Кафедра СИСТЕМ АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до бакалаврської кваліфікаційної роботи на тему

РЕАЛІЗАЦІЯ МОДЕЛІ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ ПРИ МУЛЬТИМОДАЛЬНОМУ РОЗПОДІЛІ ВУЗЛІВ

Студент групи КН-411 **Слота Назар Миколайович**

(шифр, прізвище та ініціали)

Керівник проекту _____ (**Олександр Белей**)

Консультанти _____ (_____)

_____ (_____)

_____ (_____)

_____ (_____)

Завідувач кафедри Михайло ЛОБУР

«___» _____ 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Інститут Інститут комп'ютерних наук та інформаційних технологій

Кафедра Систем автоматизованого проектування

Спеціальність F3 "Комп'ютерні науки"

„ЗАТВЕРДЖУЮ”

Завідувач

кафедри САП

Михайло ЛОБУР

«___» _____ 2025 р.

ЗАВДАННЯ

на бакалаврську кваліфікаційну роботу студента групи КН-411 ОКР Бакалавр

Слота Назар Миколайович

(прізвище, ім'я, по батькові)

1. Тема роботи (проекту) Реалізація моделі бездротової сенсорної мережі при мультимодальному розподілі вузлів

затверджена наказом по університету від 30.04.2025 р. № 1566-4-08

2. Термін подання студентом закінченої роботи (проекту) 06.06.2025

3. Вихідні дані для роботи (проекту)

- стандарти бездротової сенсорної мережі на основі технології зв'язку ZigBee;
- методика функціонування семирівневої моделі ISO\OSI.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які треба розробити)

- розробити моделі та дослідити можливість підключення Інтернету речей в умовах нерівномірного розподілу;
- виконати розрахунки та моделювання Інтернету речей у програмному середовищі OMNET++.

5. Перелік графічного матеріалу

- структури бездротової сенсорної мережів в житловому кварталі Манхеттен;
- модель аналізу бездротової сенсорної мережі при мультимодальному розподілі вузлів.

6. Перелік програмних продуктів, які належить використати в процесі розроблення роботи (проекту)

OMNET++ , C++, ZigBee

7. Консультування роботи (проекту), із зазначенням розділів роботи

Розділ	Консультант	Завдання видав		Завдання прийняв	

8. Дата, коли видано завдання 01.05.2025

Керівник **Олександр Белей**
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів роботи (проекту)	Термін виконання етапів роботи (проекту)	Примітка
1.	Ознайомлення з предметною областю, вивчення		
	літератури, подібних систем	01.05 – 5.05	
2.	Робота над першим розділом	6.05 – 11.05	
3.	Робота над другим розділом	12.05 – 17.05	
4.	Розробка і тестування системи	18.05 – 22.05	
5.	Робота над третім розділом	23.05 – 26.05	
6.	Оформлення текстової і графічної частини		
	бакалаврської кваліфікаційної роботи	27.05 – 30.05	

Студент _____
(підпис)

Керівник _____
(підпис)

АНОТАЦІЯ

Слота Н., Белей О.І. Реалізація моделі бездротової сенсорної мережі при мультимодальному розподілі вузлів. Бакалаврська кваліфікаційна робота. – Національний університет «Львівська політехніка», Львів, 2025 р.

Розширена анотація

Існує багато різних реалізацій бездротових сенсорних мереж (БСМ). Ці мережі можуть відрізнятися розміром (геометрією зони обслуговування), кількістю вузлів, інтенсивністю трафіку, просторовим розташуванням вузлів та їхньою мобільністю. Вибір методу організації радіоканалів та протоколу, що використовується для управління логічною структурою мережі, залежить від цих параметрів [1].

Різні застосування БСМ вимагають використання фіксованих або мобільних вузлів для організації мережі. Логічна структура БСМ визначається використовуваними правилами маршрутизації. У найпростішому випадку при побудові мережі збору даних часто використовується зіркоподібна структура, де всі вузли мережі розташовані в зоні обслуговування кластерного головного вузла (ГВ). Кластерний головний вузол зазвичай також виконує роль шлюзу. У цьому випадку зона обслуговування обмежена зоною ГК, яка зазвичай обмежена кількома сотнями метрів.

Щоб подолати обмеження цієї структури, для виконання функцій збору даних часто використовується структура з ретрансляційною організацією та мобільними кластерними вузлами (МКВ) [2]. Використання МКВ може значно розширити зону обслуговування БСМ та покращити зв'язок з мережею. Якщо траєкторію руху МКВ обрано таким чином, щоб вона проходила через зону зв'язку кожного вузла мережі протягом певного часу, то, вибравши відповідну швидкість руху, можна зібрати дані з заданої кількості вузлів протягом цього часу [3].

У цьому випадку тривалість збору даних залежить від швидкості руху голови кластера, кількості вузлів мережі та розміру зони обслуговування. Вимога до тривалості збору даних залежить від конкретного прикладного завдання, яке має вирішити мережа. Наприклад, у мережі для моніторингу температури навколишнього середовища та вологості ґрунту тривалість збору даних може обчислюватися хвилинами або десятками хвилин, тоді як у мережі для моніторингу наявності шкідливих речовин в атмосфері тривалість збору даних повинна бути порядку секунд.

На основі попередніх досліджень зазначимо, що для скорочення часу збору даних слід збільшити кількість МКВ. У цьому випадку виникають проблеми як у виборі кількості таких вузлів, так і в їх мобільності в межах зони обслуговування мережі, від чого залежить ефективність використання таких вузлів. Очевидно, що занадто велика кількість вузлів збільшує вартість мережі, тобто знижує ефективність мережі. Мережі мобільного зв'язку (ММЗ) зазвичай набагато дорожчі за фіксовані вузли, оскільки для їх переміщення потрібні транспортні засоби та енергія, а також підключення до глобальної мережі. У крайньому випадку від фіксованих вузлів можна повністю відмовитися, залишивши лише вузли мобільного зв'язку (ВМЗ), оснащені шлюзами, що

мінімізує час збору даних. У цьому випадку вартість мережі є найвищою. У проміжному випадку кількість мобільних вузлів повинна бути достатньою для забезпечення необхідної тривалості збору даних, але тривалість залежить не лише від кількості мобільних вузлів, але й від мобільності мобільних вузлів. Тому, як новий внесок цієї статті, ми розробляємо метод побудови мережі мобільних вузлів для підвищення ефективності використання ресурсів бездротових сенсорних мереж (БСМ). Новий метод дозволяє вибирати кластери з різною щільністю вузлів. Ідентифікація таких кластерів дозволяє використовувати мобільні головки кластерів для організації збору даних та вибору найкращої швидкості мобільного зв'язку в кожному кластері. Аналіз та моделювання демонструють ефективність запропонованої моделі. Крім того, ефективність використання мобільних головок кластерів може бути покращена відповідно до неоднорідності мереж Інтернету речей.

Метою кваліфікаційнаої роботи є проектування мережі Інтернету речей у житлових районах та розробка бездротової сенсорної мережі на основі технології зв'язку ZigBee.

Об’єктом дослідження виступають технології Інтернету речей у житловому районі.

Практична цінність бакалаврської кваліфікаційної роботи полягає у вивчені, аналізі та класифікації систем Інтернету речей. Крім того, цей проект також досліджує існуючу систему зв'язку в житлових районах Манхеттена та вибирає пристрої, що використовуються для побудови бездротової сенсорної мережі (БСМ). БСМ моделюється за допомогою програми OMNET++. Під час процесу проектування та моделювання необхідно розрахувати такі параметри, як споживання енергії, шум у тракті передачі/прийому, дальність зв'язку, рівень затухання та співвідношення сигнал/шум.

Ключові слова: Інтернет речей, бездротових сенсорних мереж, мультимодальний розподіл вузлів, мобільні кластерні вузли.

Список використаних джерел.

1. Belej, O., Fedirko, Y., Markelov, O. Ensuring accuracy of personal data processed in blockchain systems. (2024) CEUR Workshop Proceedings, 3723, pp. 13-41. - *CEUR Workshop Proceedings*, Volume 3723, Pages 13 – 41, 2024, 6th International Workshop on Modern Data Science Technologies Workshop, MoDaST 2024, Lviv, 31 May 2024 through 1 June 2024, Code 200872 –https://ceur-ws.org/Vol-3723/paper2.pdf

2. O. Belej, N. Nestor and N. Spas, "Building a Model of Fault Tolerance of Serial-Parallel Ports in a Self-Synchronous Microkernel," *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/TCSET64720.2024.10755721

3. O. Belej, I. Artyshchuk and M. Kutelmakh, "The Technology for Countering the Threats of Violation in the Information Security of Cloud Infrastructure," 2024 IEEE 19th International Conference on Computer Science and Information Technologies (CSIT), Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/CSIT65290.2024.10982655

ABSTRACT

Slota N., Belej O.I. Implementation of a wireless sensor network model with multimodal node distribution. Bachelor's thesis. - Lviv Polytechnic National University, Lviv, 2024.

