ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ДОСЛІДЖЕННЯ ПРОТОКОЛІВ БЕЗПРОВОДОВИХ МЕРЕЖ З МЕТОЮ ОРГАНІЗАЦІЇ ОПТИМАЛЬНОГО ВІДДАЛЕНОГО МОНІТОРИНГУ ПРИСТРОЇВ»**

на здобуття освітнього ступеня магістр
за спеціальності 123 Комп'ютерна інженерія
(код,найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро КОСТЕЦЬКИЙ
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр.КСДМ-62
Дмитро КОСТЕЦЬКИЙ
(ім'я, ПРІЗВИЩЕ)

Керівник: Андрій ЛЕМЕШКО
доктор філософії (PhD) *(ім'я, ПРІЗВИЩЕ)*

Рецензент:
науковий ступінь, вчене звання *(ім'я, ПРІЗВИЩЕ)*

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти «Магістр»

Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна прорама Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
(ім'я, ПРІЗВИЩЕ)
"____" _____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Костецькому Дмитру Ігоровичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Дослідження протоколів безпроводових мереж з метою організації оптимального віддаленого моніторингу пристроїв програмних послуг користувачам
керівник роботи доктор філософії, доцент кафедри КІ Лемешко А.В.
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" 10 2023 р. №145
2. Строк подання кваліфікаційної роботи
3. Вихідні дані кваліфікаційної роботи:
3.1. Інтернет ресурси стосовно безпроводових мереж.
3.2. Середовищі Omnet++.
3.3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Технології та особливості безпроводової мережі.
4.2. Технологія IOT (інтернет речей).
4.3. Моделювання безпроводових мереж у середовищі Omnet++ з використанням фреймворку Inet.

5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання “19” жовтня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	**Примітка**
1.	Підбір технічної літератури	.2023р. .2023р.	Виконано
2.	Технології та особливості безпроводової мережі	.2023р. .2023р.	Виконано
3.	Технологія IOT (інтернет речей)	.2023р. .2023р.	Виконано
4.	Моделювання безпроводових мереж у середовищі Omnet++ з використанням фреймворку Inet	.2023р. .2023р.	Виконано
5.	Оформлення роботи, висновки	.2023р. .2023р.	Виконано
6.	Розробка демонстраційного матеріалу, доповідь	.2023р. .2023р.	Виконано

Здобувач вищої освіти Дмитро КОСТЕЦЬКИЙ
(підпис) *(ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Андрій ЛЕМЕШКО
(підпис) *(ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступеня магістр: 70 стор., 15 рис., 20 джерел.

Мета роботи – Покращення ефективності, зручності та надійності роботи систем та пристроїв за допомогою організації оптимального віддаленого моніторингу.

Об'єкт дослідження – організація оптимального віддаленого моніторингу пристроїв.

Предмет дослідження – протоколи безпроводових мереж.

Короткий зміст роботи: В цій магістерській роботі розглянуто один із можливих підходів до проектування та дослідження безпроводових мереж у середовищі моделювання OMNeT++ з використанням фреймворку INET. Також розглянуто методику аналізу роботи моделі на прикладі часової діаграми.

Представлено методику проектування безпроводових мереж з використанням готових компонентів з фреймворку INET. Розглянуто можливі режими роботи безпроводових мереж, як при безпосередній взаємодії вузлів, так і при непрямій взаємодії через проміжні вузли.

Запропоноване імітаційне середовище дозволяє досліджувати проектні рішення при проектуванні безпроводових мереж. Обґрунтовано доцільність використання розроблених проектів у проектній діяльності.

КЛЮЧОВІ СЛОВА: БЕЗПРОВОДОВІ МЕРЕЖІ, КОМП'ЮТЕРНІ МЕРЕЖІ, WI-FI, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ, ПЕРЕШКОДИ, OMNET ++, INET FRAMEWORK.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 70 pages, 15 figures, 20 sources.

The purpose of the work is improving the efficiency, convenience and reliability of systems and devices with the help of optimal organization of remote monitoring.

The object of research is organization of optimal remote monitoring of devices.

The subject of research is wireless network protocols.

Summary of the work: In this master's thesis, one of the possible approaches to the design and research of wireless networks in the OMNeT++ simulation environment using the INET framework is considered. The method of analyzing the model's operation using the example of a time diagram is also considered.

The method of designing wireless networks using ready-made components from the INET framework is presented. The possible modes of operation of wireless networks are considered, both with direct interaction of nodes and with indirect interaction through intermediate nodes.

The proposed simulation environment allows you to explore design solutions when designing wireless networks. The expediency of using the developed projects in project activity is substantiated.

KEY WORDS: KEY WORDS: WIRELESS NETWORKS, COMPUTER NETWORKS, WI-FI, SIMULATION, OBSTACLES, OMNET ++, INET FRAMEWORK.

ЗМІСТ

ВСТУП

Безпроводові комп'ютерні мережі – це технологія, яка дозволяє створювати обчислювальні мережі, які повністю відповідають стандартам звичайних проводових мереж (наприклад, Ethernet) без використання кабелів. Такі мережі використовуються в якості корпоративних мереж всередині будівель, для з'єднання віддалених офісів між собою, а також в громадських місцях, таких як парки, ресторани і сквери.

Інститут інженерів з електротехніки та електроніки (IEEE) відповідає за розробку стандартів мережевого обладнання. Це громадське некомерційне об'єднання фахівців було створене в 1963 році, основною метою якого є інформаційне та матеріальне забезпечення розвитку наукової діяльності в галузі електротехніки, електроніки, обчислювальної техніки та інформатики.

Основною групою стандартів сімейства IEEE є стандарти 802. Сервіси та протоколи, зазначені в IEEE 802, знаходяться на двох нижніх рівнях моделі OSI: фізичному та пов'язаному. Стандарт 802.11 є робочою групою, яка займається безпроводовою локальною мережею та основним стандартом для всіх наступних версій специфікацій 802.11a/b/g/n.

Можна виділити наступні переваги даної технології:

- Безпроводова технологія не вимагає використання кабелю всередині мережі, що значно знижує витрати на обладнання;

- Безпроводові точки доступу здатні забезпечити високу швидкість передачі даних до 600 Мбіт/с, що значно вище, ніж 10 Мбіт/с дротовий Ethernet або 100 Мбіт/с Fast Ethernet;

- Безпроводовий доступ в інтернет може бути забезпечений в місцях, де немає можливості або вигідно прокладати кабелі. Технологія Wi-Fi гнучка в будівництві і дозволяє швидко організувати тимчасові мережі;

- Мобільність клієнтів дає можливість переміщатися в межах зони покриття, що виключає необхідність в проводах і фіксованому робочому просторі;

- Також варто відзначити високу сумісність різних типів мережевих пристроїв, таких як ноутбуки і телефони, і обладнання, що підтримує стандарти безпроводової мережі.

1 Актуальність дослідження протоколів безпроводових мереж полягає в тому, що безпроводові мережі стають все більш поширеними та важливими в різних сферах, включаючи медицину, промисловість, транспорт та інші. Вибір оптимального протоколу для віддаленого моніторингу пристроїв дозволить покращити ефективність та зручність їх використання, забезпечити надійність та безпеку передачі даних, а також знизити витрати ресурсів. Це має великий потенціал для покращення якість життя людей та розвитку різних галузей.ТЕХНОЛОГІЇ ТА ОСОБЛИВОСТІ БЕЗПРОВОДОВОЇ МЕРЕЖІ

1.1 Типи безпроводових мереж

Існують 4 різних типи безпроводових мереж: безпроводова локальна мережа, безпроводова мережа MAN, безпроводова мережа PAN та безпроводова глобальна мережа, які відрізняються розмірами, радіусом дії та вимогами до підключення.

1.1.1 Безпроводові локальні мережі

Технологія безпроводової локальної мережі (WLAN) забезпечує доступ до Інтернету всередині будівлі або на обмеженому відкритому майданчику. Спочатку технологія WLAN використовувалася в офісах та будинках, а тепер також використовується у магазинах та ресторанах. Використання домашніх мереж значно зросло, оскільки пандемія COVID-19 змусила офісних працівників, студентів, вчителів та інших осіб працювати та навчатися вдома.

Більшість проектів домашніх мереж є простими. Модем підключається до кабелю або волокна від місцевого постачальника послуг. Безпроводовий маршрутизатор підключається до модему і отримує сигнал від модему, який потім транслюється за допомогою безпроводового протоколу, такого як стандарти 802.11.

Офісні мережі складніші. Точки доступу (AP) монтуються на стелі, кожна з яких передає безпроводовий сигнал навколишній простір. У великих офісах потрібно кілька точок доступу, кожна з яких підключається до магістральної мережі офісу через з'єднання з комутатором.

На рис. 1.1 представлено схему безпроводової локальної мережі.

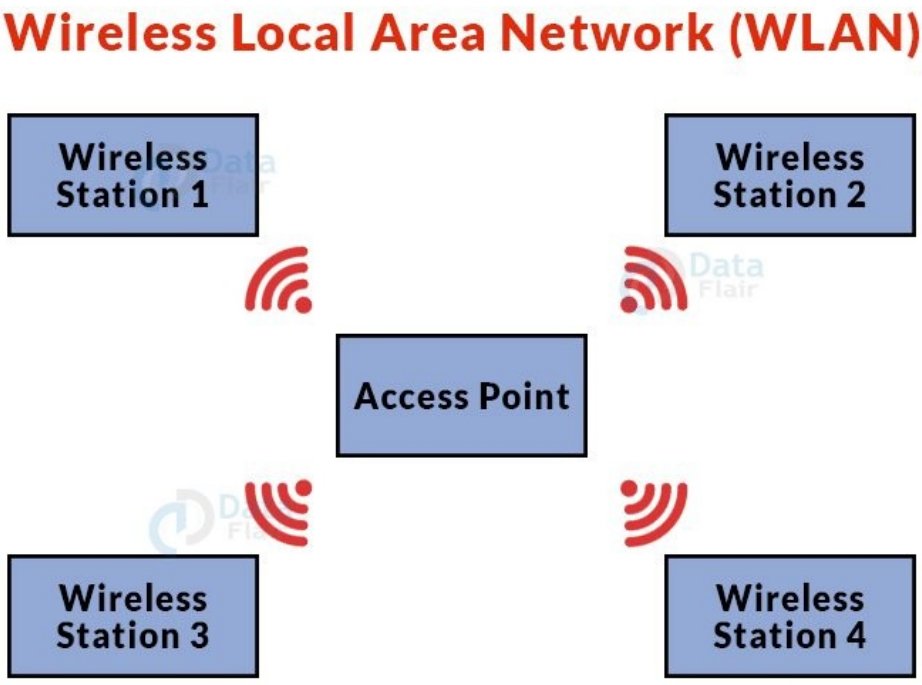


Рисунок 1.1 - Схема безпроводової локальної мережі

1.1.2 Безпроводові міські мережі

Безпроводові міські мережі були встановлені в містах по всьому світу, щоб забезпечити доступ для людей за межами офісу або домашньої мережі. Ці мережі

охоплюють ширшу територію, ніж офісні чи домашні мережі, але мають ті ж принципи.

Точки доступу розташовані з обох боків будівель або на телефонних стовпах по всій зоні покриття. Точки доступу підключені до Інтернету через дротову мережу та передають безпроводовий сигнал по всій області.

Користувачі підключаються до бажаного місця призначення, підключаючись до найближчої точки доступу, яка перенаправляє з'єднання через інтернет-з'єднання. На рис. 1.2 представлено схему безпроводової міської мережі.

Рисунок 1.2 - Схема безпроводової міської мережі

1.1.3 Безпроводові персональні мережі

Безпроводові персональні мережі охоплюють дуже обмежену територію – зазвичай максимум 100 метрів для більшості програм – з використанням таких протоколів, як Bluetooth та Zigbee.

Bluetooth дозволяє здійснювати телефонні дзвінки в режимі гучномовця, з'єднує телефон із навушниками або передає сигнали між інтелектуальними пристроями. Zigbee з'єднує станції у мережі IoT.

Інфрачервона технологія обмежена прямою видимістю, наприклад при підключенні пультів до телевізора.

Розробники безпроводового зв'язку постійно вдосконалюють технології, відкриваючи нові засоби передачі сигналів користувачам.

Ці досягнення забезпечують більш високі швидкості передачі даних та збільшення радіусу дії для кожної з цих безпроводових технологій. На рис.1.3 представлено схему безпроводової персональної мережі.

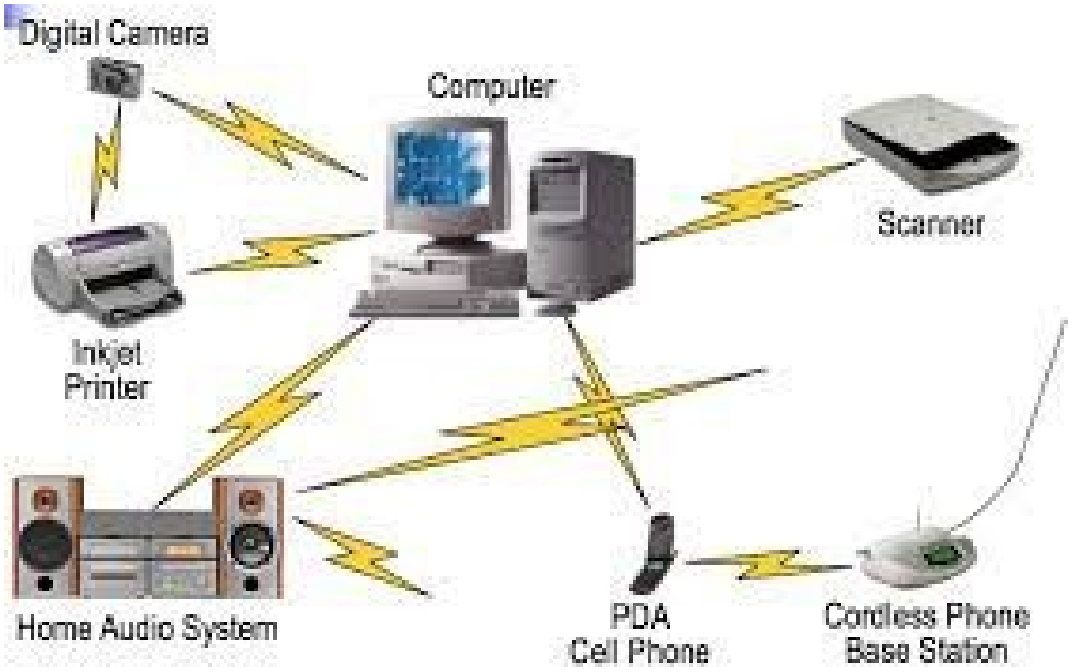


Рисунок 1.3 - Схема безпроводової персональної мережі

1.1.4 Безпроводові глобальні мережі

Безпроводові глобальні мережі використовують стільникові технології для забезпечення доступу за межі діапазону безпроводової локальної або міської мережі. Ці мережі дозволяють користувачам здійснювати телефонні

дзвінки іншим користувачам, які підключаються через безпроводову глобальну мережу або через дротову телефонну систему. Користувачі також можуть підключатися до Інтернету для доступу до веб-сайтів або серверних програм.

Вишки стільникового зв'язку розташовані майже всюди США та більшості інших країн. З'єднання користувача направляється на найближчу вежу стільникового зв'язку, яка, у свою чергу, підключена або до дротового Інтернету, або до іншої вежі, підключеної до дротового Інтернету. На рис.1.4 представлено схему безпроводової глобальної мережі.

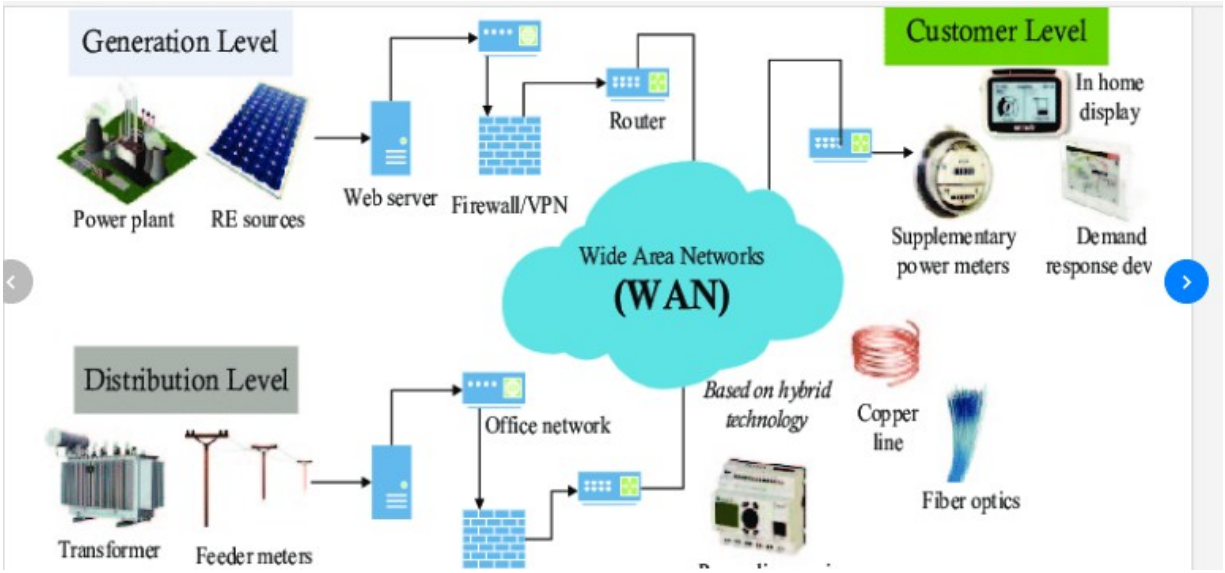


Рисунок 1.4 - Схема безпроводової глобальної мережі

1.2 Топології безпроводових мереж

На початковому етапі планування безпроводової мережі необхідно враховувати типи обладнання, що підтримують різні стандарти, технологію настройки точок доступу, це може бути індивідуальна конфігурація або централізована, а також способи побудови мережі, тобто типи підключення, способи передачі і виходу в зовнішню мережу.

