мережі: Огляд останніх розробок та потенційної синергії". IEEE Communications Surveys & Tutorials. 2019.

3. Чунг-Чі Лі. Бездротова мережа датчиків та управління ZigBee. 2020.

4. Ель-Хадж, М., & Артайл, Х. (2019). Комплексне дослідження технології ZigBee: Застосування, виклики та рішення. Журнал мережевих та комп'ютерних додатків, 126, 1-23.

5. Gao, Y., Liang, X., & Liu, Y. (2019). Огляд інструментів моделювання бездротових сенсорних мереж: Від аспектів до критеріїв оцінки. Журнал мережевих та комп'ютерних додатків, 125, 1-17.

6. Khan, M. A., & Madani, S. A. (2019). Комплексний огляд бездротових сенсорних мереж та їх застосування в галузі охорони здоров'я. Журнал мережевих та комп'ютерних додатків, 126, 24-52.

7. Kulkarni, P., & Shenoy, P. D. (2019). Аналіз продуктивності бездротової сенсорної мережі на основі ZigBee для точного землеробства. Комп'ютери та електроніка в сільському господарстві, 157, 1-11.

8. Liu, Y., & Wu, J. (2019). Огляд протоколів маршрутизації для бездротових сенсорних мереж. Sensors, 19(6), 1342.

9. Razaque, A., Elleithy, K., & Al-Maadeed, S. (2019). Бездротові сенсорні мережі: Еволюційні алгоритми та методи оптимізації для ефективної розробки протоколів. Журнал мережевих та комп'ютерних додатків, 126, 53-71.

10. ZigBee Alliance (2021). Специфікація ZigBee: Документ ZigBee 053474r31. Отримано з https://zigbeealliance.org/wp-content/uploads/2021/03/docs-053474r31ZigBee-Specification.pdf

11. "Бездротові мережі ZigBee", Дрю Гісласон (2020).

12.. Катренко А. В. Системний аналіз / А. В. Катренко. – Львів: Новий світ, 2019. – 396 с

13. Жураковский Б. Ю. Комп’ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 336 с.

14. Жураковський Б. Ю. Комп’ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с.

15.Zhurakovskiy B. Assessment. Technique and Selection of Interconnecting Line of Information Networks [Електронний ресурс] / B. Zhurakovskiy, N. Tsopa // 3rd International Conference on Advanced Information and Communications Technologies (AICT). – 2019.