Extended abstract

There are many different implementations of wireless sensor networks (WSNs). These networks can vary in size (geometry of the service area), number of nodes, traffic intensity, spatial arrangement of nodes, and their mobility. The choice of radio channel organization method and protocol used to manage the logical structure of the network depends on these parameters [1].

Different WSN applications require the use of fixed or mobile nodes to organize the network. The logical structure of the WSN is determined by the routing rules used. In the simplest case, a star-shaped structure is often used when building a data collection network, where all network nodes are located in the service area of a cluster master node (HM). The cluster master node usually also acts as a gateway. In this case, the service area is limited to the GC area, which is usually limited to several hundred meters.

To overcome the limitations of this structure, a structure with a relay organization and mobile cluster nodes (MCNs) is often used to perform data collection functions [2]. The use of MCUs can significantly expand the service area of the BSM and improve communication with the network. If the trajectory of the MCU movement is chosen so that it passes through the communication area of each network node for a certain time, then by choosing the appropriate speed of movement, it is possible to collect data from a given number of nodes during this time [3].

In this case, the duration of data collection depends on the speed of movement of the cluster head, the number of network nodes and the size of the service area. The requirement for the duration of data collection depends on the specific application task that the network must solve. For example, in a network for monitoring ambient temperature and soil moisture, the duration of data collection can be calculated in minutes or tens of minutes, while in a network for monitoring the presence of harmful substances in the atmosphere, the duration of data collection should be on the order of seconds.

Based on previous studies, we note that to reduce the data collection time, the number of MCUs should be increased. In this case, problems arise both in choosing the number of such nodes and in their mobility within the network service area, which determines the efficiency of using such nodes. Obviously, too many nodes increases the cost of the network, i.e. reduces the efficiency of the network. Mobile communication networks (MCNs) are usually much more expensive than fixed nodes, since their movement requires vehicles and energy, as well as connectivity to the global network. In the extreme case, fixed nodes can be completely abandoned, leaving only mobile communication nodes (MCNs) equipped with gateways, which minimizes the data collection time. In this case, the cost of the network is the highest. In the intermediate case, the number of mobile nodes should be sufficient to ensure the required duration of data collection, but the duration depends not only on the number of mobile nodes, but also on the mobility of mobile nodes. Therefore, as a new

contribution of this article, we develop a method for building a mobile node network to improve the resource utilization efficiency of wireless sensor networks (WSNs). The new method allows us to select clusters with different node densities. Identification of such clusters allows us to use mobile cluster heads to organize data collection and select the best mobile communication speed in each cluster. Analysis and simulation demonstrate the effectiveness of the proposed model. In addition, the efficiency of using mobile cluster heads can be improved according to the heterogeneity of the Internet of Things networks.

The purpose of the qualification work is to design an Internet of Things network in residential areas and develop a wireless sensor network based on ZigBee communication technology.

The object of the research is Internet of Things technologies in a residential area.

The practical value of the bachelor's qualification work is to study, analyze and classify Internet of Things systems. In addition, this project also investigates the existing communication system in residential areas of Manhattan and selects devices used to build a wireless sensor network (WSN). WSN is modeled using the OMNET++ program. During the design and modeling process, it is necessary to calculate parameters such as energy consumption, noise in the transmission/reception path, communication range, attenuation level and signal-to-noise ratio.

Keywords: Internet of Things, wireless sensor networks, multimodal node distribution, mobile cluster nodes.

References.

1. Belej, O., Fedirko, Y., Markelov, O. Ensuring accuracy of personal data processed in blockchain systems. (2024) CEUR Workshop Proceedings, 3723, pp. 13-41. - *CEUR Workshop Proceedings*, Volume 3723, Pages 13 – 41, 2024, 6th International Workshop on Modern Data Science Technologies Workshop, MoDaST 2024, Lviv, 31 May 2024 through 1 June 2024, Code 200872 –https://ceur-ws.org/Vol-3723/paper2.pdf

2. O. Belej, N. Nestor and N. Spas, "Building a Model of Fault Tolerance of Serial-Parallel Ports in a Self-Synchronous Microkernel," *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/TCSET64720.2024.10755721

3. O. Belej, I. Artyshchuk and M. Kutelmakh, "The Technology for Countering the Threats of Violation in the Information Security of Cloud Infrastructure," 2024 IEEE 19th International Conference on Computer Science and Information Technologies (CSIT), Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/CSIT65290.2024.10982655

ЗМІСТ

ВСТУП

Актуальність роботи. Інтернет речей – це абсолютно нова концепція, яка революціонізує не лише телекомунікації та інформаційні системи, а й спосіб життя людей. Використання технології бездротового доступу ближнього радіусу дії в системах промислової автоматизації стає все більш поширенішою.

Кількість пристроїв, підключених до Інтернету, подвоюється щороку. Впровадження Інтернету речей сприяло швидкому економічному розвитку, підвищенню рівня життя та збільшенню інвестицій. Сьогодні технологія бездротових мереж ближнього радіусу дії є єдиною довговічною бездротовою технологією, яка може вирішити проблему моніторингу промислових об'єктів. Комунікаційні мережі на основі технології ZigBee можуть створювати децентралізовану самоорганізуючу систему для збору, обробки та передачі інформації.

Розробка стандарту бездротової передачі даних ZigBee дозволяє використовувати мережі на основі цього протоколу бездротового зв'язку в багатьох сферах автоматизованого управління та моніторингу. У житловому районі для швидкого зв'язку в надзвичайних ситуаціях використовуються машинні приймачі. При розгортанні таких житлових районів для забезпечення доступу до мережі може використовуватися супутниковий зв'язок. У таких житлових районах можна організувати телефонний зв'язок, доступ до мережі та відеоконференції.

Метою бакалаврської кваліфікаційної роботи є проектування мережі Інтернету речей у житлових районах та розробка бездротової сенсорної мережі на основі технології зв'язку ZigBee.

Завдання:

- проаналізувати можливість побудови мережі Інтернету речей на основі існуючої інфраструктури мобільної мережі;

- розробити моделі та дослідити можливість підключення Інтернету речей в умовах нерівномірного розподілу;

- виконати розрахунки та моделювання Інтернету речей у програмному середовищі OMNET++.

Об’єктом дослідження виступають технології Інтернету речей у житловому районі.

Предмет випускної кваліфікаційної роботи присвячений розробці бездротової сенсорної мережі на основі технології зв'язку ZigBee.

Практична цінність бакалаврської кваліфікаційної роботи полягає у вивчені, аналізі та класифікації систем Інтернету речей. Крім того, цей проект також досліджує існуючу систему зв'язку в житлових районах Манхеттена та вибирає пристрої, що використовуються для побудови бездротової сенсорної мережі (БСМ). БСМ моделюється за допомогою програми OMNET++. Під час процесу проектування та моделювання необхідно розрахувати такі параметри, як споживання енергії, шум у тракті передачі/прийому, дальність зв'язку, рівень затухання та співвідношення сигнал/шум.

Бакалаврська кваліфікаційна робота за структурою складається із вступу, переліку умовних позначень, трьох розділів, висновків, списку використаних джерел та додатків.

1. АНАЛІЗ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ В ІНТЕРНЕТІ РЕЧЕЙ

1.1. Основні концепції та архітектура Інтернету речей

На початку 21 століття, зі швидким розвитком мереж з комутацією пакетів, особливо Інтернету, світова телекомунікаційна галузь вперше створила та впровадила нову модель розвитку комунікацій – мережу наступного покоління (NGN). Технологія NGN еволюціонувала від гнучких механізмів до підсистем виявлення каналів IMS та бездротових мереж LTE з довгостроковими перспективами розвитку. Водночас, завжди будуть мережі, що охоплюють користувачів NGN, тому кількість користувачів таких мереж буде обмежена охопленням населення Землі.

На початку 21 століття, зі швидким розвитком мереж з комутацією пакетів, особливо Інтернету, виникла та почала впроваджуватися нова парадигма розвитку комунікацій – мережа наступного покоління (NGN) [3].

Нове покоління технологій еволюціонувало від комутаторів до мультимедійних підсистем зв'язку IMS та бездротових мереж LTE, і має довгостроковий потенціал розвитку. У зв'язку з цим люди завжди вважали, що основними користувачами мереж наступного покоління будуть люди, а максимальна кількість користувачів таких мереж завжди буде обмежена чисельністю населення Землі.