1.2.1 Система безпроводового розподілу (WDS)

Завдяки системі безпроводового розподілу (WDS) точки доступу можна об'єднати в мережу з будь-яким пристроєм Wi-Fi, розширивши при цьому зону покриття. Точка доступу WDS може працювати в режимі моста Wi-Fi і в режимі ретранслятора.

Основні базові станції, як правило, підключаються до провідної мережі і в залежності від обраного режиму є джерелом безпроводової мережі, в той час як ретрансляційні станції або ретранслятори служать для зв'язку основних виносних пристроїв, виконуючи роль підсилювача і реле сигналу.

Як вже говорилося раніше, WDS може передбачати два режими підключення точок доступу:

- Перший режим безпроводового моста забезпечує безпечний доступ між пристроями з інших клієнтських пристроїв, які взаємодіють один з одним;

- Другий режим виконує роль ретранслятора.

Обов'язковою умовою настройки WDS станції є використання однієї і тієї ж частоти, методу і ключа шифрування. Конфігурація назви точки доступу або SSID може відрізнятися.

Переваги використання технології WDS:

- Простота налаштування та підключення;
- Немає проводового з'єднання між точками доступу Wi-Fi;
- Використання одного канала дозволяє швидко перебудувати топологію у разі помилок;
- Зберігання MAC-адрес мережевих клієнтів.

Незважаючи на простоту реалізації технології, є такі недоліки:

- Пропускна здатність мережі зменшується до 50% порівняно з проводовим з'єднанням;
- Немає гарантії сумісності між різними виробниками;

- Так як номер каналу завжди повинен бути постійним, є гарантія, що з'явиться ще одна станція з таким же каналом, що призведе до перекриття сигналів і зниження пропускної здатності;
- Застаріле обладнання підтримує лише шифрування WEP.

1.2.2 Mesh

Mesh-технологія — це децентралізована, однорангова організація топології сітки між вузлами мережі. Вузли в даній мережі надають послуги доступу абонентів і діють як маршрутизатори для інших вузлів у тій же мережі. В результаті з'являються масштабні зони покриття мережі з активними вузлами.

Такі технології використовуються у військових цілях, для об'єднання записів різних країн в зонах військових конфліктів, для створення операції, для створення оперативного зв’язку в стратегічних цілей. Вони широко використовуються в телекомунікаційних мережах для передачі даних. У mesh-мережах можливе об'єднання локальних мереж (Local Area Network, LAN) і мереж місцевих територій (Metropolitan Area Network, MAN) з можливістю інтеграції в глобальні мережі (Wide Area Network, WAN), що є відмінною рисою технології.

Мережі в Mesh поділяються на зони покриття, які ще називають кластерними зонами, кількість яких необмежена. Кожен кластер має від восьми до шістнадцяти вузлів. Одна точка доступу має вихід до зовнішньої мережі Інтернет, а інші вузли з'єднані між собою загальним радіоканалом, виконуючи роль ретрансляторів.

У протоколах, що описують функції mesh-мереж, кожен абонент мережі створює свою оптимальну таблицю динамічної маршрутизації для кожного пристрою. При виході з ладу одного з пристроїв визначається новий маршрут і оновлюється таблиця.

Основне застосування Mesh полягає в об'єднанні віддалених регіонів в одну загальну незалежну від провайдера мережу зі своєю унікальною топологією.

Варто відзначити, що Mesh-протоколи використовують шифрування всього трафіку, що підвищує безпеку мережі. Також використовується автоматично настроювана маршрутизація з можливістю агрегації через зовнішню мережу.

1.2.3 Ad Hoc

Технологія Ad Hoc також відноситься до децентралізованого типу безпроводової мережі. Мережа називається Ad Hoc, оскільки вона не відноситься до мереж з уже існуючою інфраструктурою, яка є одноранговим з'єднанням. Наприклад, маршрутизатори в проводових мережах, які контролюють трафік у проводових мережах або точки доступу в керованій безпроводовій мережі.

Натомість, кожен вузол бере участь у маршрутизації через перенаправлення даних на інші вузли, тобто визначення даних динамічно на кожному з'єднанні, використовуючи існуючі алгоритми маршрутизації.

Переваги безпроводової мережі Ad Hoc:

- Висока продуктивність мережі;
- Низька вартість обладнання;
- Використання ліцензованих смуг пропускання;
- Швидкий розподіл вихідного трафіку.

До недоліків можна віднести наступне:

- Динамічна топологія за рахунок мобільності клієнта;
- Необхідність високого ступеня адаптивності мережі;
- Відсутність центрального обладнання;
- Потрібні додаткові, більш складні методи маршрутизації.

Мережі Ad Hoc також поділяються за принципом маршрутизації. Існує три категорії протоколів маршрутизації:

1) Проактивний або табличний принцип (proactive, table-driven). При такій конфігурації точки доступу періодично відправляють по мережі фрейми або службові повідомлення, які містять інформацію про всі зміни в її топології. На

основі цієї інформації кожен вузол мережі будує власну таблицю маршрутизації до всіх інших вузлів, звідки зчитується маршрут при необхідності передачі повідомлення на адресу призначення.

2) Реактивний принцип, або той що працює за запитом (reactive, on-demand). У цьому методі кожна точка доступу складає таблицю маршрутизації до конкретних вузлів тільки тоді, коли є необхідність передати інформацію. Для цього вузол-відправник відправляє по всій мережі запит-повідомлення з широким вихідним кодом, яке повинно дійти до вузла призначення. У відповідь адреса призначення надсилає повідомлення з підтвердженням із зазначенням необхідного маршруту, після чого інформація записується в таблицю маршрутизації. Щоб повторно відправити повідомлення в цей пункт призначення, маршрут зчитується з таблиці. Якщо зв'язок з вузлом призначення розривається, ініціюється процедура підтримки маршруту, яка полягає в пошуку нового маршруту до пункту призначення.

3) Гібридні (hybrid). Цей принцип поєднує в собі механізми проактивного і реактивного методів. Мережа розділяють на безліч підмереж, всередині яких функціонує проактивний протокол, а зв'язок між підмережами здійснюється реактивними методами. У великих мережах це зменшує розмір таблиць маршрутизації для кожного вузла, тому їм потрібно знати лише маршрути до вузлів підмережі, до якої вони належать. Також зменшується обсяг службової інформації, що відправляється по мережі, так як більша її частина розподіляється тільки всередині підмереж.

За часом побудови маршруту, проактивні протоколи мають явну перевагу перед реактивними протоколами, оскільки проактивним протоколам потрібно лише зчитувати маршрут з таблиці. Тоді як реактивні протоколи працюють на вимогу, надсилаючи широкомовний запит, який займає відповідний час, щоб надіслати запит на адресу призначення та дочекатися відповіді. Однак проактивним також потрібно постійно розподіляти широкомовні розсилки для оновлення таблиць, що займає значну частку пропускної здатності.

Сітчасті мережі будуються для територіального взаємозв'язку між регіонами, що забезпечує складну організацію мережі та сильну топологічну мобільність. WDS не підходить через простоту реалізації, низьку надійність і відсутність динамічних протоколів. У мережах без точок доступу існують реактивні протоколи, які створюють маршрути на вимогу і не навантажують трафік частими оновленнями в таблицях, що задовольняє задану мережу частими новими клієнтами.

1.3 Протоколи безпроводових мереж

Розробкою стандартів для мереж займається відділ IEEE 802 організації (Institute of Electrical and Electronic Engineers). У 1997 році комітет 802.11 був прийнятий стандарт для безпроводової мережі, який визначав функції MAC-адрес канального рівня моделі OSI і визначав набір протоколів для найнижчих швидкостей передачі даних.

З усіх існуючих стандартів на практиці найчастіше використовуються тільки чотири: 802.11a, 802.11b, 802.11g і 802.11n.

1.3.1 Фізичні рівні протоколів 802.11a/b/g

Стандарт IEEE 802.11a має більшу пропускну здатність порівняно з сімейством стандартів 802.11, забезпечуючи швидкість передачі даних до 54 Мбіт/с. На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікація 802.11a забезпечує збільшення швидкості передачі за рахунок використання смуги пропускання 300 МГц з діапазону частот 5 ГГц. Оскільки смуга частот в цьому діапазоні ширша, їх може бути 48 і більше, в залежності від

нормативних правил конкретної країни. До недоліків стандарту 802.11a можна віднести більш високе енергоспоживання радіопередавачів і менший радіус дії.

Специфікація IEEE 802.11b все ще використовує діапазон 2,4 ГГц. Для збільшення швидкості до 11 Мбіт/с використовується більш ефективна версія методу DSSS, заснована на техніці Complementary Code Keying (CCK), яка прийшла на зміну коду Баркера. Діапазон 2,4 ГГц, зі смугою пропускання близько 80 МГц, розділений на 14 каналів, кожен з яких, крім останнього, віддалений від сусідів на 5 МГц.

Для передачі даних стандарту 802.11b використовується смуга частот шириною 22 МГц, тому необхідно об'єднати кілька суміжних каналів, щоб гарантувати деякий мінімум взаємних перешкод, що виникають від передавачів. Наприклад, використання трьох каналів 1, 6 і 11 для трьох мереж з урахуванням того, що вони не перекривають один одного, як це видно на рисунку 1.5.

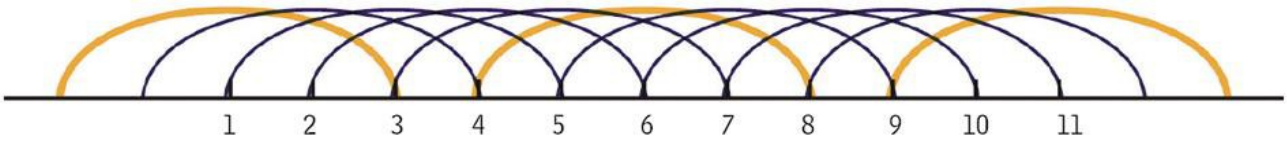


Рисунок 1.5 – Розбиття діапазону 2,4 ГГц на канали

Найбільшу популярність цей стандарт отримав серед виробників обладнання для безпроводових мереж, завдяки автоматичному уповільненню передбаченої в цьому стандарті швидкості при погіршенні якості сигналу.

Стандарт IEEE 802.11g був розроблений робочою групою IEEE у 2003 році. Це логічна еволюція стандарту 802.11a, який забезпечував ту ж швидкість до 54 Мбіт/с, і еволюція стандарту 802.11b, що працює в тому ж діапазоні 2,4 ГГц. Основна причина зростаючої популярності нової специфікації полягала в тому, що вартість обладнання 802.11g швидко зрівнялася з вартістю обладнання 802.11b.

1.3.2 Фізичний рівень протоколу 802.11n

Стандарт 802.11n був прийнятий в жовтні 2009 року. Містить багато покращень у порівнянні з пристроями стандарту 802.11g. Так, наприклад, вони можуть працювати в одному з двох діапазонів, як 2,4 ГГц, так і 5 ГГц. Рекомендованим діапазоном є діапазон 5 ГГц за рахунок більшої кількості доступних каналів і менших перешкод для численного обладнання, що працює в діапазоні 2,4 ГГц.

На фізичному рівні реалізована вдосконалена обробка сигналу і модуляція. На канальному підрівні управління реалізовано більш ефективне використання доступної пропускної здатності. Разом ці вдосконалення збільшують максимальну теоретичну швидкість передачі даних до 600 Мбіт/с, що значно вище, ніж 54 Мбіт/с у стандарті 802.11a/g.

Замість каналів зі смугою в 20 МГц, які використовуються в технологіях 802.11a і 802.11g, в тенології 802.11n застосовуються канали зі смугою 40 МГц, також допускається використання каналів в 20 МГц. Розширення смуги в 2 рази повинно призводити до підвищення бітової швидкості, так само при вдосконаленому кодуванні частотного мультиплексування з поділом каналів (OFDM), замість 52 первинних несучих частот на смугу в 20 МГц тут використовується 56 таких частот, а на смугу в 40 МГц відповідно 114. Це призводить до підвищення бітової швидкості з 54 до 65 Мбіт/с для каналів 20 МГц та до 135 Мбіт/с для каналів 40 МГц.

Для надійного розпізнавання кодових символів у технологіях 802.11a/g використовується міжсимвольний інтервал 800 нс. Технологія 802.11n дозволяє передавати дані з таким самим міжсимвольним інтервалом, а так само з міжсимвольним інтервалом в 400 нс, що підвищує бітову швидкість для каналів 40 МГц до 150 Мбіт/с.

Застосування техніки MIMO (Multiple Input Multiple Output - множинні входи і виходи) дозволяє використовувати кілька антен мережного адаптера з метою кращого розпізнавання сигналу, що прийшов до приймача різними

шляхами. Через такі ефекти поширення радіохвиль, як відображення, дифракція і розсіювання, приймач отримує кілька сигналів, що дійшли від передавача по різних фізичних шляхах і мають зсув по фазі. До появи техніки MIMO, щоб уникнути таких негативних наслідків, у кожний момент часу використовувалася лише одна антена, яка приймала сигнал кращої якості.

У системі MIMO існує одна перевага, яка називається просторовим мультиплексуванням. Завдяки цьому з'явилася можливість обробляти кілька незалежних потоків даних, переданих за допомогою декількох антен. Типовою системою MIMO стандарту 802.11n є система 3 × 3 : 2, тобто система з трьома передаючими і трьома приймаючими антенами, яка дозволяє передавати два незалежних потоку даних. Це забезпечує підвищення бітової швидкості вдвічі, тобто до 300 Мбіт/с для каналів 40 МГц. Стандарт 802.11n передбачає різні варіанти системи MIMO аж до 4 × 4 : 4, що підвищує бітову швидкість до 600 Мбіт/с.

1.3.3 Технологія Ad Hoc мереж протоколу 802.11s

Стандарт IEEE 802.11s це покращений стандарт для протоколів IEEE 802.11, що визначає тип взаємодії безпроводових пристроїв, які використовуються для створення фіксованої топології в мережах Ad Hoc і Mesh.

Стандарт 802.11s працює на другому рівні, рівні MAC-адрес моделі OSI, і визначає архітектуру, що підтримує як широкомовні (broadcast), так і мультикастові (multicast) способи доставки. Так само визначено юнікастовий (unicast) спосіб доставки, що використовує метрику радіомовлення поверх топології, що самоналаштовується з великою кількістю проміжних вузлів.

Для вибору оптимальних маршрутів у мережі використовуються метрики. Метрики включають таку інформацію, як довжина шляху, пропускна здатність, вартість передачі трафіку, завантаження, надійність, затримка.

Найбільш поширеною метрикою є довжина шляху, тобто кількість переходів, через які проходять дані від джерела до одержувача. Довжина шляху, у цьому разі, це кількість переходів від джерела до адреси призначення по вузлам мережі.

Метрика, пов'язана з пропускною здатністю, відображає ступінь зайнятості мережевих ресурсів, таких як канали та маршрутизатори. Завантаження обчислюється різними способами, наприклад, завантаження процесора і числом пакетів, що обробляються або передаються в секунду. Слід зазначити, що постійний аналіз цих показників вимагає значної зайнятості ресурсів мережного устаткування.

Також використовується надійність. Під «надійністю» мається на увазі частка втрат пакетів у кожному з каналів, які мають властивості розриву або втрати зв'язку, на що витрачається час для відновлення зв'язку та пошуку нового оптимального маршруту.

Інша метрика, що часто використовується - затримка, яка розраховує необхідний час для доставки пакета від джерела до одержувача. Затримка залежить від таких факторів, як пропускна здатність каналу, черги в портах вузлів на шляху пакета, завантаження мережі всіх проміжних каналах, а так само фізична відстань, яку потрібно подолати.

Метрика вартості суттєво відрізняється від перерахованих вище критеріїв. Деякі компанії воліють використовувати шляхи через власні платні канали інших операторів, а не через більш високопродуктивні.

Так само метрика окремих каналів може бути статичною та динамічною. Статична метрика задається адміністратором мережі і такою метрикою може бути, наприклад, вартість. Істотно відрізняється динамічна метрика, яка може змінюватися за затримкою пакетів, рівнем сигналу і безлічі інших параметрів. Причому вона може визначатися без додаткових службових пакетів і використовувати спеціальні «пробні» запити для збору статистики кожного каналу.

Стандарт IEEE 802.11s вводить обов'язковий критерій для сумісності пристроїв, щоб усі пристрої підтримували метрику часу передачі в каналі. В основі методу вибору шляху передачі даних у стандарті 802.11s лежить механізм профілів. Цей механізм забезпечує сумісність пристроїв від різних виробників, які можуть підтримувати як стандартизовані механізми, так і власні. У профіль входять такі дані: ідентифікатор профілю, ідентифікатор протоколу маршрутизації, ідентифікатор метрики протоколу маршрутизації. Пристрій може підтримувати кілька профілів роботи, але одночасно лише один може бути активним.

У зв'язку з розширенням пропускної здатності і способів передачі трафіку, розвиток стандартів безпроводових мереж призвів до більш надійних з'єднань і передачі даних на високих швидкостях, порівнянних тільки з дротовою мережею. На сьогоднішній день основними протоколами безпроводової мережі є стандарти 802.11b/g/n, а також можна з упевненістю сказати, що ці версії стандарту вбудовані в усі сучасні пристрої, що підтримують безпроводові з'єднання.

1.4 Безпека безпроводової мережі

З появою безпроводової локальної мережі головним завданням стало підвищення безпеки як комерційної, так і некомерційної передачі даних. Як і будь-яка комп'ютерна мережа, мережа Wi-Fi часто схильна до несанкціонованих атак. Крім того, проникнути в безпроводову мережу набагато простіше, ніж в проводову. Досить перебувати в зоні прийому сигналу.

Основна безпека безпроводових мереж забезпечується на фізичному та канальному рівнях моделі OSI. Для захисту використовуються математичні моделі аутентифікації, шифрування даних і контроль цілісності передачі, але потенціал витоку даних дуже високий.

1.4.1 WAP

Одним з найбільш ранніх алгоритмів безпеки безпроводової мережі, розроблених в 1997 році, є специфікація Wired Equivalent Privacy (WEP). WEP використовує спільний ключ, який можна використовувати для автентифікації або шифрування пакетів даних. Цей ключ відомий лише при обміні двома пристроями між вузлом мережі та точкою доступу.

WEP використовує алгоритм шифрування RC4, який складається з 40 розрядів 64-бітного ключа і 24-бітного вектора ініціалізації. Для підвищення безпеки безпроводових мереж цей алгоритм було розширено до 128-бітного або довшого ключа, що складається зі 104-бітної або довшої частини користувача та вектора ініціалізації. Тому існує два типи WEP, це WEP-40 і WEP-104.

В даний час цей метод захисту інформації є застарілим і не рекомендований до використання, так як були виявлені його вразливості і слабкі місця, наприклад, метод аутентифікації і алгоритм шифрування.

1.4.2 WPA/WPA2

На зміну технології безпроводової безпеки WPA прийшов WAP. Версії WPA і WPA2 (Wi-Fi Protected Access) - це оновлена програма сертифікації пристроїв безпроводового зв'язку і забезпечує більш високий захист від небажаного злому інформації. Ще однією відмінною рисою є множинна сумісність між безпроводовими пристроями як на апаратному, так і на програмному рівнях. На даний момент WPA розробляється Wi-Fi Alliance.

Новий метод захисту інформації WPA підтримує шифрування за стандартом AES (Advanced Encryption Standard), що має ряд переваг перед технологією WEP RC4. Ось деякі з особливостей WPA:

- Просунута схема шифрування;

- Автентифікація за допомогою протоколу розширюваної автентифікації (Extensible Authen-tication Protocol EAP);

- Централізована система безпеки.

Основна проблема WEP полягає в тому, що він використовує занадто багато ключів для пакетів даних. Цю проблему вирішує новий протокол тимчасової цілісності ключів TKIP (Temporal Key Integrity Protocol). Протокол TKIP відповідає за збільшення розміру ключа з 40 до 128 біт з автоматично згенерованими ключами. У цій методиці використовується спеціальна ієрархія ключів і управління ключами, що зменшує надмірну передбачуваність, що використовується в WEP. Динамічна генерація ключа шифрування використовується за допомогою двостороннього ключа, який використовується для шифрування кожного пакета даних. Ця ієрархія замінює статичний ключ WEP на 500 мільярдів можливих ключів, які використовуються для шифрування.

Також варто звернути увагу на основні режими шифрування WPA-Personal і WPA-Enterprise, які відрізняються як способом аутентифікації, так і способом використання.

Більшість домашніх мереж використовують режим WPA-Personal або WPA-PSK (Pre Shared Key). У цьому варіанті, після встановлення пароля на точці доступу, пароль поширюється на всіх користувачів і повинен вводитися вручну при аутентифікації кожним користувачем окремо.

Цей режим не є безпечним, оскільки пароль зберігається на безпроводових пристроях. А будь-який авторизований користувач, який має доступ до мережі, може підключитися до пристрою, а також побачити пароль. Тому рекомендується використовувати цей режим у домашній мережі.

Другий режим називається WPA-Enterprise або RADIUS. Цей режим складніший у налаштуванні та являє собою централізоване керування доступом з індивідуальною аутентифікацією користувача. Тобто при підключенні до мережі кожен користувач повинен мати особистий кабінет для авторизації.

Цей режим передбачає встановлення сервера RADIUS, який працює за протоколом 802.1x. При такому налаштуванні користувачеві не доведеться мати справу з ключами шифрування. Кожен ключ призначається під час кожного сеансу

користувача у фоновому режимі після надання особистих даних серверу. Цей режим шифрування зазвичай використовується в корпоративних офісах або навчальних закладах.

Методи шифрування є важливою частиною безпроводових мереж, які захищають інформацію від небажаного вторгнення. На сьогоднішній день WPA2 є найбільш широко використовуваним методом шифрування, з двома режимами доступу: WPA-Personal з попередньо визначеним паролем і WPA-Enterprise з установкою сервера RADIUS і індивідуальними налаштуваннями для кожного користувача.

2 ТЕХНОЛОГІЯ IOT (ІНТЕРНЕТ РЕЧЕЙ)

Оскільки кількість пристроїв IoT продовжує зростати, загальна кількість пристроїв IoT у світі перевищила кількість пристроїв, відмінних від IoT. За прогнозами, до 2030 року 75% усіх пристроїв будуть IoT. Зв'язок або можливість підключення між пристроями IoT зараз став важливою темою. Щоб забезпечити легке підключення пристрою IoT до Інтернету, існує кілька протоколів IoT з різною продуктивністю, швидкістю передачі даних, покриттям, потужністю та пам'яттю, і кожен протокол має свої переваги та/або більш-менш недоліки.

Ключовим аспектом вибору ідеального безпроводового протоколу IoT для проекту IoT є чітке визначення вимог, щоб можна було зосередитися лише на життєздатних варіантах. Такими вимогами можуть бути швидкість передачі даних, робочий діапазон, енергоспоживання та вартість всього проекту.

Пристрої безпроводового зв'язку реалізують зв'язок між пристроями або з послідовними серверами за різними протоколами IoT. І багато різних типів безпроводових протоколів IoT вже широко використовуються в апаратних пристроях IoT і зв'язку між машинами (M2M).

В даний час IEEE налічує більше десяти груп технічних завдань 802.15. До цих груп завдань стандарту 802.15 належать: WPAN/Bluetooth, співіснування,

високошвидкісний WPAN, низькошвидкісний WPAN, Mesh-мережа, мережа тіла та зв'язок у видимому світлі тощо. Кожен із цих протоколів безпроводової передачі має різну продуктивність, швидкість зв'язку, покриття, потужність і ємність сховища.

Інтернет речей (IoT) – це ширший термін для постійно зростаючої кількості розумних пристроїв, які можуть надсилати або отримувати дані через Інтернет.

2.1 Інтернет речей для розумного будинку

Інтернет речей революціонізує всесвіт фізичних об'єктів, забезпечуючи обробку даних, розширену аналітику та підключення до Інтернету. Концепція «розумного будинку» є втіленням IoT та його застосування на особистому рівні. Використовуючи мобільний додаток або веб-сайт, можна регулювати температуру термостата, вмикати/вимикати світло, перевіряти стан детекторів диму, відкривати двері та навіть дзвонити у двері, оскільки всі вони підключені до центрального вузла IoT, де дані передаються через Інтернет.

2.2 Промисловий Інтернет речей

З точки зору промислового Інтернету речей (IIoT), IIoT вбудовує мільярди датчиків і пристроїв з доступом до Інтернету, генеруючи потоки даних, проаналізованих за допомогою алгоритмів штучного інтелекту (ШІ) для підвищення операційної ефективності у виробничих і розподільчих системах. Ці дані дозволяють аналітикам прогнозувати потенційні відмови обладнання, оптимізувати параметри продуктивності та запобігати недовикористанню ресурсів.

2.3 Протокол IoT

Безпроводовий протокол дозволяє пристроям обмінюватися даними по безпроводовому зв'язку на великих відстанях. З початку XXI століття безпроводовий зв'язок IoT дозволив створити величезну, складну, взаємопов'язану мережу з більш ніж 20 мільярдами пристроїв по всьому світу. Ці пристрої можуть отримувати, обробляти, передавати та отримувати дані через мережу, що охоплює мільйони миль. Ці пристрої охоплюють різноманітні галузі, починаючи від нафтогазової, виробничої та сервісної організацій, таких як банки, телекомунікації, готельний бізнес тощо.

Однак безпечне з'єднання є обов'язковим для зв'язку цих пристроїв. І це складає основу для розробки протоколу IoT.

Плюси та мінуси безпроводового протоколу IoT.

Плюси:

- Немає необхідності в громіздкій фізичній інфраструктурі, такій як дроти, кабелі та антени.
- Безпроводові мережі відносно прості в установці та економічно вигідні в обслуговуванні та моніторингу.
- Дані передаються або приймаються миттєво.
- Виявити несправності та провести діагностику порівняно з проводовими мережами відносно просто.
- Безпроводові мережі забезпечують користувачам більшу мобільність, оскільки мережу можна легко переміщати та перевстановлювати.

Мінуси:

- Оскільки зв'язок відбувається на відкритому просторі, безпроводові технології вважаються менш безпечними.
- Вони відносно більш сприйнятливі до перешкод сигналу і, отже, більш ненадійні.

- На швидкість передачі даних можуть впливати екстремальні погодні умови, такі як шторми тощо.
- Швидкість передачі даних залежить від відстані до мережі.
- Безпроводові технології мають обмежений радіус дії.

2.3.1 Різні типи протоколів IoT

Зазвичай протоколи IoT поділяються на дві категорії: одна зазвичай відповідає за мережу та зв'язок між пристроями в підмережі, а інша – це насамперед протокол зв'язку пристроїв, який працює на звичайному інтернет-протоколі TCP/IP і відповідає за обмін даними та зв'язок між пристроями через Інтернет. Щоб краще зрозуміти різницю, треба прояснити концепцію: модель взаємозв'язку відкритих систем (OSI).

2.4 Модель OSI

Комп'ютерна мережева система, що пропонує різні послуги та функції, є досить складною. В результаті була створена модель OSI для підвищення популярності мережевих додатків. Він спрямований на те, щоб заохотити всі підприємства використовувати цю специфікацію для управління мережею, щоб усі компанії могли бути підключені за однією специфікацією. Модель ISO розділяє всю функцію зв’язку на сім рівнів за такими принципами:

- Всі вузли в мережі мають однакові рівні;
- Різні вузли виконують одні й ті ж функції на одному рівні;
- Суміжні шари в межах одного вузла обмінюються даними через інтерфейси;
- Кожен рівень використовує послуги, запропоновані нижчим рівнем, і надає послуги своєму верхньому ярусу;
- Однорангові рівні різних вузлів пірируются відповідно до протоколу.

Модель OSI представлено на рисунку 2.1.

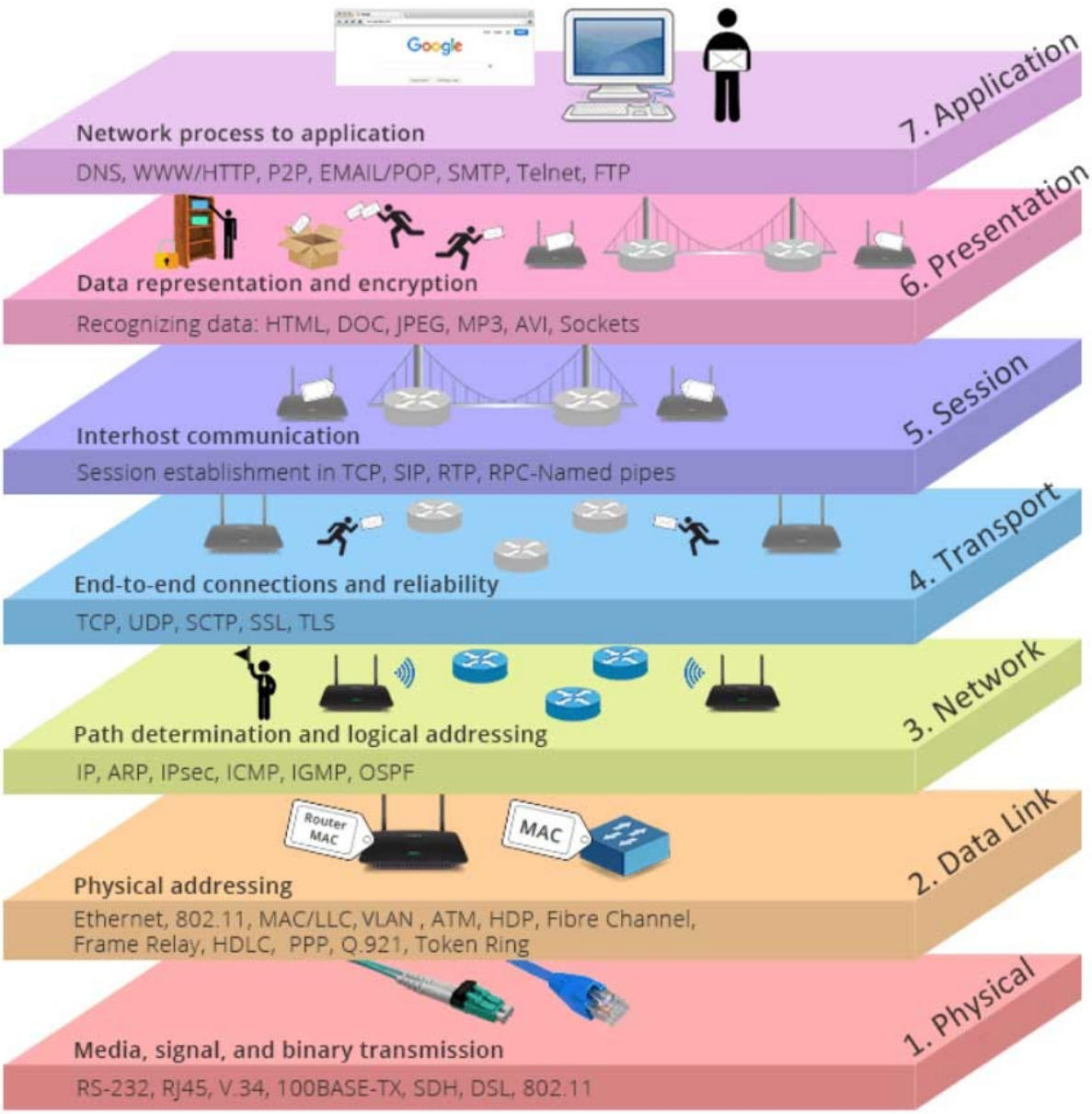


Рисунок 2.1 - Модель OSI

Прикладний рівень

Прикладний рівень відноситься до програми, яка взаємодіє з іншими комп'ютерами і в основному відповідає службі зв'язку прикладної програми.

Наприклад, текстова програма, яка не має функції зв'язку, не здатна виконати код, що забезпечує зв'язок, а програміст, який працює над цією програмою, може взагалі не піклуватися про рівень OSI 7. Однак, якщо потрібно

додати опцію передачі файлів, ця текстова програма повинна підтримувати рівень OSI 7. Наприклад, SMTP, NFS, TELNET, HTTP і FTP.

Рівень представлення

Формат даних і визначення шифрування є основними обов'язками презентаційного рівня.

Наприклад, FTP дає можливість надсилати дані у двійковому або ASCII форматі. Якщо вибрано двійковий формат, ні відправник, ні одержувач не зможуть змінити вміст файлу. Якщо вибрано ASCII, відправник перетворює текст із набору символів відправника на стандартний ASCII, а потім надсилає дані. А приймаюча сторона переводить стандартний ASCII в набір символів комп'ютера, що приймає.

Рівень сеансу

Рівень сеансу визначає, як починати, відстежувати та завершувати сеанс. Цей процес включає моніторинг і керування кількома двонаправленими повідомленнями, щоб прикладний рівень міг бути сповіщений, коли завершено лише частину безперервного повідомлення. Це зробить дані, видимі на рівні перегляду, безперервними. Презентаційний рівень іноді може бути представлений даними, якщо він отримав усі дані. Наприклад, RPC, SQL тощо.

Транспортний рівень

Можливості транспортного рівня включають в себе три аспекти:

1. Вибір між протоколом відновлення помилок і протоколами безпомилкового відновлення.
2. Мультиплексування введення потоків даних з різних додатків на одному хості.
3. Зміна порядку отриманих пакетів даних, які розташовані в неправильному порядку.

Приклади: TCP, UDP, SPX.

Мережевий рівень

Мережевий рівень визначає наскрізну передачу пакетів. Він визначає логічну адресу, яка може ідентифікувати кожен вузол, а також те, як реалізована та

навчена маршрутизація. Мережевий рівень також визначає, як розділити пакет на менші пакети, щоб адаптуватися до середовища передачі, максимальна довжина одиниці якого менша за довжину пакета. Прикладами можуть служити IP, IPX і т.д.

Канальний рівень

Канальний рівень даних задає параметри передачі даних по одному каналу. Ці протоколи стосуються різних засобів масової інформації. Наприклад, ATM, FDDI тощо.

Фізичний рівень

Фізичний рівень пов'язаний з властивостями середовища передачі, а специфікації зазвичай посилаються на стандарти, розроблені іншими організаціями. Роз'єми, кадри, використання кадрів, струм, кодування та модуляція світла – все це частини різних специфікацій фізичного рівня. Для визначення всіх частин на фізичному рівні також часто використовуються численні специфікації. Приклади включають Rj45, 802.3 тощо.

У додатках IoT технології зв'язку включають Wi-Fi, RFID, NFC, ZigBee, Bluetooth, LoRa, NB-IoT, GSM, GPRS, мережі 3/4/5G, Ethernet, RS232, RS485, USB тощо та пов'язані з ними протоколи зв'язку. (стеки протоколів, технічні стандарти) включають Wi-Fi (IEEE 802.11b), RFID, NFC, ZigBee, Bluetooth, LoRa, NB-IoT, CDMA/TDMA, TCP/IP, WCDMA, TD-SCDMA, TD-LTE, FDD-LTE, TCP/IP, HTTP тощо.