За останні роки спостерігається значний прогрес у таких технологіях, як радіочастотна ідентифікація (RFID), бездротові сенсорні мережі (WSN), ближній польовий зв'язок (NFC) та міжмашинний (M2M) зв'язок, які в поєднанні з Інтернетом допомагають забезпечити зв'язок між великою кількістю різних технологічних пристроїв.

Загалом, Інтернет речей розуміється як група різноманітних пристроїв, датчиків та обладнання, які підключені до Інтернету через будь-які доступні канали зв'язку, взаємодіють один з одним за допомогою різних протоколів та отримують доступ до глобальної мережі за допомогою єдиного протоколу.

Загалом, Інтернет речей розуміється як група різноманітних пристроїв, датчиків та обладнання, які підключені до мережі через будь-які доступні канали

зв'язку, взаємодіють один з одним за допомогою різних протоколів та підключаються до глобальної мережі за допомогою єдиного протоколу.

В Інтернеті речей кожна річ має свій унікальний ідентифікатор, і разом ці речі утворюють континуум, який може взаємодіяти, створюючи тимчасові або постійні мережі. Таким чином, об'єкти можуть брати участь у процесі свого руху, обмінюватися інформацією про своє поточне географічне розташування та, завдяки вбудованому інтелекту, змінювати свої властивості та адаптуватися до навколишнього середовища. Деякі речі можуть виявляти та взаємодіяти з іншими речами, які до них підключені. Інтернет речей – це сукупність розумних пристроїв та людей, підключених через комунікаційні мережі. Разом вони можуть створювати широкий спектр систем, включаючи ті, що призначені для роботи в середовищах, незручних або неможливих для доступу людей.

Вважається, що перший у світі підключений продукт був створений Джоном Ромкі в 1990 році, коли він підключив свій тостер до Інтернету. Однак лише у 21 столітті, з швидким розвитком інформаційно-комунікаційних технологій, концепція Інтернету речей оформилася та була по-справжньому реалізована. Розвиток Інтернету речей можна проілюструвати блок-схемою, показаною на рисунку 1.1. Все почалося з необхідності оптимізації корпоративної логістики та систем управління ланцюгами поставок[4].

Друга хвиля інновацій була зумовлена необхідністю зниження витрат на спостереження, безпеку, транспорт тощо.

Третя причина – попит на послуги геолокації. Четверта хвиля буде зумовлена потребою людей дистанційно брати участь у діяльності, яка вимагає їхньої уваги, і крихітні вбудовані процесори зроблять це можливим. Наступним кроком буде створення майбутньої mesh-мережі, що складається з міток, датчиків, вимірювальних приладів та пристроїв керування.

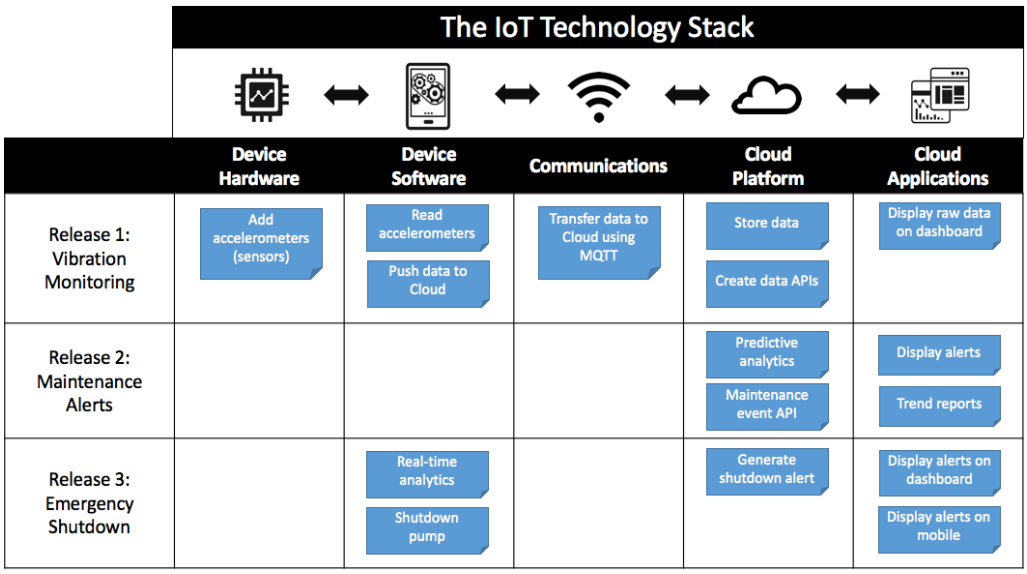


Рис. 1.1. Дорожня карта технології Інтернету речей

У міру зростання Інтернету речей все більше об'єктів будуть підключені до глобальної мережі, створюючи нові можливості для безпеки, аналітики та управління. Це відкриє нові широкі перспективи та сприятиме покращенню якості життя людей. Очікується, що в майбутньому «речі» стануть активними учасниками соціальних та інформаційних процесів. Вони взаємодіятимуть один з одним без втручання людини, обмінюватимуться інформацією про навколишнє середовище, реагуватимуть і впливатимуть на процеси, що відбуваються у світі навколо них [5].

Інтернет речей базується на трьох основних принципах. По-перше, повсюдна комунікаційна інфраструктура; по-друге, глобальна ідентифікація кожного об'єкта; і по-третє, здатність кожного об'єкта надсилати та отримувати дані через власну персональну мережу або мережу, до якої він підключений.

Найважливіші відмінності між Інтернетом речей та існуючим Інтернетом людей:

a) Зосередження уваги на речах, а не на людях;

b) Кількість підключених об'єктів значно збільшується;

c) Розмір об'єктів стає набагато меншим, а швидкість передачі даних зменшується;

d) Зосередження уваги на читанні повідомлення, а не на комунікації;

d) Необхідно створити нову інфраструктуру та альтернативні стандарти.

Концепція мережі наступного покоління (NGN) полягає в тому, що люди зможуть спілкуватися (безпосередньо або через комп'ютери) будь-де та будь-коли. Концепція Інтернету речей включає ще один напрямок - комунікацію будь-якого пристрою чи речі (Рисунок 1.2).

Рис. 1.2. Нові напрямки в комунікаціях, що приносить Інтернет речей

Концепцію та термінологію Інтернету речей (IoT) вперше представив Кевін Ештон, засновник дослідницької групи Auto-ID в Массачусетському технологічному інституті, у презентації 1999 року для керівників Procter & Gamble. У презентації обговорювалося, як широке впровадження RFID-міток змінює спосіб управління компаніями своїми ланцюгами поставок. Офіційне визначення Інтернету речей наведено в Рекомендації ITU-T Y.2060, в якій зазначено, що Інтернет речей – це глобальна інфраструктура для інформаційного суспільства, яка надає розширені послуги шляхом організації зв'язку між речами (фізичними чи віртуальними), на основі існуючих та нових сумісних інформаційно-комунікаційних технологій [2].

Під «речами» ми маємо на увазі фізичні об'єкти (фізичні речі) або об'єкти у віртуальному (інформаційному) світі (віртуальні речі, такі як мультимедійний контент або програми), які можна ідентифікувати та підключити через комунікаційні мережі. Окрім поняття «речі», ITU-T також використовує поняття

«обладнання», яке стосується обладнання з обов'язковими комунікаційними можливостями та додатковими можливостями, такими як виявлення, керування, збір, обробка та зберігання даних. Це означає, що ITU-T більше зосереджується на аспектах зв'язку та сумісності, ніж на програмах Інтернету речей.

Схема представлення фізичних об'єктів та віртуальних об'єктів показана на рис. 1.3. Як видно з рисунка, віртуальні речі можуть існувати без фізичного прояву, тоді як фізичні об'єкти/речі повинні відповідати принаймні одному віртуальному об'єкту. У цьому випадку домінуючу роль відіграють пристрої, які можуть збирати всіляку інформацію та поширювати її через комунікаційні мережі різними способами: через шлюзи, через мережу; без шлюзів, але через мережу; безпосередньо між ними. Рекомендація Y.2060 описує різні комбінації перелічених способів підключення. Це показує, що ITU-T передбачає використання різних мережевих технологій для реалізації Інтернету речей – глобальних мереж, локальних мереж, бездротових ad hoc мереж та mesh-мереж. Ці комунікаційні мережі передають дані, зібрані пристроями, до відповідних програмних додатків, а також передають команди від програмних додатків до пристроїв. [3]

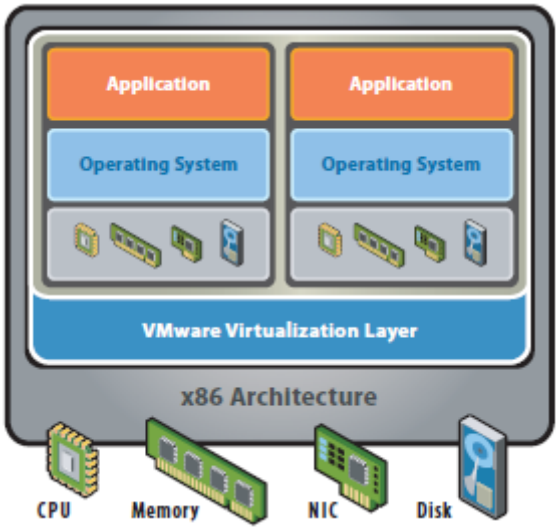


Рис. 1.3. Схематичне зображення фізичних та віртуальних речей

Варто зазначити, що Інтернет речей та пов’язані з ним пристрої можуть мати складні керуючі процесори для виконання обробки даних.