Комунікаційне середовище IoT включає Ethernet, Wi-Fi, RFID, NFC (зв'язок ближнього радіусу дії), Zigbee, 6LoWPAN (IPV6 через низькошвидкісні безпроводові персональні мережі), Bluetooth, GSM, GPRS, GPS, 3G, 4G тощо, і кожен з них має певну сферу застосування. Наприклад, AMQP, JMS і REST/HTTP працюють через Ethernet. Протокол COAP спеціально розроблений для пристроїв з обмеженими ресурсами, тоді як DDS і MQTT набагато сумісніші.

Загалом протоколи зв'язку IoT поділяються на чотири групи: зв'язок ближньої дії, стільниковий зв'язок великої дальності, нестільниковий зв'язок на великі відстані і проводовий зв'язок.

RFID

Радіочастотна ідентифікація (RFID) – це тип технології автоматичної ідентифікації. Він використовує радіочастоту для безконтактної двосторонньої передачі даних і зчитування носіїв запису (електронних міток або радіочастотних карт) для ідентифікації цілей і обміну даними. Залежно від способу живлення міток, технологію RFID можна розділити на три групи: пасивний RFID, активний RFID і напівактивний RFID.

Пасивний RFID

Пасивний RFID – той, що дебютував першим, є найбільш розвиненим і має найширше застосування з усіх інших. Приймаючи мікрохвильовий сигнал, що передається зчитувачем RFID, і отримуючи енергію через електромагнітну індукційну котушку для забезпечення себе протягом короткого часу, пасивна електронна мітка RFID може завершити обмін інформацією.

Оскільки система живлення відсутня, розмір пасивних RFID-виробів може досягати сантиметрового рівня або навіть менше, а також мати просту конструкцію, низьку вартість, низьку частоту відмов і тривалий термін служби. Але з іншого боку, ефективна відстань ідентифікації пасивного RFID зазвичай невелика, і він зазвичай використовується для ідентифікації контактів на невеликій відстані. Пасивний RFID в основному працює в нижчих частотних діапазонах: 125 кГц, 13,56 МГц тощо, а його типові застосування включають: автобусні картки, посвідчення особи, картки живлення їдальні тощо.

Активний RFID

Поява активного RFID тривала недовго, але він відіграв незамінну роль у різних сферах, зокрема в електронній безперервній системі збору плати за проїзд на швидкісних автомагістралях. Активні елементи RFID зазвичай живляться від зовнішнього джерела живлення і активно посилають сигнали на RFID-зчитувачі.

Їх обсяг відносно великий, але вони також мають більшу відстань передачі та вищу швидкість передачі. Типова активна RFID-мітка може контактувати з RFID-зчитувачем на відстані 100 метрів, а швидкість зчитування може досягати 1 700 зчитувань в секунду.

Активний RFID працює в основному у вищих діапазонах частот, таких як 900 МГц, 2,45 ГГц і 5,8 ГГц, і здатний ідентифікувати кілька міток одночасно. Активний RFID незамінний у різноманітних програмах RFID, які вимагають більшої продуктивності та більшого радіусу дії завдяки своїм характеристикам широкому діапазону та високим характеристикам ефективності.

Напівактивний RFID

Напівактивний RFID – це компроміс між пасивним RFID та активним RFID, його ще називають технологією активації низької частоти. Напівактивні RFID-продукти зазвичай знаходяться в сплячому стані і подають живлення тільки на ту частину, яка зберігає дані, тому їх енергоспоживання низьке і може тривати тривалий час. Коли мітка потрапляє в ідентифікаційний діапазон RFID-зчитувача, зчитувач активує її, використовуючи спочатку низькочастотні, а потім високочастотні сигнали для швидкої передачі даних. Типовим сценарієм застосування є активація напівактивних RFID-елементів на великій площі, охопленій високочастотним сигналом. Численні низькочастотні зчитувачі розташовані в різних точках для визначення місцезнаходження, збору та передачі інформації.

2.5 Технологія NFC

NFC – це абревіатура від Near Field Communication (зв'язок ближнього поля). Це високочастотна технологія безпроводового зв'язку малого радіусу дії, яка дозволяє передавати дані між електронними пристроями від точки до точки без фізичного дотику (в межах 10 см). Споживачі можуть легко та інтуїтивно обмінюватися інформацією та отримувати доступ до контенту та послуг завдяки

простому сенсорному рішенню NFC. Ця технологія походить від безконтактного RFID і зворотно сумісна з RFID. Вперше його рекламували Philips, Nokia та Sony, і в основному його можна використовувати в портативних пристроях, таких як мобільні телефони.

Вважається, що NFC має величезні перспективи в таких галузях, як мобільні платежі, завдяки своїй безпеці ближнього поля. Він поєднує в собі одноранговий безконтактний зчитувач карт і функціональність картки в одному чіпі, створюючи безліч нових варіантів стилю життя для користувачів. На відміну від RFID, NFC використовує двосторонню ідентифікацію та підключення. Він працює в діапазоні частот 13,56 МГц в радіусі 20 см і здатний швидко і автоматично встановлювати безпроводову мережу, забезпечуючи зв'язок Bluetooth, Wi-Fi і стільникових пристроїв, дозволяючи електронним пристроям обмінюватися даними на невеликій відстані.

Під NFC-платежами в першу чергу мається на увазі додаток з відкритим циклом, який перетворює мобільний телефон з функцією NFC в банківську картку для використання в супермаркетах і торгових центрах.

Безпека NFC в основному використовується для перетворення мобільного телефону на віртуальну картку контролю доступу та збереження даних з існуючої плати контролю доступу до NFC мобільного телефону. Так, немає необхідності носити з собою додаткову карту контролю доступу.

Запис деякої інформації на NFC-мітку дозволяє користувачам миттєво отримати доступ до неї, просто помахавши NFC-міткою перед телефоном із підтримкою NFC. Наприклад, ритейлери можуть прикріплювати NFC-мітки до дверей вітрин магазинів, на яких розміщені плакати, флаєри та рекламні матеріали. Споживачі можуть використовувати мобільні телефони NFC для отримання актуальної інформації відповідно до своїх потреб.

2.6 Технологія Bluetooth

Технологія Bluetooth була названа на честь датського короля 10-го століття «Вісник Блаттанда», де «Blattand» означає «Bluetooth». Метою проекту є створення недорогої технології безпроводового зв'язку малого радіусу дії, заснованої на радіочастотних хвилях в діапазоні 10 ГГц і дозволяє двом пристроям зв'язуватися один з одним для швидкої передачі даних.

Передача Bluetooth має три різні рівні відстані: клас 1 становить близько 100 метрів, клас 2 - близько 10 метрів і клас 3 - близько 2-3 метрів. Його нормальний робочий діапазон становить 10 метрів за нормальних умов. У цьому діапазоні можливе з'єднання між кількома пристроями. Тим часом пристрої з підтримкою Bluetooth використовують метод «частотного стрибкоподібного розширеного спектру», який робить їх набагато безпечнішими та запобігає прослуховуванню хакерами.

Тепер Bluetooth можна керуватиГрупа спеціальних інтересів Bluetooth (SIG), і використовується для обміну даними між стаціонарними та мобільними пристроями на коротких відстанях і побудови персональних мереж (PAN). Виробник пристрою Bluetooth повинен відповідати стандартам Bluetooth SIG, щоб продавати його.

Bluetooth Low Energy (BLE) призначений для значного зниження енергоспоживання та вартості при збереженні аналогічного діапазону зв'язку. В основному він використовується в нових програмах IoT в охороні здоров'я, фітнесі, маяках, безпеці та домашніх розвагах. Він не залежить від класичного Bluetooth і не має сумісності.

Щоб гарантувати, що дані, надіслані одним пристроєм Bluetooth, підтверджуються іншим пристроєм лише після авторизації, перед підключенням необхідно з'єднати два пристрої Bluetooth. Технологія Bluetooth поділяє пристрої на два типи: головні та ведені.

Зазвичай головний пристрій Bluetooth має вхід. Основні пристрої включають мобільні телефони Bluetooth, ПК з підтримкою Bluetooth іШлюзи Bluetooth. зазвичай не мають вхідних даних. Таким чином, коли ведений пристрій виходить із заводу, відповідний 4- або 6-значний пароль фіксується в його чіпі Bluetooth. Підлеглі пристрої включають цифрові ручки UD, Bluetooth-гарнітури тощо. Раба не можна зіставити з рабом, однак можна зіставити господаря і господаря, господаря і раба. Крім того, хост-пристрій може бути пов'язаний з одним або декількома іншими пристроями.

Сьогодні багато PED (персональні електронні пристрої) використовують технологію Bluetooth. Наприклад, носимі пристрої, такі як навушники, Air Pods, або такі пристрої, як безпроводові клавіатури, миші, принтери, веб-камери тощоBluetooth Інтернет речейТехнологія Bluetooth також широко використовується у фітнес-браслетах, розумних годинниках абоПереносні пристрої для віддаленого моніторингу пацієнтівщоIoT RPMРішення. Крім того, шляхом інтеграціїЛокатор області застосуванняіПозиціонування в приміщенніBluetooth, також широко використовується для персоналу таВідстеження місцезнаходження активів.

Z-Wave був представлений датською компанією Zensys в 1999 році. Створивши сітчасту мережу з використанням малопотужних радіохвиль, що працюють у діапазоні нижче 1 ГГц, Z-Wave здійснила революцію у світі автоматизації житлових і комерційних будівель. .

Z-wave чимось схожий на Wi-Fi, який був налаштований для автоматизації розумного будинку. Z-Wave Alliance – це міжнародний конгломерат з більш ніж 300 компаній, які в даний час експлуатують цю технологію. Ці компанії виготовили та розгорнули вражаючу кількість із понад 100 мільйонів розумних пристроїв на базі Z-Wave.

Ці пристрої включають, але не обмежуються ними, різні пристрої розумного будинку, такі як дверні замки, термостати, освітлення, датчики, контролери вентиляторів і системи безпеки. Ви можете використовувати свій смартфон,

ноутбук або планшет для віддаленого або навіть локального керування та моніторингу системи Z-Wave за допомогою спеціальної смарт-панелі зі шлюзом Z-Wave, який діє як центральний концентратор і контролер.

Типовий діапазон для Z-Wave коливається від 100 до 800 метрів, тоді як для Z-Wave LR він становить до 1 600 метрів.

Інтернет-Fi (Wi-Fi)

Наприклад, на сайті Wi-Fi Alliance зазначено, що Wi-Fi:

- Виділяється як найбільш часто використовувана безпроводова технологія.

- Він служить основним засобом для всесвітнього інтернет-трафіку.

- Інвестував приголомшливі 3,3 трильйона доларів у світову економічну екосистему.

- Спостерігається безпрецедентне зростання: щороку постачається понад 4 мільярди пристроїв і використовується 16 мільярдів пристроїв.

Розроблений Wi-Fi Alliance, Wi-Fi, абревіатура від Wireless Fidelity, є протоколом безпроводової мережі, заснованим на мережевому стандарті IEEE (Institute of Electrical and Electronics Engineers) 802.11. Вона зробила революцію в тому, як люди спілкувалися протягом більш ніж двох десятиліть. Використовуючи радіохвилі, Wi-Fi дозволяє кільком пристроям підключатися до Інтернету в домашньому або діловому середовищі через безпроводовий маршрутизатор, який, у свою чергу, підключається безпосередньо до вашого інтернет-модему та функціонує як концентратор для трансляції інтернет-з'єднання на всі мережі WIFI. Підключені пристрої, такі як мобільні телефони, планшети, телевізори тощо.

Wi-Fi забезпечує відносно більшу мобільність у межах покриття мережі, а типовий радіус дії коливається від 125 футів до 250 футів.

Оскільки Wi-Fi є найбільш затребуваною безпроводовою технологією на сьогоднішній день, вкрай важливо, щоб мережа та безпека даних були найвищої якості.

Завдяки безпечному доступу до Wi-Fi (WPA) альянс WI-FI знаходиться в авангарді забезпечення безпечного цифрового зв'язку для приватних осіб і

компаній за допомогою автентифікованого шифрування, HMAC (Hashed Message Authentication Mode) з безпечним алгоритмом хешування (HMAC-SHA256). і надійний захист рами керування.

Протокол стільникового зв'язку на великих відстанях - це, по суті, стандарт і протокол, прийнятий різними операторами в рамках 2/3/4/5G, NB-IoT та інших технологій. Тут мова піде про LTE Cat 1 (також LTE-M). У порівнянні з іншими стільниковими рішеннями, LTE-M характеризується низьким енергоспоживанням і забезпечує значне зниження витрат на обслуговування. Він також має величезну перевагу зворотної сумісності з існуючими мережами LTE, що економить гроші операторів зв'язку, усуваючи необхідність будівництва нової станції.

Абревіатура LTE-M розшифровується якДовгострокова еволюціядля машин, яка є малопотужною глобальною мережею, яка використовує радіочастотні хвилі для додатків M2M (машина-машина) та Інтернету речей (IoT). Підтримується та розвиваєтьсяЗGPPLTE-M – ідеальне рішення для вузькосмугового мобільного зв'язку, яке дозволяєПристрої IoTякРозумні датчики, виконавчі механізми, регулятори і т.д.Промисловий стільниковий шлюзпристрої передачі даних при цьому забезпечують відносно низьке енергоспоживання і високе проникнення сигналу.

LTE-M перевершує інші протоколи IoT з точки зору забезпечення надійного зв'язку по всьому світу, що робить його ідеальним вибором для оновлення статусу в режимі реального часу для відстеження автопарку.Віддалений моніторинг IoT, відстеження активів, панелі сигналізації та POS-пристрої (точки продажу). У віддалених місцях з низьким покриттям, де рівень сигналу LTE низький, система може легко переключитися на 3G (WCDMA-Broadband Code Division Multiple Access) або 2G (GPS-Common Packet Radio Service) для забезпечення зв'язку.

Використовуючи систему позиціонування веж стільникового зв'язку, LTE-M також надає OEM-виробникам економічно ефективне базове відстеження місцезнаходження для своїх пристроїв. SIM-карта, або чіп модуля ідентифікації абонента, вбудована в друковану плату кожного пристрою LTE-M, а ключі

оператора включені, що робить його одним із найбезпечніших протоколів IoT, оскільки ключі не можна змінити без фізичного доступу.

Однак, оскільки для роботи SIM-карти обов'язкова підписка на будь-якого з операторів мобільного зв'язку, пов'язані з цим витрати, як правило, фіксовані. Остання версія, версія 14, пропонує підвищену швидкість передачі даних до 4 Мбіт/с, забезпечуючи підвищену мобільність і надійність мережі.

Термін «ZigBee» відноситься до способу спілкування бджолиних сімей, при якому бджоли танцюють зигзагоподібними візерунками, щоб передати таку інформацію, як напрямок, місцезнаходження та відстань до джерел їжі. Zigbee – це нове покоління технології безпроводового зв'язку.

Належить ZigBee Alliance, альянсу кількох компаній, які розробили та опублікували цей стандарт, ZigBee був концептуалізований у 1998 році, стандартизований у 2003 році, а потім переглянутий у 2006 році. Як зазначено на їхньому веб-сайті, протокол ZigBee вбудований і розгорнутий на мільйонах пристроїв по всьому світу.

У більшості країн світу Zigbee використовує промислові, наукові та медичні (ISM) радіоканали і працює на частоті 2,4 ГГц (Giga Hertz). У більшості країн світу Zigbee використовує промислові, наукові та медичні (ISM) радіоканали і працює на частоті 2,4 ГГц (Giga Hertz). Відстані передачі обмежені низьким енергоспоживанням і коливаються від 10 до 100 метрів прямої видимості, залежно від вихідної потужності та факторів навколишнього середовища. Zigbee найкраще підходить для епізодичної передачі даних з датчика або пристрою введення, оскільки має встановлену швидкість до 250 кбіт/с. Мережі Zigbee додатково захищені 128-бітними симетричними ключами шифрування. В результаті ZigBee забезпечує безпроводову однорангову мережу з низьким енергоспоживанням, низькою пропускною здатністю та малим радіусом дії, яка є безпечною та легко масштабованою.

Zigbee дозволяє створювати однорангові мережі Mesh і дозволяє вузлам мережі з'єднуватися один з одним через кілька безпроводових каналів зв'язку.

Використовуючи таку сітчасту мережу проміжних пристроїв для передачі даних на великі відстані, пристрої Zigbee можуть досягати більш віддалених пристроїв. Сітчаста мережа Zigbee теоретично може вмістити до 65 000 XNUMX вузлів Zigbee.

Zigbee зазвичай використовується в програмах з низьким бітрейтом, які вимагають тривалого часу автономної роботи та безпечної мережі. Він має такі переваги, як низька вартість, висока пропускна здатність мережі, безпека та надійність. Крім того, ZigBee продовжує час автономної роботи блоку живленняПродукти IoTнайбільшою мірою. Таким чином, це ідеальний технічний варіант для передачі даних для різних систем управління промисловою автоматикою. Більше того, технологія, визначена специфікацією Zigbee, повинна бути менш складною та дешевшою, ніж інші безпроводові персональні мережі, такі як Bluetooth та Wi-Fi.

Розумний будинок також є найпоширенішим варіантом використання ZigBee. Ця технологія дозволяє підключати кілька пристроїв розумного будинку одночасно. Як ідеальний вибір для домашньої мережі, користувачі можуть реалізувати зв'язок між такими пристроями, як розумні дверні замки, системи керування освітленням, роботи таТермостатиі доповнитиУніверсальний шлюз ZigBeедля підключення до Інтернету та виконання командного керування в режимі реального часу.

Zigbee можна використовувати спеціально дляРозумні будівлі та домашня автоматизаціяВключаючиУправління освітленням IoT, кондиціонери, штори та інша побутова техніка; побутове електронне обладнання, включаючи дистанційне керування телевізорами, DVD-програвачами, програвачами компакт-дисків та іншими електричними пристроями; Автоматичний збір, аналіз та обробка медичного обладнання, а такожВіддалене управління IoTмедичні датчики, кнопки екстреного виклику пацієнта тощо.

Технологія LoRaWAN

Як і ZigBee, LoRaWAN (Long Range Wide Area Network) є запатентованою технологією, розробленоюАльянс LoRa, яка є неприбутковою організацією. Протокол LoRaWAN – це набір стандартів протоколу передачі, заснований на передачі LoRa на фізичному рівні і, головним чином, на рівні каналу передачі даних. LoRaWAN відповідає рівню MAC у семишаровій моделі OSI. Це відкритий мережевий протокол, який усуває апаратну несумісність, а також має такі функції, як багатоканальний доступ, перемикання частоти, адаптивна швидкість, управління каналами, синхронізація надсилання та прийому, автентифікація доступу до вузлів, шифрування даних і роумінг.

Як випливає з назви, LoRaWAN належить до категорії WAN. Отже, LoRaWAN є кращим варіантом для компаній, які хочуть розробити глобальну мережу для гаджетів IoT, що живляться від акумуляторів. LoRaWAN широко використовується для моніторингу пристроїв керування та датчиків, розгорнутих на великих територіях, таких як міста чи селища. Використовуючи неліцензовані радіодіапазони, він може керувати міськими вуличними ліхтарями, системами управління фермою та іншими датчиками навколишнього середовища.

Точно налаштований для зв'язку на великих відстанях, LoRaWAN розгортає кілька діапазонів частот субгігагерц залежно від регіону роботи. У Північній Америці використовується діапазон 915 МГц. 868 МГц для Європи, а також використовуються діапазони 169 і 433 МГц. Звичайна швидкість передачі даних коливається від 0,3 кбіт/с до 50 кбіт/с.

Протоколи IoT потрібно використовувати на апаратних пристроях IoT. Для різних проектів IoT може знадобитися різне обладнання IoT з різними функціями, але базова структура розробки залишається незмінною. Ми обговоримо деякі з ключових апаратних засобів, які повинні бути в проекті IoT.

Датчики IoT

Як випливає з назви, датчик IoT — це пристрій, який виявляє зміну фізичного стану будь-якої системи та перетворює її на електричний сигнал, який потім передається на центральний процесор.

Датчики бувають різних типів: оптичні, тиску, контактні, акустичні, вологості, магнітні, хімічні та багато інших, залежно від фізичних змін, які потрібно виявити.

Шлюз IoT

Діючи як міст, інтернет-шлюз, по суті, служить центральним з'єднувальним вузлом для пристроїв IoT і з'єднує їх з хмарою та один з одним, полегшуючи спілкування та перетворюючи необроблені дані на корисну інформацію за допомогою будь-якого з протоколів IoT, розглянутих раніше. Шлюз IoT також функціонує як обчислювальна платформа, яка має вбудовані настроювані програми для керування пристроями та даними, безпеки та різних інших функцій шлюзу.

Як вибрати правильні протоколи IoT для ваших проектів IoT

Важко визначити, який із протоколів IoT, розглянутих вище, найкраще підходить для ваших проектів IoT, але переможцем, безумовно, є той, який легко доступний і працює з відповідною швидкістю на більшості нових пристроїв IoT і мобільних телефонів. Однак, виходячи з різноманіття варіантів використання, які існують, суть справи полягає не в тому, щоб знайти «найкращий» варіант, а в тому, щоб знайти «найбільш підходящий» варіант, виходячи з потреб.

У режимі реального часу завжди будуть певні сценарії компромісу, де вам, можливо, доведеться піти на компроміс щодо деяких факторів. Наприклад, великий робочий діапазон вимагає більш високого рівня енергоспоживання і, отже, більш високих пов'язаних з цим витрат. Тому потрібно визначитися з критеріями оформлення, а потім почати звужувати варіанти, поки не знайдете найбільш підходящий.

Wi-Fi буде ідеальним, якщо вам потрібно передавати великі обсяги даних і файлів через мережу, а Bluetooth буде першим вибором, якщо ви хочете займатися роздрібним маркетингом.

Підсумовуючи, успішний вибір протоколу IoT повністю залежить від того, чого ви хочете досягти, і ключовим аспектом вибору ідеальних бездротових

протоколів IoT для вашого проекту IoT є чітке визначення ваших вимог, щоб ви могли зосередитися лише на життєздатних варіантах. Такими вимогами можуть бути швидкість передачі даних, робочий діапазон, енергоспоживання та вартість всього проекту.

Ось кілька ключових факторів, які слід враховувати при виборі правильного бездротового протоколу IoT для проекту IoT.

Обсяг переданих даних

Якщо потрібна передача величезних порцій даних, наприклад, зображення або відео з високою роздільною здатністю або великі файли даних датчиків, вам слід вибрати протокол IoT, який може передавати ці величезні дані за короткий проміжок часу. WLAN іПротокол BluetoothМоже стати відмінним виборомУ такій ситуації вони будуть витрачати велику кількість енергії в процесі.

Однак більшість проектів IoT з інтелектуальними сенсорними модулями вимагають бездротової передачі даних. Невеликі обсяги даних короткими серіями. У таких сценаріях ви можете легко перейти на малопотужні рішення, такі як ZigBee або EnOcean, які розроблені спеціально для пристроїв з наднизьким енергоспоживанням.

Кількість пристроїв, які одночасно передають дані

Для бездротового протоколу IoT доступний діапазон частот виділяється мережевим пристроям. Якщо у вас є багато пристроїв, які використовують один і той самий діапазон частот у певному місці, радіосигнали можуть спотворюватися через перешкоди, що призводить до затримки даних і втрати даних.

Деякі діапазони частот використовуються ширше, ніж інші, що робить системи, які використовують певні протоколи, більш сприйнятливими до перешкод. Хорошим прикладом є діапазон 2,4 ГГц – він використовується для бездротового підключення комп'ютерів, принтерів та іншого IT-обладнання та не потребує ліцензування в усьому світі, що робить його популярним вибором. Bluetooth і WLAN використовують цей діапазон, як і більшість пристроїв ZigBee.

Є деякі інші протоколи, які потрапляють у діапазон нижче категорії 1 ГГц, що означає, що радіохвилі, які використовуються в цих протоколах для передачі даних, мають частоти менше 1 ГГц. У вас набагато більше шансів отримати передачу без перешкод, використовуючи ці групи, оскільки вони набагато менш населені.

Енергоспоживання IoT-проектів

Якщо датчики IoT, розгорнуті у вашому проекті IoT, живляться від батарейок, вам потрібно знати період заміни батареї. Крім того, вам також потрібно буде утилізувати їх належним чином і переконатися, що у вас завжди є напоготові заміни. Тим, хто шукає рішення IoT з низьким енергоспоживанням і низьким рівнем обслуговування, слід розглянути акумулятори меншої потужності, які живляться від фотоелектричних елементів або, Простіше кажучи, вони використовують сонячну енергію як джерело живлення. Більше того, вибір бездротового протоколу IoT з низьким енергоспоживанням може позбавити вас від усіх цих проблем. Zigbee і BLE (Bluetooth Low Energy) є хорошими прикладами.

Сумісність з іншими бездротовими протоколами та платформами

Оскільки існує багато різних виробників пристроїв IoT та систем автоматизації, вони зазвичай використовують різні протоколи IoT. Наприклад, деякі складні промислові рішення IoT або проекти компанії вимагають великої кількості обладнання IoT, датчиків, смарт-терміналів та іншого обладнання для завершення виробництва. Однак протоколи IoT, що підтримуються різними типами апаратного забезпечення, відрізняються. Більш того, різні сценарії і процеси промислового виробництва призводять до великих відмінностей в ступені автоматизації, інформатизації та інтелекту. Ось чому так складно повністю підключити всі пристрої одного підприємства. Весь Інтернет речей настільки фрагментований, що стандартизація ще не завершена. Тому необхідно вирішити, який протокол IoT ви виберете для свого проекту IoT, буде сумісний з іншими платформами та бездротовими протоколами, і використовувати шлюзи IoT для трансформації протоколу IoT.

ПриDusun IoTМи розробляємо апаратне забезпечення шлюзу IoT та готові рішення IoT, сумісні з LTE-M, Wi-Fi, BLE, Z-WAVE,Підпункт, LoRa та багато інших протоколів IoT. Наші шлюзи IoT також підтримують програмування, вторинну розробку та інші SDK, що дозволяє користувачам легко налаштовувати свої програми шлюзу IoT.

3 МОДЕЛЮВАННЯ БЕЗПРОВОДОВИХ МЕРЕЖ У СЕРЕДОВИЩІ OMNeT++ З ВИКОРИСТАННЯМ ФРЕЙМВОРКУ INET

Проектування будь-якої сучасної інформаційної системи зі складною структурою з широким набором протоколів завжди починається з побудови і

вивчення її імітаційної моделі. Метою моделювання є визначення оптимальної топології, адекватний підбір мережевого обладнання, визначення продуктивності мережі та можливого майбутнього розвитку. Однією з переваг імітаційного моделювання є можливість проведення ряду досліджень для визначення надійності системи та її стійкості у разі відмов обладнання. Проводити подібні дослідження на працюючій мережі не можна, так як це може негативно позначитися на стабільності її роботи, до того ж при виході з ладу використовуваного обладнання є ризик понести фінансові втрати. Точне моделювання досліджуваного обладнання дозволяє отримати ті ж результати, що і при реальному використанні даного обладнання, заощадивши при цьому кошти на його придбанні.

На сьогоднішній день існує безліч інструментів моделювання, до яких пред'являються досить жорсткі вимоги, такі як: детальна реалізація протоколів на всіх рівнях, можливість підключення власних модулів, гнучка можливість зміни параметрів імітаційної моделі, незалежність від платформи, розвинений графічний інтерфейс, а також доступність продукту і його ціна. Одним з таких інструментів, що відповідає цим вимогам, є симуляційне середовище OMNeT++, яке має розвинений графічний інтерфейс як для побудови моделей, так і для аналізу отриманих результатів. Ще однією важливою перевагою є його доступність, при цьому функціонал середовища не поступається іншим платним інструментам моделювання.

3.1 Постановка проблеми та об'єкт дослідження

У дипломній роботі розглядається один з можливих підходів до проектування та аналізу безпроводової локальної мережі (WLAN) з використанням середовища моделювання OMNeT++1,2. Поставлено задачу комплексного дослідження імітаційної моделі найпростішої мобільної

безпроводової локальної мережі шляхом її послідовного ускладнення для врахування особливостей різних режимів роботи безпроводової мережі. В якості основи для розробки моделей пропонується використовувати типові компоненти фреймворку INET, конфігурація яких дозволяє моделювати пристрої, що відповідають необхідним вимогам.

Об'єктом дослідження є безпроводові локальні мережі, які повністю відповідають стандарту таких водних мереж, як Ethernet, але використовують інше середовище передачі даних: інфрачервоне випромінювання або радіохвилі НВЧ діапазону. Ці мережі можуть бути стаціонарними та мобільними. Стаціонарні вузли мережі жорстко прив'язані до певної точки простору. Мобільні вузли дозволяють переміщати вузли мережі в межах однієї точки доступу або одного сегмента мережі, в той час як мобільні мандрівники не тільки дозволяють переміщати вузли мережі, але і переміщати їх за допомогою автоматичного перепідключення з однієї точки доступу в іншу. За характером з'єднань WLAN вони можуть підтримувати два основні режими роботи:

— point-to-point, або Ad-Hoc режим, при якому зв'язок між вузлами встановлюється безпосередньо, без використання спеціальних точок доступу;

— Point-to-multipoint, або режим інфраструктури, в якому мережа складається принаймні з однієї точки доступу, підключеної до проводової мережі, і деякого набору безпроводових вузлів.

У роботі основну увагу приділено аналізу моделей мобільних Ad-Hoc мереж, що функціонують як з прямою взаємодією вузлів, так і з опосередкованою взаємодією через проміжні вузли. Це дозволило дослідити роботу самоорганізованих WLAN з динамічною маршрутизацією повідомлень до вузлів, розташованих поза зоною радіодоступу конкретного малопотужного трансивера вузла, використовуючи для цієї мети проміжні вузли і значно розширивши зону дії конкретного сегмента WLAN.

Для імітаційного моделювання таких мереж пропонується використовувати фреймворк INET1,2, який входить в комплект поставки OMNeT++. Він містить

широкий спектр компонентів для моделювання як мережі в цілому, так і окремих її елементів, а саме: фізичного середовища і режимів поширення сигналу в ній, різних типів антен, приймачів, передавачів і мережевих карт з можливістю обліку їх енергоспоживання.

Першим етапом на шляху до вирішення цього завдання стала розробка технології процесу побудови і вивчення найпростішої WLAN, що складається всього з двох вузлів, з'єднаних радіоканалом для передачі дейтаграм UDP. Для проектування імітаційної моделі такої мережі достатньо використовувати лише три компоненти фреймворку INET, а саме:

— Композитний модуль WirelessHost

— Композитний модуль IdealRadioMedium

— простий модуль IPv4NetworkConfigurator.

Композитний модуль WirelessHost є моделлю безпроводового хоста і є одним із розширень модуля StandartHost, на якому базуються всі інші моделі хостів TCP/IP. Внутрішня структура цього модуля (рис. 3.1) складається з чотирьох рівнів: додаткового, транспортного, мережевого та канального, який представлений мережевим інтерфейсом.

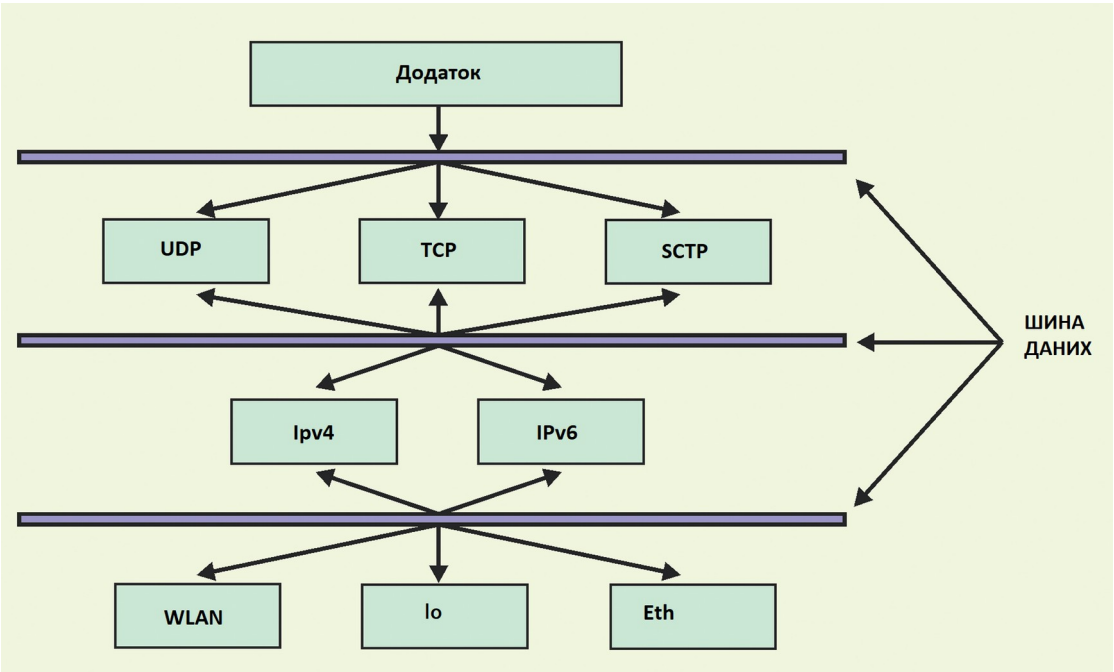


Рисунок 3.1 - Внутрішня структура хоста WirelessHost

Кожен з шарів включає в себе набір попередньо визначених компонентів з фреймворку INET, тип яких можна змінити через конфігураційний файл. Зокрема, прикладний рівень містить безрозмірний масив компонентів програми, кожен з яких імітує, як додаток поводиться на хост-моделі. Цей модуль може як генерувати вихідний трафік, передаючи його в нижні шари, так і приймати вхідний трафік. Транспортний рівень складається з трьох компонентів, які моделюють протокол користувацьких дейтаграм (UDP), протокол керування передачею (TCP) і протокол передачі керування потоком (SCTP). На мережевому рівні є два компоненти: протокол Inernet версії 4 (IPv4) і протокол Inernet версії 6. Канальний рівень містить компоненти, що реалізують мережеві інтерфейси, такі як дротовий Ethernet (Eth), безпроводовий (wlan), внутрішній loopback (lo) тощо.

Для імітації фізичного середовища, в якому відбувається безпроводовий зв'язок, використовується композитний модуль IdealRadioMedium. Він відповідає за імітацію поширення сигналу, його загасання при віддаленні, облік перешкод та інших фізичних явищ. Модель фізичного середовища описує, коли, де і як передача і сторонні шуми досягають приймачів. Модуль IdealRadioMedium має складну структуру (рис. 3.2) і включає в себе інші заздалегідь визначені компоненти, що моделюють наступні фізичні явища і процеси:

- Поширення — описує, як радіосигнал поширюється в просторі в часі.

- аналогове представлення радіосигналу (analogModel) - імітує процес перетворення аналогового представлення передач в аналогове представлення прийомів;

- backgroundNoise є моделлю фонового шуму і описує тепловий шум, космічний фоновий шум та інші випадкові флуктуації електромагнітного поля, що впливають на якість каналу зв'язку;

- Зменшення потужності на відстані (pathLoss) — описує зменшення потужності під час поширення сигналу в просторі.

- ObstacleLoss — це модель втрат, яка описує зменшення потужності сигналу під час проходження через перешкоди та фізичні об'єкти.