Як «система на кристалі», вона містить власну операційну систему, датчики/детектори навколишнього середовища та комунікаційний блок.

Необхідно розрізняти поняття «Інтернет речей» та «Інтернет речей». Інтернет речей – це будь-який пристрій, який має такі характеристики: він здатний підключатися до Інтернету та передавати або запитувати будь-які дані; він має певну адресу або ідентифікатор у глобальній мережі, через який може надаватися зворотний зв'язок; та він має інтерфейс для взаємодії з користувачами.

Концептуально Інтернет речей – це мережа наступного покоління, тому його архітектура дуже схожа на чотиришарову архітектуру NGN, яку ми знаємо. Інтернет речей складається з набору різних інформаційно-комунікаційних технологій, які дозволяють йому працювати, а його архітектура показує, як ці технології пов'язані одна з одною. Архітектура Інтернету речей складається з чотирьох функціональних рівнів, як описано нижче (Рисунок 1.4) [7].

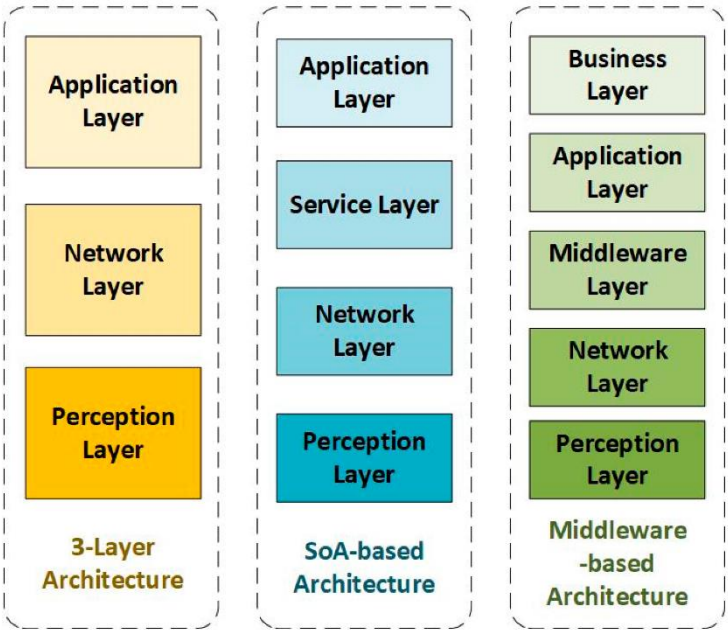


Рис. 1.4. Архітектура мережі Інтернету речей

Найнижчий рівень архітектури Інтернету речей складається з інтелектуальних об'єктів, які інтегрують датчики. Датчики з'єднують фізичний світ та віртуальний (цифровий) світ, забезпечуючи збір та обробку інформації в режимі реального часу. Мініатюризація призвела до зменшення фізичних розмірів апаратних датчиків, що дозволяє вбудовувати їх безпосередньо в

об'єкти фізичного світу. Різні типи датчиків використовуються для різних цілей, таких як вимірювання температури, тиску, швидкості, положення тощо. Датчики можуть мати невелику пам'ять, що дозволяє їм записувати багато вимірювань. Датчики можуть вимірювати фізичні параметри об'єкта/явища та перетворювати їх на сигнали, які може приймати відповідне обладнання. Залежно від їх використання, датчики можна розділити на датчики навколишнього середовища, датчики людини, датчики побутової техніки, датчики транспортних засобів тощо. Більшість датчиків потребують підключення до агрегатора датчиків (шлюзу), що може бути здійснено за допомогою локальної мережі (LAN), такої як Ethernet Wi-Fi, або персональної мережі (PAN), такої як ZigBee, Bluetooth та надширокосмуговий (UWB) бездротовий зв'язок. Для датчиків, які не потребують підключення до агрегатора, можна використовувати широкосмугові бездротові мережі, такі як GSM, GPRS та LTE, для забезпечення їх зв'язку із сервером/додатком. Датчики з низьким енергоспоживанням та низькою швидкістю передачі даних утворюють так звані бездротові сенсорні мережі (WSN). Бездротові сенсорні мережі (WSN) стають дедалі популярнішими, оскільки вони можуть вмістити більше датчиків, мати резервне живлення від батареї та охоплювати більші площі [11].

2. Шлюз та мережевий рівень. Величезні обсяги даних, що генеруються численними мікросенсорами на першому рівні Інтернету речей, вимагають надійної та високопродуктивної дротової або бездротової мережевої інфраструктури як середовища передачі. Існуючі комунікаційні мережі, що використовують різні протоколи, можуть бути використані для підтримки M2M-комунікацій та їх застосувань. Для реалізації широкого спектру послуг та застосувань в Інтернеті речей необхідно забезпечити сумісність кількох мереж, що використовують різні технології та протоколи доступу в гетерогенних конфігураціях. Ці мережі повинні забезпечувати необхідні значення якості передачі інформації, насамперед з точки зору затримки, пропускної здатності та безпеки. Цей рівень складається з конвергентної мережевої інфраструктури, створеної шляхом інтеграції гетерогенних мереж в єдину мережеву платформу.

Конвергентна мережева абстракція в Інтернеті речей дозволяє кільком користувачам незалежно спільно використовувати ресурси в одній мережі через відповідні шлюзи без шкоди для конфіденційності, безпеки та продуктивності.

3. Сервісний рівень. Сервісний рівень включає набір інформаційних сервісів, призначених для реалізації автоматизації технологій Інтернету речей та бізнес-операцій: підтримка операцій та бізнес-діяльності (OSS/BSS, система підтримки операцій/система підтримки бізнесу), аналіз та обробка різних типів інформації (статистика, аналіз даних та тексту, прогнозний аналіз підприємства тощо), зберігання даних, інформаційна безпека та управління бізнес-правилами (BementRM).

4. Прикладний рівень. Четвертий рівень архітектури Інтернету речей складається з різних типів додатків, орієнтованих на відповідні промислові сектори та сфери діяльності (енергетика, транспорт, торгівля, охорона здоров'я, освіта тощо). Додаток може бути «вертикальним», якщо він розроблений для певної галузі, або «горизонтальним», якщо його можна використовувати в кількох секторах економіки [3].

1.2. Методи передачі даних Інтернету речей

Одним з основних завдань організації Інтернету речей є забезпечення взаємодії:

- Інтернету речей,
- користувачів та мережевих речей,
- віддалених серверів та Інтернету речей.

Інтернет речей використовує широкий спектр комунікаційних мереж для передачі даних: від BAN (мереж на тілі) на відстані десятків сантиметрів від тіла людини до Всесвітньої мережі. Для зв'язку на близькій відстані використовуються такі технології, як RFID, NFC, Bluetooth та Wi-Fi.

Зв'язок на великій відстані базується на різних стільникових мережах (2G/3G/4G), бездротових широкосмугових мережах WiMAX, мережах позиціонування GPS/GLONASS тощо. Телекомунікаційні мережі, що використовуються Інтернетом речей, можна розділити на чотири категорії за їх покриттям (рис. 1.5):

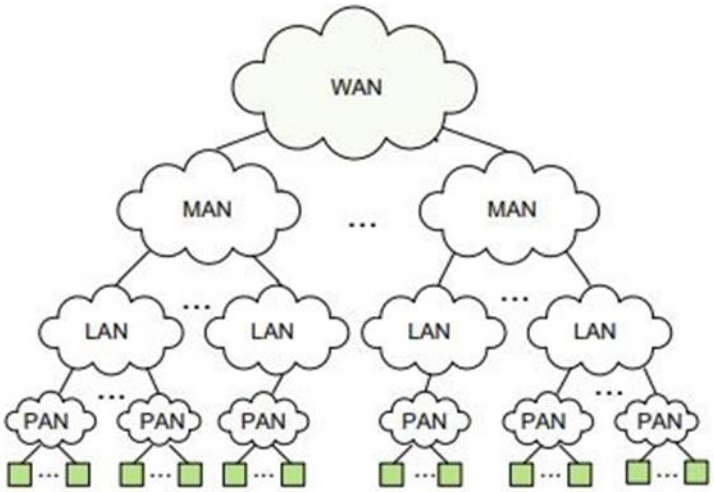


Рис. 1.5. Ієрархія мережевих технологій, що використовуються в Інтернеті речей

1. Персональна мережа (PAN) – мережа, побудована «навколо» окремої людини. Ці мережі розроблені для інтеграції всіх персональних пристроїв користувача. У контексті Інтернету речей ця мережа побудована «навколо» пристроїв.