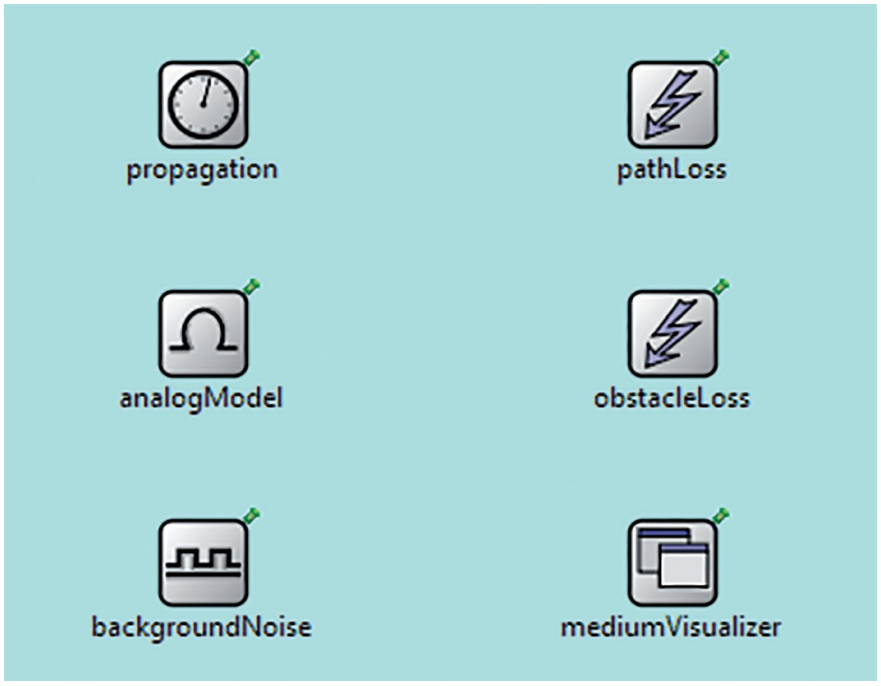


Рисунок 3.2 - Внутрішня структура композитного модуля IdealRadioMedium така: propagation — поширення, analogModel — аналогова модель, backgroundNoise — фоновий шум, pathLoss — втрата потужності, obstacleLoss — втрата потужності через перешкоди, mediumVisualizer - візуалізатор поширення радіосигналу

В цілому моделі фізичного середовища, реалізовані в INET, описують фізичний пристрій, який здатний передавати і приймати сигнали. До них відносяться: модель антени, моделі приймача і передавача, а також модель енергоспоживання. Модель антени поділяється на модель передавача та модель приймача. Відокремлення моделі передавача від моделі приймача дозволяє отримати асиметричні конфігурації.

3.2 Модель зв'язку UDP двох безпроводових вузлів

Підхід до побудови даної моделі буде розглянуто на прикладі безпроводової мережі, що складається з двох вузлів, що взаємодіють між собою за протоколом

UDP. У даній моделі вузли будуть розташовуватися на відстані 400 м один від одного, з дальністю дії трансивера 500 м для кожного з вузлів. Фреймворк INET містить два типи модулів, які працюють за протоколом UDP:

- UDPBasicApp – модуль, який генерує UDP-пакети заданої довжини на задану IP-адресу через заданий інтервал часу;

- UDPSink – це модуль, який імітує програму, яка отримує повідомлення з UDP-шару, підраховує їх кількість і зупиняє їх подальшу обробку.

У досліджуваній моделі хостА необхідно згенерувати UDP-повідомлення розміром 1 КБ і передати його хостБ через випадковий проміжок часу. Модель безпроводового вузла WirrelessHost, що використовується з фреймворку INET, вже має модуль інтерфейсу програми, тому для реалізації завдання потрібно лише перевизначити тип модуля, що використовується в конфігураційному файлі, який може виглядати так:

*.hostB.numUdpApps = 1

*.hostB.udpApp[0].typename="UDPSink"

*.hostB.udpApp[0].localPort=5000

*.hostA.numUdpApps =1

*.hostA.udpApp[0].typename="UDPBasicApp"

*.hostA.udpApp[0].destAddresses = "hostB"

*.hostA.udpApp[0].destPort = 5000

*.hostA.udpApp[0].messageLength = 1000B

*.hostA.udpApp[0].sendInterval = exponential(10 мс)

Цей параметр повідомляє, що hostA використовує модуль UDPBasicApp, який генерує повідомлення UDP розміром 1 КБ і надсилає їх через випадковий інтервал часу, описаний експоненціальним розподілом із середнім значенням 10 мс. Для того, щоб згенеровані повідомлення дійшли до адресата, у конфігураційному файлі вказується ім'я вузла, для якого призначене повідомлення, а також номер порту, наприклад 5000. HostB використовує модуль UDPSink, а також працює на порту 5000.

Крім прикладного рівня, конфігураційний файл повинен містити визначення фізичного рівня, який представлений в моделі хоста WirelessHost у вигляді мережевого адаптера, що включає в себе антену і радіоприймач-передавач. У середовищі INET існує велика різноманітність радіостанцій, які підтримують різні протоколи фізичного рівня, але в цьому прикладі буде використовуватися ідеалізована модель фізичного середовища, хости якої містять модуль IdealRadio як частину IdealWirelessNic. Виходячи з вищесказаного, конфігурація фізичного рівня буде наступною:

.host.wlan[*].typename = "IdealWirelessNic"

.host.wlan[*].radio.transmitter.CommunicationRange = 500m

.host.wlan[*].radio.receiver.ignoreInterference = true

**.бітрейт = 1 Мбіт/с

Після того, як запускається імітаційна модель, відкриється графічне вікно середовища виконання, яке показує всю мережу та її модулі. Середовище дозволяє в будь-який момент відобразити внутрішню структуру складеного модуля подвійним клацанням на його піктограмі. Слід зазначити, що відображувана структура модуля буде відрізнятися від показаної на рис. 1. Це пов'язано з тим, що після того, як модель була запущена середовищем моделювання, воно обробило конфігураційний файл і налаштувало параметри компонентів WirelessHost.

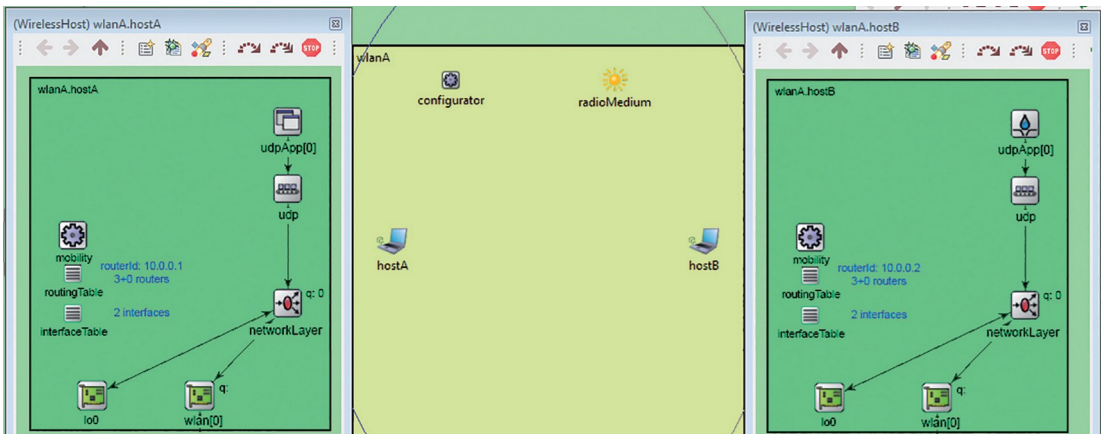


Рисунок 3.3 - Модель WLAN та внутрішня структура композитних модулів вузлів hostA та hostB: udpApp[0] — прикладний модуль, udp — модуль протоколу UDP, networkLayer — мережевий рівень, Io0 — закільцьований мережевий

інтерфейс, wlan[0] — безпроводовий мережевий інтерфейс, mobility — модуль положення вузла в просторі, routingTable — таблиця маршрутизації interfaceTable — таблиця мережевих інтерфейсів

На рисунку 3.3, кожен хост тепер має лише один мережевий адаптер, але з двома мережевими інтерфейсами кожен. При цьому один з них є внутрішнім шлейфом (lo), а другий - зовнішнім (wlan) і підключається до безпроводової мережі через внутрішній трансивер. Обидва вузли мають однакову структуру не тільки на фізичному рівні, але і на канальному, мережевому, транспортному рівнях. Різниця лише на рівні додатків, а саме в типі використовуваного додатка.

Коли запускається модель, ви можете побачити, як UDPBasicApp, що працює на hostA, генерує UDP-пакети з випадковими часовими циклами. Потім ці пакети проходять через рівні UDP і IPv4 і потрапляють до мережевого інтерфейсу WLAN, який ставить вхідні пакети в чергу і передає їх в найкоротші терміни. Використовуючи стекову реалізацію в мережевому інтерфейсі, ви можете зіставити частоту пакетів з верхнього шару з пропускною здатністю каналу, а також зі швидкістю середовища передачі. Це означає, що поки в черзі стека є пакети, вони будуть передаватися один за одним без пробілів між ними.

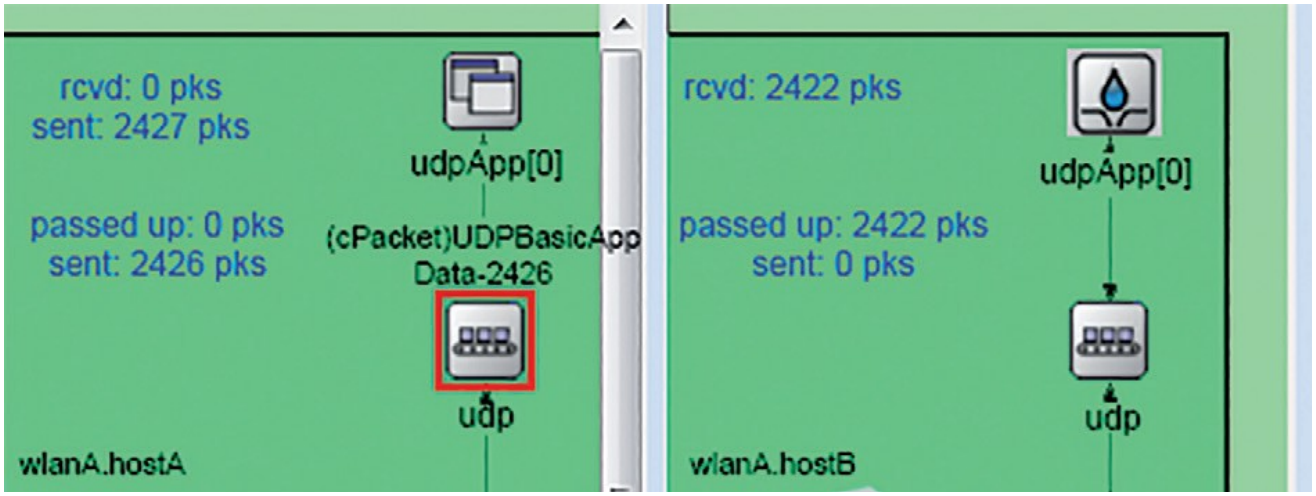


Рисунок 3.4 - Результати виконання імітаційної моделі:
rcvd - кількість отриманих пакетів; sent - кількість відправлених пакетів
Pass Up — кількість пакетів, переданих додатку

За результатами моделювання (рисунок 1.4) можна побачити, що UDP-додаток на hostA згенерував 2427 пакетів за 25 секунд. При цьому на транспортному рівні UDP було оброблено 2426 пакетів. З них 2422 пакети були передані по радіо і надійшли на хостБ. Тут вони пройшли через канальний, мережевий і транспортний рівні цього вузла і увійшли в UDP-додаток hostB. Таким чином, кількість пакетів вказує на те, що за 25 секунд було отримано 2422 пакети довжиною 1028 B (1000 B message + 8 B UDP + 20 B IP), а це означає, що швидкість передачі склала близько 800 Кбіт/с.

3.3 Статична модель маршрутизації для зв'язку з віддаленим хостом

Середовище моделювання OMNet++ не обмежується проектуванням і дослідженням простих моделей. Це також дає можливість вивчати більш складні моделі і ситуації, де ефективність використання резервування передачі була проаналізована на прикладі імітованої моделі провідної комп'ютерної мережі. Інший приклад, який буде розглянуто нижче, демонструє підхід до проектування і вивчення більш складної структури безпроводової мережі.

Припустимо, що є необхідність забезпечити безпроводовий зв'язок і передачу UDP-повідомлень від hostA до hostB з радіусом дії всього 250 м для їх трансиверів, а відстань між цими вузлами становить 400 м, що виключає можливість їх безпосереднього зв'язку. Крім того, між вузлами є ще три вузли, hostR1, hostR2 і hostR3, які в процесі своєї роботи можуть заважати роботі сусідніх вузлів. Особливість досліджуваної моделі полягає в тому, що трансивери мережевих адаптерів, маючи невелику потужність, обмежують діапазон своєї дії, що призводить до неможливості прямого зв'язку між двома вузлами. Однак з'єднання може бути встановлено, якщо між цими вузлами є інші вузли, які можуть транслювати і передавати мережеві пакети. Для цього всі або частина проміжних вузлів повинні підтримувати маршрутизацію.

Якщо до початкової моделі додати ще три вузли (рис. 1.3), обмежити потужність всіх трансиверів до 250 м, і запустити модель, то можна побачити, що hostA посилає UDP-пакети сусіднім вузлам, але останні їх не приймають, тому що ці пакети для них не призначені. Для того, щоб сусідні вузли не відкидали отримані пакети, а передавали їх іншому вузлу, необхідно, щоб на проміжних вузлах була налаштована таблиця маршрутизації. У цьому найпростішому випадку буде розглянуто приклад статичної маршрутизації, яка налаштовується через простий модуль IPv4NetworkConfiguration у конфігураційному файлі, який виглядає так:

#Автоматичне Налаштування статичних маршрутів

*.configurator.config = xml("<config>

<інтерфейс host='**' address='10.0.0.x' netmask='255.255.255.0' />

<autoroute metric='errorRate' />

</config>")

#Відключення Оптимізація записів таблиці маршрутизації

*.configurator.optimizeRoutes = false

#Відключення Записи таблиці маршрутизації, створені з маски мережі

Ця конфігурація виконується за допомогою рядка XML, параметри якого вказують конфігуратору призначити IP-адреси в діапазоні 10.0.0.x і використовувати розрахунковий рівень помилок передачі між хостами для налаштування статичних маршрутів. Таким чином, маршрути будуть розроблені таким чином, щоб мінімізувати кумулятивні помилки, що призведе до правильно налаштованої мережі IPv4 без будь-якого додаткового ручного налаштування. Сформовані таблиці маршрутизації зберігаються в параметрі routingTable кожного хоста, який можна переглядати у графічному середовищі виконання (рисунок 1.5).

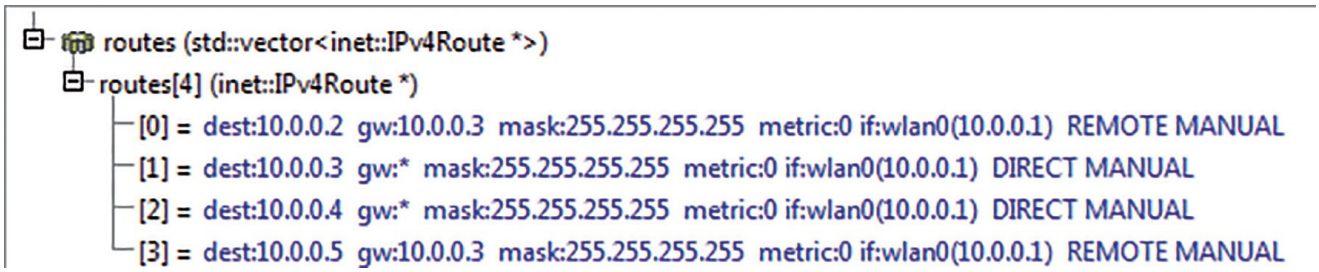


Рисунок 1.5 - Таблиця маршрутизації HostA:

dest — адреса призначення, gw — шлюз; mask—маска підмережі Metric – мережевий показник

Як видно з таблиці, hostA (10.0.0.1) має прямий інтерфейс до hostR1 (10.0.0.3) і hostR2 (10.0.0.4). Також у таблиці є маршрут, який інформує про те, що hostB (10.0.0.2) можна отримати через hostR1, використовуючи hostR1 як шлюз, а до hostR3 (10.0.0.5) можна отримати доступ через шлюз hostR2. Коли ви закінчите налаштовувати мережеву модель і запускати її, ви зможете з часом побачити, як UDP-пакет, згенерований hostA, надходить на hostR1, але тепер він не відкидає цей пакет, а приймає його і пересилає на інший хост.

Цей процес відбувається відповідно до статичних налаштувань маршрутизації, в яких проміжні вузли цього сегмента WLAN виступають в ролі шлюзів, майже вдвічі збільшуючи діапазон можливої безпроводової взаємодії між хостом A і хостом B. Основна відмінність цієї моделі полягає в тому, що вона імітує процес, при якому пакет, згенерований hostA (UDPBasicAppData-0), не потрапляє в радіоканал безпосередньо на хостB, а проходить через мережевий і канальний шари хостаA і тепер адресується хостR1 (рисунок 1.6).

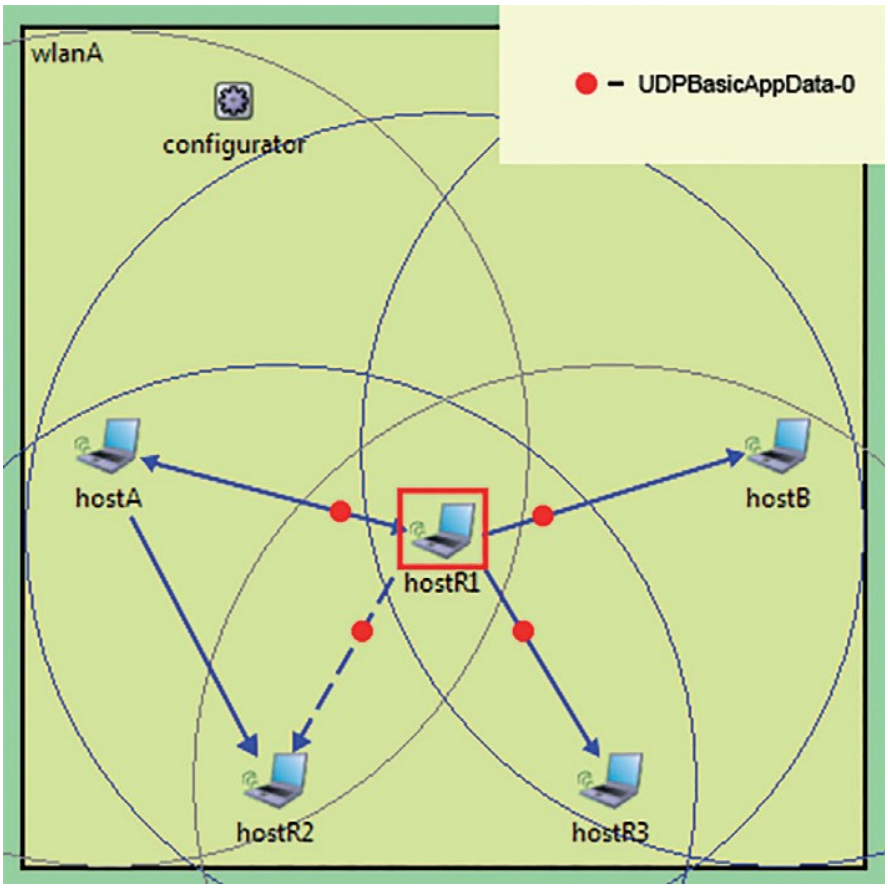


Рисунок 1.6 - Налаштована модель WLAN зі статичною маршрутизацією. configurator — seti configurator, hostA — uzel A, hostR1 — uzel R1, hostB — uzel B, hostR2 — uzel R2, hostR3 — узел R3

Цей процес виконується на базі даних, що зберігається в пам'яті хоста, таблиці маршрутизації, з якої всі пакети, призначені для доставки в хостВ, направляються на вхід хоста R1. Пакети, що надходять на його вхід, будуть підняті на мережевий рівень і негайно відправлені назад в мережу відповідно до таблиці маршрутизації, що зберігається в пам'яті hostR1. Оскільки hostR1 має прямий шлях доступу до hostB, UDP-пакет, що надходить до нього, буде безпосередньо перекладено до hostB.

3.4 Інтерференційна модель

У попередній моделі WLAN були реалізовані ідеалізовані мережеві умови, які не враховували таке фізичне явище, як інтерференція радіохвиль, що виникає при надходженні двох або більше радіосигналів на вхід радіоприймача, через що вони стикаються, спотворюють і порушують нормальну роботу приймача радіосигнал. До сих пір цей ефект не враховувався, і пристрої з повнодуплексним зв'язком по суті моделювалися. У той же час середовище OMNeT++ реалізує чотири основні способи опису та представлення сигналів.

Перший вид називається дальнім. Саме це реалізовано в компоненті IdealRadioMedium. Перевагами такої конструкції є компактність, передбачуваність і висока продуктивність. Однак його недоліком є те, що він не точно відображає реальну поведінку фізичного середовища.

Друга структура являє собою вузькосмуговий сигнал зі скалярною потужністю сигналу, несучою частотою і смугою пропускання. Його перевага полягає в тому, що він може обчислювати відношення сигнал/шум і є достатнім у більшості випадків для моделювання мережі IEEE 802.11.

Третя структура даних описує сигнал, сила якого змінюється з часом. У цьому випадку рівень сигналу представлений одновимірним значенням часу, яке точно слідує за переданими імпульсами. Це представлення використовується в радіохвильовому моделюванні IEEE 802.15.4a UWB.

Четверте представлення використовує багатовимірні значення для опису потужності сигналу, яка змінюється як за часом, так і за частотою. Це представлення можна використовувати для моделювання радіохвиль IEEE 802.11b.

У всіх цих прикладах ми використовували просту модель фізичного середовища на основі модуля IdealRadioMedium, яка використовує представлення діапазону, де ступінь впливу сигналу на сусідні вузли залежить від відстані, на якій вони розташовані. При роботі з цим модулем і його конфігурації існує всього три основних діапазони.

1. Дальність зв'язку — дальність надійного прийому і передачі радіосигналів;

2. Interference Range — діапазон, в якому нормальний зв'язок вже неможливий, але він все ще має значний вплив на трансивери інших пристроїв;

3. Дальність виявлення — діапазон, де немає впливу вузла на приймально-передавальні пристрої інших пристроїв, але є можливість виявити наявність і роботу цього пристрою.

Для дослідження ступеня інтерференції радіохвиль у конфігураційному файлі компонент IdealRadioMedium був налаштований на смугу перешкод з відстанню 500 м. Призначені параметри описують той факт, що радіосигнали слабшають з відстанню, але є смуга, в якій їх вже не можна правильно приймати, але вони все ще досить сильні, щоб впливати на інші сигнали. що призводить до збою прийому.

Допускаємо враховувати перешкоди в радіоприймачі від роботи сусідніх вузлів

*.host * .wlan[*].radio.receiver.ignoreInterference = rangt

Зробіть діапазон перешкод рівним двоканальному діапазону *.host*.wlan[*].radio. transmitter.maxInterferenceRange = 500m

Відображення діапазону перешкод хостаA на діаграмі

*.hostA.wlan[0].radio.displayInterferenceRange = true

Щоб дослідити цей режим, конфігураційний файл був увімкнений для запису та запису подій, які відбуваються в моделі під час її запуску. По закінченню роботи моделі були сформовані файли звітів, згідно з якими в процесі роботи моделі:

- hostA згенерував 92 повідомлення UDP по 1 КБ кожне.

- Рівень UDP HostA передав 91 1008B дейтаграм.

- У мережу було відправлено 89 пакетів розміром 1028B, що проходять через MAC-рівень;

- однак hostB отримав лише 1 пакет за 1 секунду модельного часу.

Якщо ми тепер проаналізуємо часову діаграму процесу моделювання зареєстрованої мережі, то виявимо, що лише за 800 мс вхідного часу моделі,

wlanB.hostB.udpApp(0) отримав одне з перших повідомлень, згенерованих хостом А та ретрансльованих хостR1. Висока інтенсивність (середній час 10 мс) випадкової генерації UDP-пакетів хостом, на-

В результаті перешкод перешкод і боротьби за доступ до безпроводового носія даних повідомлення було відправлено з хостаА на хостБ тільки в момент значної паузи на хостА. У той же час боротьба за доступ до безпроводового середовища передачі даних точилася між hostA і hostR1, які хотіли передавати як прямі, так і ретрансльовані UDP-пакети на hostB. Але якщо hostB отримав одне з перших повідомлень, відправлених з hostA, це означає, що він не загубився в мережі і міг десь зберігатися. На це питання відповідає графік залежності від часу (T) довжини черги (L), що генерується в буфері мережевого адаптера hostR1, який ретранслює пакети між хостом А і хостом В. На рисунку 1.7 видно, що за 1 секунду модельного часу в цьому буфері зберігалося майже 80 пакетів, відправлених хостом, які hostR1 не встиг передати хостВ. На даний момент значення максимальної довжини буфера адаптера визначено за замовчуванням у модуль фреймворку INET. У реальній безпроводовій мережі довжина буфера або розмір буфера має велике значення для продуктивності мережі, особливо якщо адаптер використовується в такому пристрої, як шлюз.

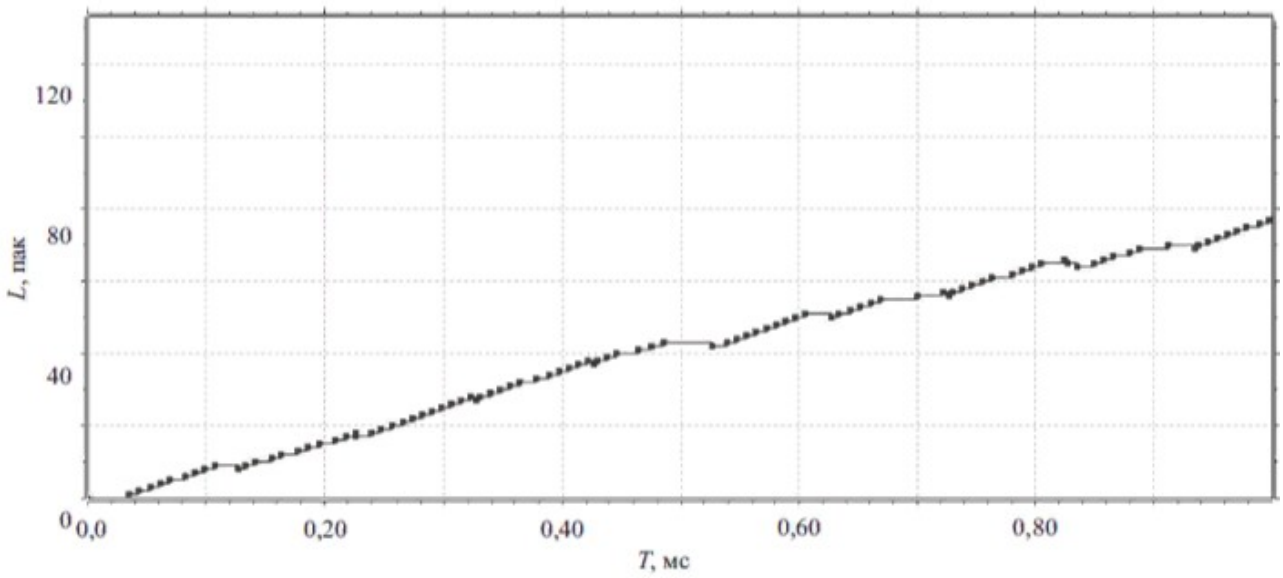


Рисунок 3.7 - Графік довжини черги в буфері мережевого шлюзу hostR1

Що заважало UDP-пакету з буфера шлюзу hostR1 потрапити в змодельовану мережу раніше? Відповідь на це питання дає аналіз зареєстрованих в мережі подій, що відбуваються в процесі її функціонування. На рисунку 1.8 наведена тимчасова діаграма роботи всіх елементів для всіх вузлів неводної мережі, з якої видно, що:

- перший пакет (UDPData-0) надходить в мережу (подія #22) і досягає hostR1 (#23) і hostB (#26) через певний проміжок часу. Причому друга подія відбувається пізніше, так як hostB знаходиться далі;

- hostB приймає радіосигнали від хостаA (від #26 до #45), але не розпізнає їх через значну віддаленість від джерела передачі;

- hostR1 починає успішно отримувати пакет від hostA (від #23 до #32);

- У процесі відправки першого пакета wlanB.hostA.udpApp(0) (#27) генерує друге повідомлення UDPBasicAppData-1, яке не може бути відправлено в мережу відразу. Він поміщається в буфер мережевого адаптера і залишається там до тих пір, поки мережевий адаптер не закінчить роботу з першим пакетом. Цей момент описується подією #36 та зеленою пунктирною стрілкою, що пов'язує її з подією #27;

- hostR1, успішно завершивши прийом першого пакета (#32), звертається до своєї таблиці маршрутизації (#35). На його основі він пересилає отриманий пакет на hostB і відправляє його в мережу (#39);

- однак трохи раніше (#32) hostA почав відправляти другий пакет, який раніше зберігався в буфері його мережевого адаптера;

- Одночасно з входом хост-приймача приймаються два радіосигнали (#48 і #51), які створюють перешкоди один одному, не дозволяючи вузлу hostB розпізнати UDP-пакет, що надходить зі шлюзу.

Підводячи підсумки дослідження моделі WLAN з урахуванням перешкод від роботи сусідніх пристроїв, слід зазначити, що спостерігається значне зниження їх продуктивності. Більшу частину часу передавальний вузол і шлюз працюють

одночасно, через що на трансивер приймального вузла надходять відразу два сигнали і «стикаються» один з одним.

Такий підхід до безпроводових мереж неприйнятний, і для того, щоб мінімізувати перешкоди, необхідний певний протокол доступу до медіасередовища, що визначає, який хост уповноважений на передачу даних і коли. Одним з таких протоколів може бути протокол на основі MAC на основі CSMA/CA з додатковими підтвердженнями і механізмом повторних спроб, який реалізований в середовищі OMNeT++ модулем CsmaCaMac, який при правильному налаштуванні може успішно апроксимувати базовий режим 802.11b Ad-Hoc.

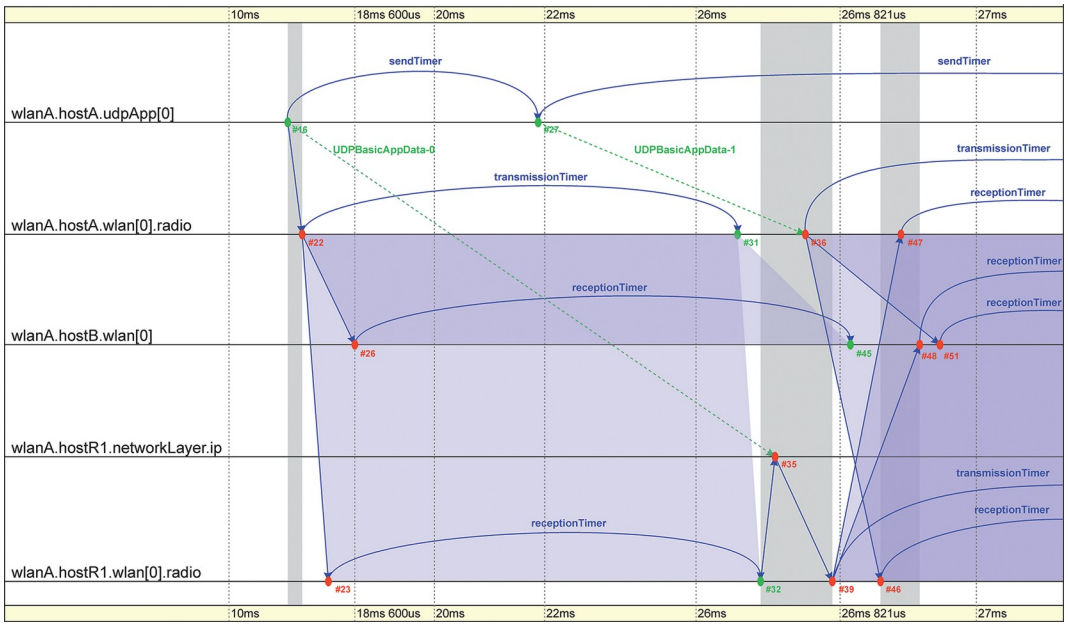


Рисунок 3.8 - Графік часу бездротової мережі:

sendTimer — час надсилання повідомлення receptionTimer — час прийому пакета

transmissionTimer — час передавання UDPBasicAppData-0 - це перший пакет, згенерований udpApp.

UDPBasicAppData-1 — другий пакет, згенерований udpApp

ВИСНОВКИ

В результаті кваліфікаційної роботи, присвяченої моделюванню роботи мережі на основі стандарту IEEE 802.11 та оцінці її стійкості засобами OMNet++, були проаналізовані технології та особливості безпроводової мережі.

Розглянуто методи побудови топології безпроводової мережі на основі технологій WDS, Ad-Hoc та Mesh, в результаті чого обрано технологію Ad Hoc. Наведено методи захисту безпроводової мережі, такі як WAP, WPA та WPA2, а також проаналізовано відмінності між основними режимами роботи WPA-PSK та WPA-Enterprise. Також описані стандарти взаємодії безпроводової точки доступу з кінцевими вузлами. Ці стандарти мають сертифікати IEEE 802.11g та 802.11n.

Представлені в роботі дослідження дозволяють продемонструвати, як імітаційне моделювання використовується при проектуванні та вивченні реальних безпроводових мереж. Показано, що можна створювати імітаційні моделі безпроводових мереж з використанням готових компонентів з фреймворку INET, які допомагають описати різні елементи мережі, а також зробити їх гнучку конфігурацію для моделювання необхідної поведінки.

На початковому етапі мережевого моделювання була розроблена структурна схема для загального розуміння роботи безпроводового зв'язку і проаналізована передбачена площа лісового покриття. В результаті робляться висновки про особливості рельєфу місцевості, описуються причини, які можуть вплинути на поширення сигналу. В якості місць для установки обладнання обрані ліхтарні стовпи, відстань між якими достатня для покриття точок безпроводового зв'язку і дозволяє створювати резервну топологію в разі виходу з ладу одного з пристроїв. Знайдено майданчики для подальшого моделювання та аналізу поведінки мережі.

В якості основної програми для моделювання мереж обрано OMNet++. Ця програма підходить для написання протоколів різних рівнів, для моделювання дротових і безпроводових мереж, а також дозволяє аналізувати роботу мережі за допомогою графіків, збираючи інформацію, отриману в ході моделювання мережі.

Підхід до моделювання різних режимів роботи безпроводових мереж демонструється реалізацією прямої взаємодії при проектуванні режиму Ad-Hoc, а також непрямого, при якому реалізується процес маршрутизації через проміжні вузли. Дослідження такого фізичного явища, як інтерференція, у дипломній роботі виявило факт негативного впливу один на одного суміжних вузлів, які погіршують якість радіозв'язку та можуть призвести до зниження швидкості передачі даних або їх повної втрати.

У дипломній роботі також продемонстровано підхід до вивчення роботи безпроводової мережі шляхом аналізу файлу часової діаграми, вивчення якого дозволило пояснити причину значних затримок у ретрансляції мережевих пакетів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Duan Q., Virtualized Software-Defined Networks and Services / Q. Duan, Toy M. – Норвуд: Arttech House, 2019. – 334 с.