2. Локальна мережа (LAN) – мережа, яка зазвичай охоплює відносно невелику площу або групу будівель. До локальних мереж також належать мережа контролерів CAN, промислова мережа, основною метою якої є об'єднання різних виконавчих механізмів та датчиків в межах одного підприємства в єдину мережу.

3. Метрополітенська мережа (MAN) – з'єднує окремих користувачів та регіональні мережі в межах міста. Вона більша за локальну мережу (LAN), але менша за глобальну мережу (WAN) та глобальні WAN (Wide Area Networks), які з'єднують користувачів Інтернету, розташованих за сотні або навіть тисячі кілометрів один від одного. Інтернет речей має мало конкретних вимог до технологій LAN, MAN та WAN, які добре описані в технічній літературі. Тому в

цьому розділі розглядаються лише стандарти та протоколи для мереж короткого та середнього радіусу дії, які широко використовуються в Інтернеті речей.

Усі технології передачі даних в Інтернеті речей можна розділити на дві категорії: дротові та бездротові[8], залежно від використовуваного середовища передачі.

Дротова технологія передачі даних в Інтернеті речей може використовувати металеві (мідні) кабелі зв'язку, дроти (технологія PLC - зв'язок по лініях електропередач) або оптоволоконні кабелі. Однак через складність фізичної реалізації ліній зв'язку рівень використання дротової технології в IoT-зв'язку нижчий, ніж у бездротових технологій.

В Інтернеті речей використовуються три типи бездротових мереж ближнього радіусу дії:

1. Бездротова персональна мережа (WPAN). Вони використовуються для підключення різноманітних пристроїв, включаючи комп'ютери, домашнє та офісне обладнання, комунікаційне обладнання тощо. Фізичний рівень та рівень каналу передачі даних регулюються стандартом IEEE 802.15.4. Діапазон WPAN коливається від кількох метрів до десятків сантиметрів. Цей тип мережі використовується як для з'єднання окремих пристроїв один з одним, так і для їх підключення до мереж вищого рівня, таких як глобальний Інтернет. Бездротові сенсорні мережі (WPAN) можуть бути розгорнуті з використанням різних мережевих технологій, таких як Bluetooth, ZigBee, 6LoWPAN тощо, які обговорюються далі в цьому розділі.

2. Бездротова сенсорна мережа (WSN). Розподілена самоорганізуюча мережа, що складається з кількох датчиків або виконавчих механізмів, з'єднаних між собою радіоканалами. Оскільки такі мережі здатні передавати інформацію від одного елемента до іншого, їх радіус дії може становити від кількох метрів до кількох кілометрів.

3. Крихітна мережа (TIN). Комп'ютерна мережа, розгорнута в невеликому офісі або приватному будинку. Їх часто називають домашніми мережами,

оскільки вони з'єднують домашні комп'ютери, побутову електроніку та системи сигналізації. Як правило, такі мережі побудовані на технології Wi-Fi.

Взаємодія між великою кількістю різних пристроїв в Інтернеті речей вимагає стандартизованих інтерфейсів, форматів даних та протоколів зв'язку. У таблиці 1.1 наведено деякі стандарти та протоколи Інтернету речей, їх робочі частоти, швидкості передачі даних, підтримку рівня OSI (Physical PHY, Media Access MAC, Network NWK, Transport TRP), а також реалізацію APS (Application Support Sublayer), підтримку ACL (Access Control List) та 128-бітних стандартів шифрування AES (Advanced Encryption Standard).

Таблиця 1.1. Порівняльний аналіз технологій Інтернету речей

Стандарт	**Частота, МГц**	**Швидкість, кбит/с**	**Рівні протоколу**						**Шифрування**
			PHY	MAC	NWK	TRP	APS	ACL	
IEEE	868/91	20/40/ 250	+	+	-	-	-	+	+
802.15.4	5/2 400								
ZigBee	2400	250	-	-	+	+	+	+	+
6LoWPAN	-	50-200	-	-	+	-	-	+	+
WirelessHART	2400	250	+	+	+	+	+	+	+
ISA100.11	2400	250	+	+	+	+	+	+	+
Z-Wave	865/91	9,6/40	+	+	+	-	+	-	-
Bluetooth	2400	1000	+	+	+	+	+	+	+
DECT ULE	1880-	1000	+	+	+	-	-	+	+

1.3. Технологія ZigBee в Інтернеті речей

Засновники технології ZigBee позиціонували її для систем моніторингу та управління, що передають невеликі обсяги даних, таких як контролери освітлення приміщень, термостати, кондиціонери, пульти дистанційного керування, бездротові комп'ютерні клавіатури та миші, детектори диму та вуглекислого газу, пристрої екстреного виклику для людей похилого віку та дітей, обладнання домашньої автоматизації тощо. У корпоративному секторі такими застосуваннями можуть бути складські системи, системи промислової автоматизації, різні датчики тощо [5]

Тому стандарт ZigBee переважно використовується як метод зв'язку між незалежними пристроями та пристроями управління. Це призводить до вимог до впровадженої технології:

- Підтримує мережі з сотнями функціональних пристроїв (можна підключити до 255 пристроїв);

- Забезпечує середню дальність мережі в реальних домашніх умовах близько 30 метрів;

- Легко встановлюється та використовується.

Для порівняння, Wi-Fi (IEEE 802.11b) підтримує 50 пристроїв без втрати продуктивності мережі, тоді як WirelessUSB та Bluetooth (головний конкурент Zigbee) підтримують 7 елементів на пікомережу.

З іншого боку, домашній Wi-Fi має радіус дії 100 метрів, тоді як WirelessUSB та Bluetooth мають радіус дії до 10 метрів. Тому нова технологія має чітке позиціонування на споживчому ринку – частково конкуруючи з вищезгаданими технологіями та повністю замінюючи аналогічні дротові та бездротові системи (LonWorks, HomePNA тощо) [9].

IEEE 802.15.4 допоможе нам зрозуміти, що таке ZigBee, як працює ця бездротова мережа, як вона «дихає», що насправді передається по повітрю, крім даних, як пристрої отримують доступ до мережі та інші тонкощі.

Архітектура мереж LR-WPAN зазвичай стандартна та дуже схожа на класичні комп’ютерні мережі. LR-WPAN складається з набору «будівельних блоків», шарів або ієрархій, які з’єднані між собою логічними зв’язками. Кожен шар відповідає за виконання певного набору функцій та надання послуг вищим шарам. Структура шарів IEEE 802.15.4 відповідає стандартній, широко використовуваній моделі взаємодії відкритих систем (OSI). Основним методом доступу до фізичного середовища, запропонованим цим стандартом, є випадковий доступ з виявленням несучої та запобіганням колізіям - CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). Тут також реалізовані додаткові функції, такі як виявлення енергії (ED) та індикатор якості з'єднання

(LQI). У діапазоні 2450 МГц для передачі доступно 16 каналів, у діапазоні 915 МГц - 10 каналів для передачі, та 1 канал для передачі в діапазоні 868 МГц.

Примітною особливістю мереж IEEE 802.15.4 є підтримка так званої структури "суперкадру". Формат суперкадру визначається координатором мережі. Нагадаємо, що координатор - це основний мережевий пристрій, який контролює всі потоки даних. Суперкадр починається з передачі спеціального кадру, який називається "мережевий маяк", який надсилається самим координатором. Мітки в основному використовуються для синхронізації та керування роботою всіх активних пристроїв у мережі. Після надсилання "мітки" координатор передає керування мережею та дозволяє пристроям "дізнатися", хто головний. Для цього в суперкадрі вказується спеціальний часовий інтервал – період, протягом якого пристрої конкурують за доступ до бездротового каналу (ContentionAccessPeriod), який поділяється на фіксовані часові інтервали – так звані часові слоти. Водночас, для застосувань, критично важливих до швидкості та пропускної здатності передачі даних, після періоду конкуренції може бути встановлений додатковий часовий період (ContentionFreePeriod), щоб забезпечити можливість надсилання або отримання екстрених повідомлень [9].