2. Duan Q., Network як Service для Next Generation Internet (Telecommunications) Q. Duan, Wang S. - Стівенідж: The Institution of Engineering and Technology, 2017. - 440 с.

3. OPNET Community, OPNET [Електронний ресурс], режим доступу - https://sandilands.info/sgordon/teaching/resources/opnet.html.

4. Zhang Y. Network Function Virtualization: Concepts and Applicability in 5G Networks (Wiley - IEEE) / Y. Zhang - Нью-Йорк: Wiley-IEEE Press, 2017. 179 с.

5. Хабаров С.П. Моделювання мереж Ethernet в середовищі OMNeT++ INET. Науково-технічний журнал інформаційних технологій, механіки та оптики, 2018, том 18, No 3, с. 462–472. DOI: 10.17586/2226-1494-2018-18-3-462-472

6. Заяць А.М., Хабаров С.П. Організація доступу до безпроводових Ad Hoc мереж моніторингу лісових територій з середовища Windows 10 [Організація доступу до безпроводових Ad Hoc мереж моніторингу лісових територій з середовища Windows 10]. 2018. No 223. 285–299. DOI: 10.21266/2079-4304.2018.223.285-299

7. Сластіхін І.А., Богатирьов В.А. Резервне першочергове обслуговування в багатоканальних системах // Proc. 2018 Wave Electronics та її застосування в інформаційно-телекомунікаційних системах (WECONF). 2018. С. 8604301. doi: 10.1109/WECONF.2018.8604301

8. Арустамов С.А., Богатирьов В.А., Поляков В.І. Резервне копіювання передачі даних у дубльованих комп'ютерних системах у реальному часі // Досягнення інтелектуальних систем та обчислень. 2022. Т. 451. P. 103–109. DOI: 10.1007/978-3-319-33816-3_11

9. Богатирьов В.А., Алексанков С.М., Деркач А.М. Модель надійності кластера з міграцією віртуальних машин та відновленням на певному рівні деградації системи // Proc. 2018 Wave Electronics та її застосування в

інформаційно-телекомунікаційних системах (WECONF). 2018. С. 8604317. doi: 10.1109/WECONF.2018.8604317

10. Сластіхін І.А., Богатирьов В.А., Носков І.І. Імітаційна модель системи з агрегованими каналами та резервними передачами на рівні множинного доступу // CEUR Workshop Proceedings. 2019. Т. 2344.

11. Носков І.І., Богатирьов В.А., Сластіхін І.А. Імітаційна модель локальної комп'ютерної мережі з агрегацією каналів та випадковим способом доступу при резервуванні передач. 2018. Т. 18. No 6. P. 1047–1053. DOI: 10.17586/2226-1494-2018-18-6-1047-1053

12. Коломойцев В.С., Богатирьов В.А. Відмовостійка дворівнева схема безпечного доступу «сполучний вузол» // ACSR-Advances in Computer Science Research. 2017. Т. 72. P. 271–274. DOI: 10.2991/ITSMSSM-17.2017.56

13. Коломойцев В.С., Богатирьов В.А. Відмовостійка структура багаторівневого захищеного доступу до ресурсів мережі загального користування Комунікації в інформатиці та інформатиці. 2016. Т. 678. P. 302–313. DOI: 10.1007/978-3-319-51917-3_27

14. Хабаров С.П. Організація програмних точок доступу за допомогою ОС Windows 10 // Інформаційні системи і технології: Теорія і практика: Збірник наукових праць. Том. 10. Частина 2.., 2018. P. 60–73.

15. Богатирьов В.А., Сластіхін І.А. Моделі резервування передачі через агреговані канали // ACSR-Advances in Computer Science Research. 2017. Т. 72. P. 294–299. DOI: 10.2991/ITSMSSM-17.2017.60

16. Пролетарський А.В., Баскаков І.В., Чирков Д.М., Федотов Р.А., Бобков А.В., Платонов В.А. Безпроводові мережі Wi-Fi. М.: Національний відкритий університет «ІНТУЇТ», 2016. – 284 с.

17. Рошан П., Лієрі Д. Основи побудови безпроводових локальних мереж стандарту 802.11. Провулок. М.: Видавництво Вільямс, 2014. – 304 с.

18. Хабаров С.П. Моделювання мереж Ethernet у фреймворковому середовищі OMNeT++ INET. 2018. Т. 18. No3. 462–472. DOI: 10.17586/2226-1494-2018-18-3-462-472

19. Богатирьов В.А., Богатирьов С.В. Уніфікація резервних серверів у кластерах високонадійної комп'ютерної системи. 2019. No 6. P. 41–47.

20. Думов М.І., Хабаров С.П. Використання OMNET++ для моделювання безпроводових мереж Wi-Fi.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАГІСТЕРСЬКА РОБОТА

«Дослідження протоколів безпроводових мереж з метою організації оптимального віддаленого моніторингу пристроїв»

виконав студент: **Дмитро КОСТЕЦЬКИЙ**
керівник: **Андрій ЛЕМЕШКО,** доктор філософії, доцент

Актуальність:

Актуальність дослідження протоколів безпроводових мереж полягає в тому, що безпроводові мережі стають все більш поширеними та важливими в різних сферах, включаючи медицину, промисловість, транспорт та інші. Вибір оптимального протоколу для віддаленого моніторингу пристроїв дозволить покращити ефективність та зручність їх використання, забезпечити надійність та безпеку передачі даних, а також знизити витрати ресурсів. Це має великий потенціал для покращення якість життя людей та розвитку різних галузей.

Типи безпроводових мереж

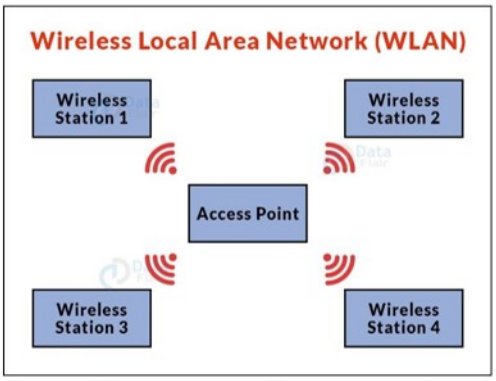


Схема безпроводової локальної мережі

Схема безпроводової міської мережі

Схема безпроводової персональної мережі

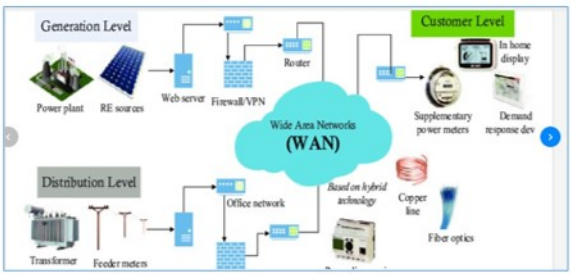
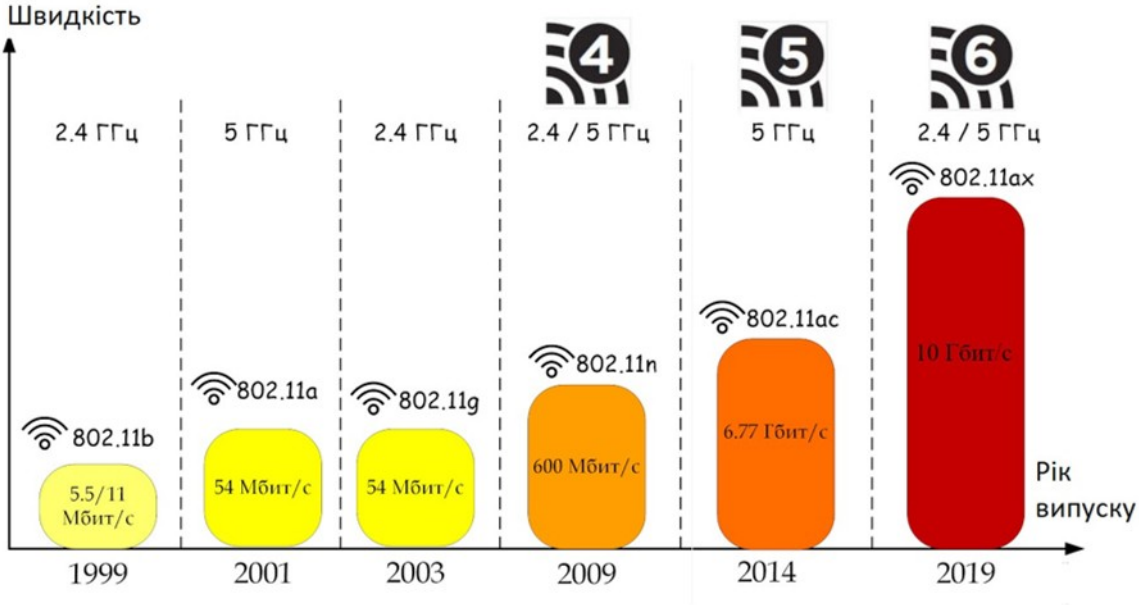
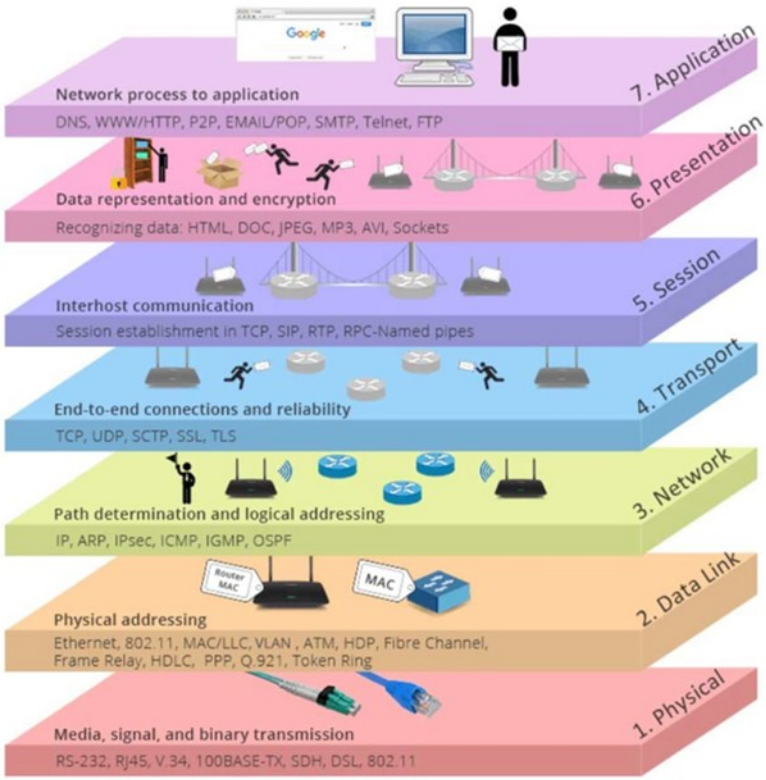


Схема безпроводової глобальної мережі

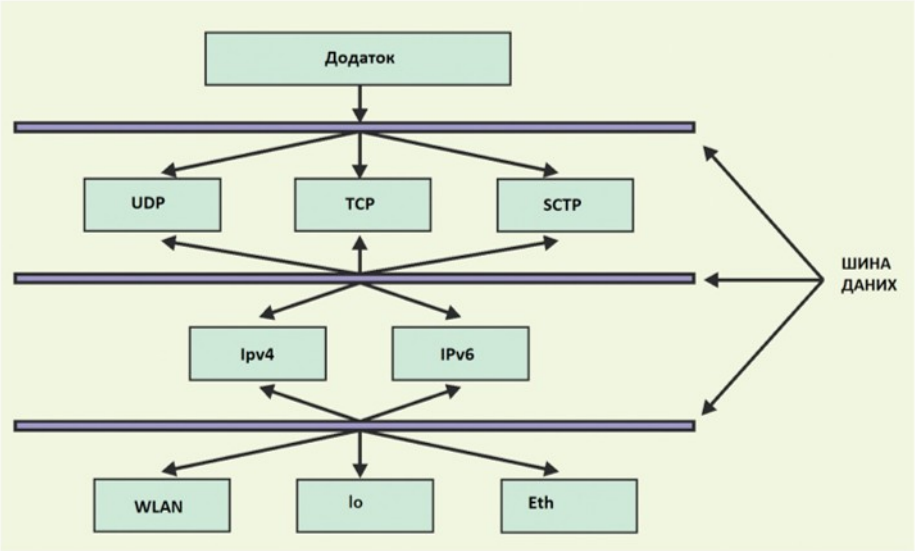
Наочна еволюція «літерних» стандартів Wi-Fi



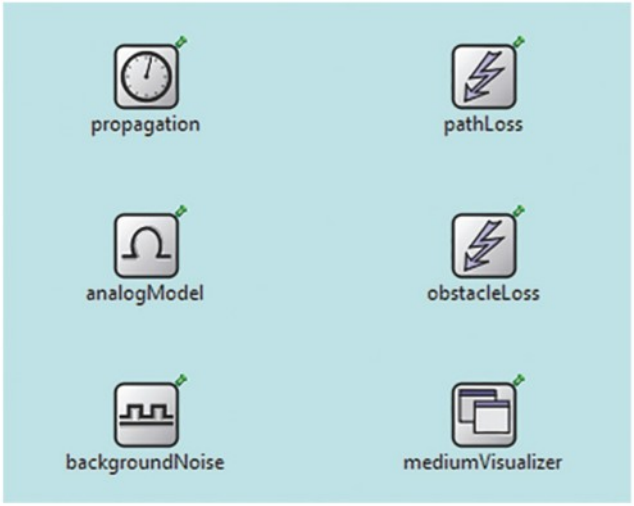
Модель OSI



Внутрішня структура хоста WirelessHost

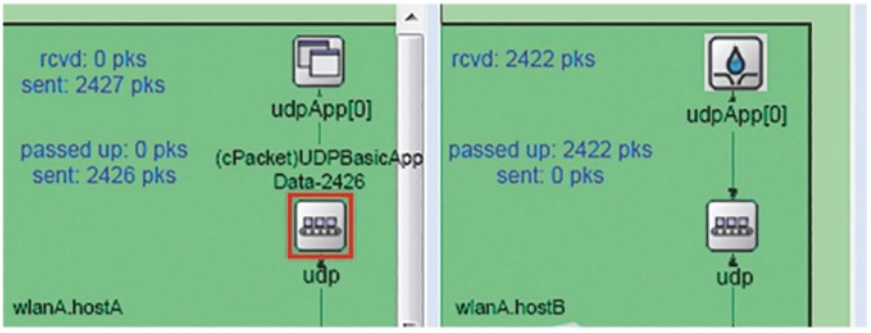


Внутрішня структура композитного модуля IdealRadioMedium

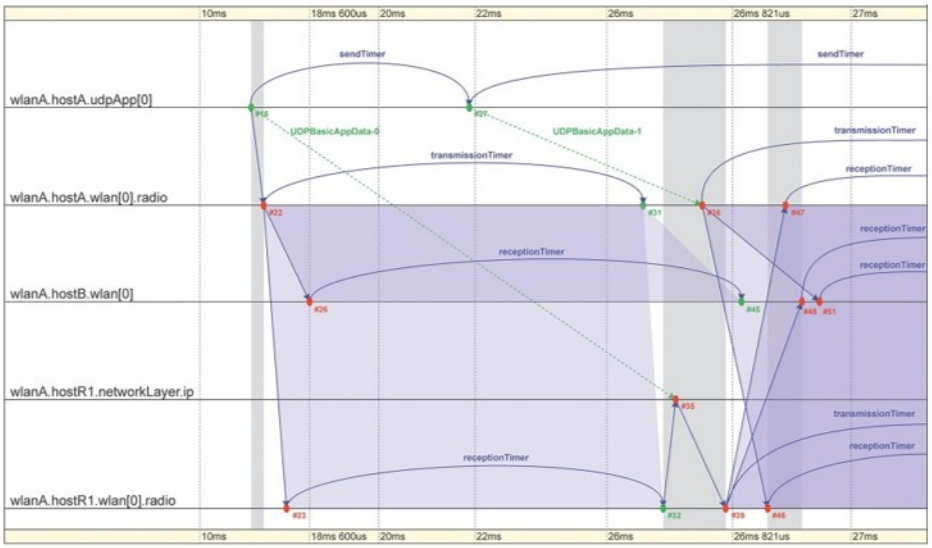


Модель WLAN та внутрішня структура композитних модулів вузлів hostA та hostB

Результати виконання імітаційної моделі



Часова діаграма роботи безпроводової мережі



Висновки

Представлені в роботі дослідження дозволяють продемонструвати, як імітаційне моделювання використовується при проектуванні та вивченні реальних безпроводових мереж. Показано, що можна створювати імітаційні моделі безпроводових мереж з використанням готових компонентів з фреймворку INET, які допомагають описати різні елементи мережі, а також зробити їх гнучку конфігурацію для моделювання необхідної поведінки.

Підхід до моделювання різних режимів роботи безпроводових мереж демонструється реалізацією прямої взаємодії при проектуванні режиму Ad-Hoc, а також непрямого, при якому реалізується процес маршрутизації через проміжні вузли. Дослідження такого фізичного явища, як інтерференція, у дипломній роботі виявило факт негативного впливу один на одного суміжних вузлів, які погіршують якість радіозв'язку та можуть призвести до зниження швидкості передачі даних або їх повної втрати.

У дипломній роботі також продемонстровано підхід до вивчення роботи безпроводової мережі шляхом аналізу файлу часової діаграми, вивчення якого дозволило пояснити причину значних затримок у ретрансляції мережевих пакетів.

Список публікацій:

1. Лемешко А.В, Антоненко А.В., Костецький Д.І., Шрам М.М., Закреничний А.С. Моделювання безпроводових мереж у середовищі OMNET++ з використанням Inet Framework. Науковий журнал«IT SYNERGY», 2023, випуск 1 (4), 37-59