Традиційно розробники бездротових стандартів зосереджувалися на двох або трьох нижніх рівнях семирівневої моделі відкритих систем ISO. На рис. 1.6 показано архітектуру стандарту, показуючи знизу вгору фізичний рівень (PHY) для діапазонів 868 МГц (Європа) та 915 МГц (США), а також PHY для більш поширеного діапазону 2,4 ГГц. Вище цього знаходиться транспортний рівень, який визначає розділення радіосигналів під час доступу до мережевих пристроїв.

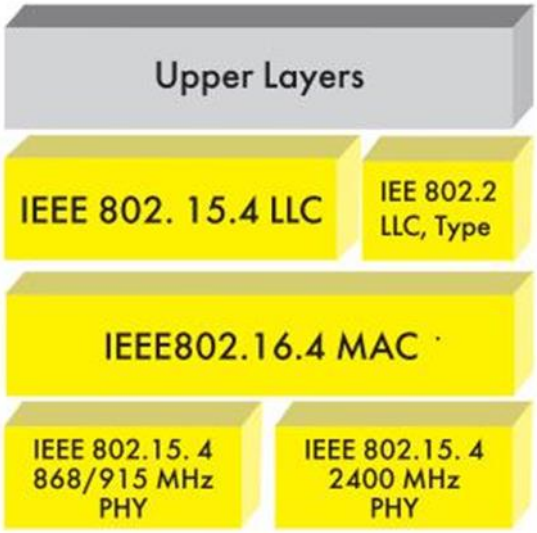


Рис. 1.6. Архітектура стандарту

Розподіл «сфери відповідальності» між розробниками технологій та споживачами показано на рисунку нижче (рисунок 1.7). Нижчі рівні визначені стандартами IEEE, а середні рівні повністю контролюються ZigBee Alliance (рисунок 1.7), але технологія використовується споживачами (клієнтами), які визначають споживчі властивості використовуваних пристроїв. Доступ до середовищ передачі даних за допомогою таких методів, як CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) - Множинний доступ

З функціями моніторингу несучої та запобігання колізіям. Цей тип доступу є спадщиною бездротового стандарту Ethernet. [7]

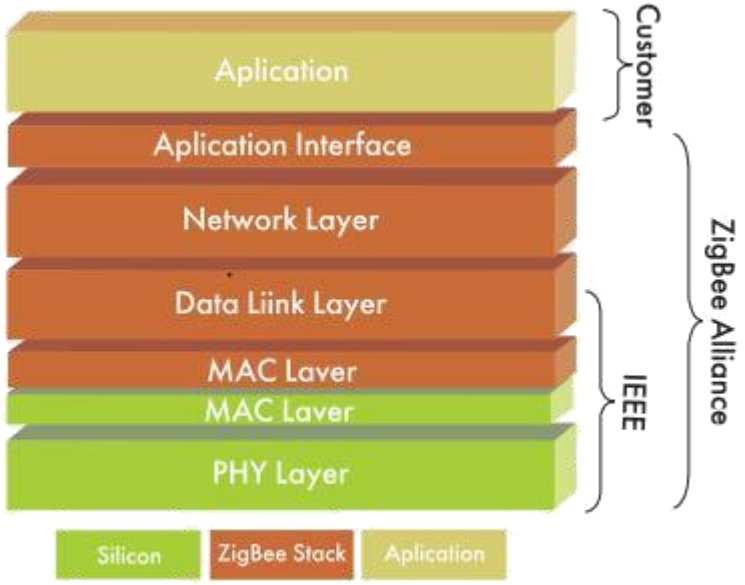


Рис. 1.7. Ієрархія семирівневої моделі

Структура пакета даних показана на рис. 1.8. Технічні параметри цієї технології змінюються залежно від діапазону частот.

1. У діапазоні 2,4 ГГц (глобально): - швидкість передачі повідомлень 250 кбіт/с;

- Технічна швидкість передачі даних 62,5 кбіт/с, кодування 4 Біти/символ;

2. У діапазоні 868 МГц (Європа) або 915 МГц (США): - Швидкість передачі повідомлень 20 кбіт/с;

- Швидкість передачі технічних даних 20 кбіт/с, кодування 1 біт/символ.

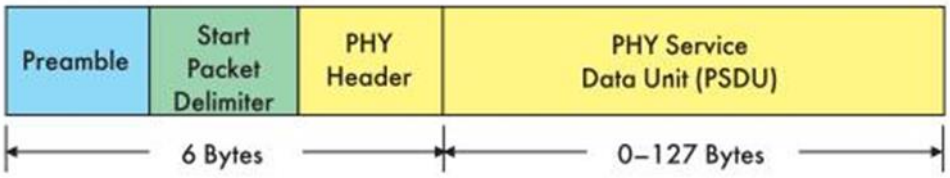


Рис. 1.8. Структура набору

Поля пакета (зліва направо): Преамбула (32 біти) використовується для синхронізації пакетів, прапор пакета (8 бітів) визначає один із трьох типів пакетів, що використовуються, заголовок (8 бітів) визначає довжину поля даних, а PSDU – це поле даних, яке може мати довжину від 0 до 127 байт.

Повідомляється про швидкість передачі даних до 40 кбіт/с.

У цьому діапазоні для всіх варіантів тип модуляції несучої однаковий – відносна фазова маніпуляція; для передачі використовуються неліцензовані частотні діапазони[3].

Огляд дев'яти команд, які дозволено передавати мережею, допоможе вам зрозуміти функціональність самої мережі ZigBee, а також обладнання, яке в ній працює. Отже, перерахуємо їх: • «Associationrequest» – запит на приєднання до існуючої мережі. Коли пристрій хоче приєднатися до мережі, він надсилає цей запит координатору. Запит містить інформацію про характеристики пристрою – чи може він виступати координатором мережі, тип пристрою, як він живиться, чи вимикає пристрій радіозв'язок у режимі «сну», чи підтримує він захист шифруванням, та чи потрібна пристрою 16-бітна чи 64-бітна адреса. Запит на підключення може бути надісланий лише пристроєм, який ще не підключений до мережі. [2]

- «Associationresponse» – відповідь координатора мережі на запит пристрою на приєднання до мережі. У цьому випадку координатор може: підключити пристрій до мережі та призначити адресу, повідомити про відсутність вільних слотів або заборонити доступ без пояснення причини.

- «Disconnection notification» – команда для розриву мережевого з'єднання. Його може надіслати координатор, і в цьому випадку він надає адресу пристрою, який потрібно виключити з мережі. Цю команду також може надіслати будь-який пристрій у мережі, і в цьому випадку він повідомляє координатора про свою адресу.

- "Datarequest" – це команда, що надсилається пристроєм для запиту даних у координатора.

- "PAN ID Conflict Notification" – це команда, яку пристрій надсилає мережевому координатору, коли виявляє конфлікт мережевого ідентифікатора.

- "Disconnect Notification" – це команда, що надсилається, коли пристрій, підключений до мережі, втрачає синхронізацію з координатором.

- Beacon Request – це команда, що надсилається пристроєм для виявлення всіх мережевих координаторів у межах його робочого діапазону.

- "Coordinatorrelaignment" – це команда ресинхронізації мережі, що надсилається координатором у відповідь на команду Orphannotification або зміну певних мережевих атрибутів. У першому випадку команда надсилається на певний пристрій, який має проблему синхронізації; у другому випадку команда розсилки надсилається на всі доступні пристрої. -

- Запит GTS – це команда, яка використовується для керування гарантованим часовим слотом передачі даних, виділеним певному пристрою в кадрі токена. Запит GTS дозволяє пристрою запитувати призначення таких слотів та звільняти вже призначені слоти. Щоб часові слоти призначалися лише пристроям з короткими адресами, у запиті вказується кількість необхідних або звільнених часових слотів, напрямок передачі даних (лише отримання або лише передача пристрою, що запитує) та 1 біт – сам запит виділити або звільнити вказаний часовий слот.

Розглядаючи команди, що виконуються в мережі ZigBee, варто зазначити такі факти. Пристрої з обмеженими можливостями можуть не підтримувати більшість із них. Також типово, що специфікації описують ці команди по-різному. Деякі з них є «необов’язковими», а інші можуть бути «обов’язковими». Незрозуміло, яка різниця між цими двома випадками, але дуже ймовірно, що це один і той самий випадок.

Надійність. Повернемося до функціональності IEEE 802.15.4. Ви пам’ятаєте, що однією з помітних особливостей бездротових мереж, побудованих за цим стандартом, є висока надійність передачі даних. Тепер нам потрібно з’ясувати, які механізми використовуються на рівнях PHY та MAC для досягнення цього.

LR-WPAN використовує різні механізми для забезпечення надійності та автентичності переданих повідомлень. Ці методи включають використання механізму передачі CSMA-CA, кадрів підтвердження та кадрів перевірки даних. Давайте розглянемо це детальніше.

IEEE 802.15.4 використовує два типи доступу до каналу залежно від конфігурації мережі. У мережах, які не використовують кадри "токенів" (мережі без маяків), і де доступ до каналу є випадковим, використовується механізм, який називається "механізм безслотового доступу до каналу CSMA-CA". Щоразу, коли пристрою потрібно передати кадр даних або команду MAC, він повинен спочатку зачекати певний час (кількість часу вибирається випадковим чином). Якщо канал вільний, пристрій передає дані. Якщо канал все ще зайнятий після випадкової затримки, пристрій повинен зачекати ще один випадковий час, перш ніж спробувати знову отримати доступ до каналу [4].

У мережі з тегованими кадрами використовується безслотовий механізм CSMA-CA для очікування передачі протягом фіксованого інтервалу часу одразу після тегованого кадру. Щоразу, коли пристрій хоче передавати протягом періоду конкуренції, він повинен спочатку визначити межі найближчого слота сну.

І випадковим чином підрахувати кількість однакових слотів. Якщо канал зайнятий після цієї паузи, пристрій повинен зачекати ще одну випадкову кількість фіксованих інтервалів часу, перш ніж спробувати знову отримати доступ до каналу. Якщо канал неактивний, пристрій може негайно розпочати передачу з краю найближчого слота сну.

Споживання енергії. Як згадувалося вище, однією з головних переваг стандарту ZigBee є його орієнтація на низьке енергоспоживання бездротових пристроїв. Не випадково цей важливий параметр згадується одним із перших у рекламних та промоційних брошурах. Насправді ж все зазвичай складніше. Проблема полягає в тому, що стандарт IEEE 802.15.4, на якому базується ZigBee, мало що говорить про низьке енергоспоживання. Наприклад, там написано: В принципі, цей стандарт застосовний до середовищ з обмеженим електропостачанням. Однак фізична реалізація стандарту вимагає подальших досліджень у цьому напрямку, що виходить за рамки IEEE 802.15.4. Водночас розробники також надають загальні рекомендації щодо зниження енергоспоживання пристрою там, де це дійсно необхідно. В обладнанні, яке використовує батареї або акумулятори як джерело живлення, завжди рекомендується циклічний режим роботи. Такі пристрої повинні перебувати в режимі "сну" більшу частину часу. Крім того, необхідно також регулярно відкривати радіоканал і прослуховувати радіо, щоб повідомлення можна було надсилати в будь-який час. Цей простий, але гнучкий механізм дозволяє розробникам програмних застосунків підтримувати тонкий баланс між енергозбереженням та затримкою повідомлень[6].

Безпека. Ще одним важливим параметром, що характеризує будь-яку мережу, особливо бездротову, є безпека переданих даних та їх захист від несанкціонованого доступу. У знайомих нам локальних дротових мережах ця проблема зазвичай не вирішується на апаратному рівні; безпека переданих даних гарантується сервісами та функціями на вищому програмному рівні.

Розробники IEEE 802.15.4 могли б зробити те саме, але вони все одно включили базовий набір функцій для забезпечення базового рівня безпеки на

рівні MAC. Базові послуги в цій області включають підтримку списків контролю доступу (ACL) та шифрування переданих даних.

Можливість виконання базових операцій безпеки не є обов'язковою, але розробники наполегливо рекомендують використовувати ці функції послідовно на всіх пристроях.

Згідно з технологією ZigBee, бездротова мережа передачі даних включає два типи пристроїв: повнофункціональні пристрої (FFD) та пристрої з обмеженими функціями (RFD).

Перший тип пристроїв забезпечує розширений функціонал для побудови топології мережі та може виступати в ролі координатора мережі (головної станції радіомережі) та обмінюватися повідомленнями з будь-якою іншою станцією в мережі. Другий тип обладнання може працювати лише в мережі типу "зірка", не може взяти на себе функцію координації роботи мережі обміну даними та має відносно просту конструкцію. Останньою характеристикою є нерівні можливості пристроїв, що працюють у мережі, що спочатку було закладено в ідеологію технологій та дозволяло їм забезпечувати надзвичайно низьке енергоспоживання. Хоча характеристики споживання енергії Bluetooth-пристроїв подібні до характеристик мобільних телефонів, які потребують періодичного підзаряджання, тут основна увага приділяється довгостроковому використанню одноразових джерел живлення (батарейок типу AA) для живлення кількох користувацьких пристроїв та домашньої мережі (тобто координатора) [7]. Параметри часу алгоритмів роботи мережі кожної технології також суттєво відрізняються: для виходу Bluetooth-пристрою з режиму сну потрібно близько 3 секунд, тоді як ZigBee – 15 мілісекунд; час доступу до контексту пристрою становить 15 мілісекунд та 2 мілісекунди відповідно; і навіть час, необхідний для «реєстрації» нового елемента в мережі, сильно варіюється: Bluetooth – понад 3 секунди, тоді як ZigBee – майже 303 секунди. Однією з головних переваг цієї технології є її здатність забезпечувати надзвичайно тривалі періоди автономного живлення; очікується, що для автономної роботи пристрою протягом кількох місяців знадобляться лише два-три пальці. Фактично, ці дані підкреслюють, що

технології, що порівнюються, орієнтовані на різні сфери застосування і тому взагалі не є порівнянними.

На рис. 1.9 показано структуру мережі типу «зірка». Завдання адміністратора мережі:

- Передача мережевих токенів;
- Об'єднання користувацьких пристроїв в одну мережу;
- Керування користувацьким обладнанням;
- Зберігання інформації про стан мережі;
- Організація передачі даних між сусідніми елементами мережі;
- Отримання електроенергії з мережі;
- Завжди в режимі прийому.

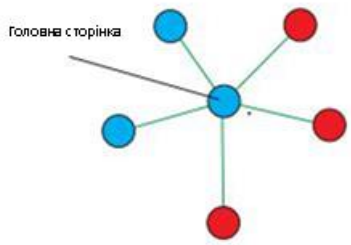


Рис. 1.9. Структура мережі типу «зірка»

Центр є станцією першого рівня і є головною станцією мережі. Обидва типи станцій є підлеглими та підключеними до неї.

У свою чергу, підлегла мережа:

- отримує та передає дані відповідно до виконаних запитів;
- визначає, чи потрібно передавати якісь дані;
- Запитує необхідну інформацію у координатора мережі, якщо це необхідно;
- Зазвичай живиться від окремого акумулятора;
- Може тривалий час підтримувати режим сну.

Перший тип сайту також може утворювати однорідну структуру, як показано на рисунку 1.10[7].

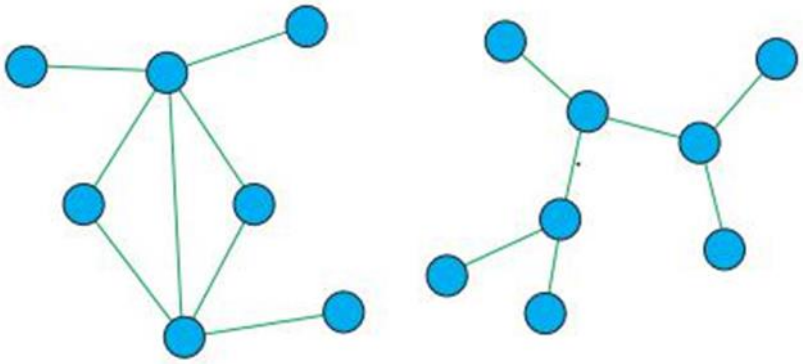


Рис. 1.10. Структура однорідної мережі

Зрештою, як і у випадку з Bluetooth, технологія дозволяє створювати змішані структури (рис. 1.11).

Залежно від типу мережевої структури змінюється і адресація її елементів. Використовуються такі методи адресації: мережа + ідентифікатор пристрою (зірчаста структура), ідентифікатор джерела/призначення (плоска структура), дерево кластерів джерела/призначення + ідентифікатор пристрою (гібридна структура). Алгоритм процесу передачі даних оптимізований для типу вхідного трафіку та може мати такі часові параметри:

- Передача даних (датчики, телеметрія) у різних напрямках з рівними інтервалами;

- Передача даних у різних напрямках з випадковими часовими інтервалами (керування освітленням, жалюзі);

- Одностороння випадкова передача даних з великими інтервалами (керується мишею або клавіатурою ПК).

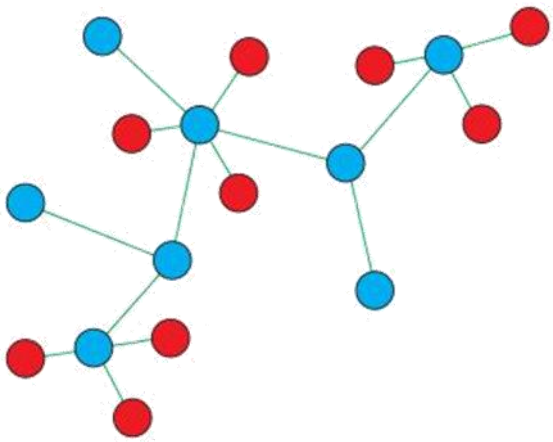


Рис. 1.11. Змішана структура

Протокол ZigBee визначає роботу сенсорних мереж. Ці пристрої утворюють ієрархічну мережу, яка може включати координатори, маршрутизатори та кінцеві пристрої. Коренем мережі є координатор ZigBee. Маршрути можуть враховувати ієрархії та оптимізувати потік інформації. Координатор ZigBee визначає мережу та встановлює для неї оптимальні параметри. Маршрутизатори ZigBee підключаються до Інтернету через координатор ZigBee або інші маршрутизатори, підключені до Інтернету. Кінцеві пристрої можуть підключатися до будь-якого маршрутизатора ZigBee або координатора ZigBee. За замовчуванням трафік повідомлень розподіляється між гілками ієрархії. Якщо маршрутизатори мають відповідні можливості, вони можуть визначити найкращий маршрут до заданої точки та зберегти його в таблиці маршрутизації для подальшого використання [8].

1.4. Висновок до розділу 1

Для розробників додатків ZigBee існує програмне забезпечення Z-Stack. Програмне забезпечення надає стек протоколів від транспортного рівня до рівня додатків та дозволяє налаштувати роботу бездротової системи та її окремих компонентів за допомогою профілів пристроїв. Пакет Z-Stack дозволяє організовувати мережі з різними топологіями (точка-точка, зірка, кластер-дерево, багатоблочні мережі). Програмний пакет також забезпечує сумісність з іншими сертифікованими пристроями ZigBee та надає підтримку та оновлення для придбаного програмного забезпечення. Z-Stack постачається з повним комплектом документації (посібник користувача, нотатки розробника тощо).

2. МОДЕЛІ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ ПРИ МУЛЬТИМОДАЛЬНОМУ РОЗПОДІЛІ ВУЗЛІВ

2.1. Архітектура мережі Інтернету речей

Послуги M2M можуть надаватися та керуватися ними за допомогою виділених мереж машина-до-машини (M2M), побудованих на існуючій мережевій інфраструктурі LTE постачальників та операторів послуг M2M. Сучасні мобільні мережі були створені для вирішення проблеми мобільності та надання послуг голосового зв'язку, SMS, MMS, мультимедійних повідомлень через інтерфейси «людина-людина» (H2H) або «сервер-людина» (завантаження даних додатків/потокове аудіо/відео). Тому технологія та архітектура мереж мобільного бездротового зв'язку, побудованих за принципом H2H, не підходять для послуг M2M, що спонукає людей наполегливо працювати над створенням нової інфраструктури комунікаційної мережі для послуг M2M та пов'язаних з ними додатків. Мережа M2M - це мережа, яка з'єднує кінцеві пристрої, що працюють без втручання людини, або з обмеженим втручанням людини, або лише з обмеженим втручанням людини з боку кінцевого користувача [3-4]. Варто зазначити, що окремі особи як кінцеві користувачі не є типовими ініціаторами входу в мережу M2M, а є лише епізодичними або одноразовими споживачами результатів мережі M2M. Головною особливістю та відмінністю мережі M2M порівняно з мобільною мережею є те, що трафік термінальних пристроїв відносно невеликий, але кількість термінальних пристроїв у мережі дуже велика, на порядок більша за кількість мобільних користувачів, і їх необхідно об'єднати в єдину мережу. Архітектура мережі M2M. Основні елементи архітектури мережі M2M поділяються на три домени: домен пристроїв M2M (капілярний мережевий домен); мережевий домен (основна мережа M2M) та прикладний домен [5]. Окрім вищезазначених мережевих доменів, мережа M2M також включатиме відповідні мережі доступу та транспортні мережі. Ці мережеві домени побудовані на мережі 3GPP NGN. Обладнання M2M: реалізує швидке розгортання та використання послуг M2M та функцій доменної мережі. Пристрої M2M можуть бути підключені до мережі доступу безпосередньо або

через локальну мережу M2M та шлюз M2M. Локальна мережа M2M забезпечує з'єднання між пристроями M2M та шлюзом M2M. Наприклад: технології PAN, такі як IEEE 802.15, SRD, UWB, Zigbee, Bluetooth тощо, або технології LAN, такі як PLC, M-BUS, Wireless M-BUS тощо. Шлюз M2M: пристрій, що забезпечує гарантовану сумісність та зв'язок для пристроїв M2M між мережами та доменами застосувань. Шлюзи M2M можуть використовуватися для різних застосувань пристроїв M2M. Функціонально шлюз M2M може бути поєднаний з пристроєм або набором мереж доступу M2M в одному модулі: мережа доступу - це мережа, яка дозволяє домену пристроїв M2M взаємодіяти з ядром мережі M2M (базовою мережею). Функціональність мереж доступу M2M базується на можливостях існуючих мереж доступу (xDSL, HFC, PLC, VSAT, GERAN, UTRAN, LTE, W-LAN та WiMAX) та дозволяє розширити спектр послуг та їх функціональність. Транспортна мережа: мережа, що забезпечує передачу даних між доменом мережі та доменом застосування. Функціональність транспортної мережі в мережі M2M базується на можливостях існуючої транспортної мережі та, подібно до мережі доступу, дозволяє розширити перелік послуг M2M та їх можливості. Базова мережа M2M: складається з базової мережі та її бізнес-функцій і можливостей. Базова мережа M2M: забезпечує IP-з'єднання, послуги управління мережею, мережеву сумісність, роумінг та безпеку для елементів мережі M2M. Функції базової мережі M2M базуються на відповідних функціях існуючої базової мережі 3GPP CN (таких як GPRS, EPC та ETSI TISPAN CN)[6]. Модуль функцій обслуговування M2M: реалізований базовою мережею M2M, який забезпечує функції для реалізації інтеграції різних додатків. Вони взаємодіють на основі відкритого інтерфейсу мережі M2M. Окрім власних функцій, мережа M2M також може використовувати функції базових мереж 3GPP та TISPAN. Ці модулі також надають можливість спрощення та оптимізації використовуваних додатків та послуг M2M. Основні функціональні можливості (бізнес-можливості) базової мережі M2M реалізуються відповідними функціональними модулями мережі M2M, включаючи: – Управління підтримкою застосунків (xAE); – Мережева сумісність – Універсальний зв'язок

(xGC); – Забезпечення доступності пристроїв/шлюзів, адресації та зберігання даних – Сховище доступності, адресації та зв'язку (xRAR) (xRx);

– Історія та зберігання даних – Історія та зберігання даних (xHDR); – Керування запитами – Управління транзакціями (xTM); – Управління заробітною платою – Брокер із заробітної плати (xCB); – Ризик оператора (xTOE); – Проксі-сервер довіреного інтернет-протоколу (xIP). Інтерфейс основної мережі M2M. Інтерфейси основної мережі M2M були стандартизовані та перелічені в TS 102 921[6]. Під час процесу розробки, щоб забезпечити еквівалентність та повноту стандартизації інтерфейсів, точки з'єднання елементів мережі M2M були визначені, головним чином враховуючи три аспекти, а саме:

- Визначення термінів протоколу/інтерфейсу прикладного програмування (API); - Визначення ресурсів та підресурсів мережі M2M; - Сумісність використовуваних протоколів, включаючи визначення ключових протоколів інфраструктури. Основні функції базової мережі M2M, побудованої на платформі IMS, включають [7-8]: реєстрацію, автентифікацію, авторизацію, зберігання бази даних користувачів мережі, управління сеансами, управління мережевими політиками, обробку трансляції адрес мережі NAT тощо. Враховуючи функції базової мережі M2M, які не повністю охоплюються платформою IMS, функції IMS можуть бути використані для доповнення деяких бізнес-функцій базової мережі M2M таких як функції безпеки NSEC, доступність елементів мережі NRAR для досягнення управління мережею M2M. Відповідно до принципів побудови функціональної архітектури мережі M2M, інтерфейс повинен відповідати наступним вимогам:

- Бути застосовним до широкого спектру мережевих технологій та не обмежувати свою застосовність при використанні в інших мережах;

- Залишатися незмінним для всіх областей застосування мережі M2M та бути незалежним від використовуваних програм M2M та мереж доступу.

Інтерфейси мережі M2M mIa, dIa та mId: виходячи з принципу відкритих інтерфейсів, вони забезпечують взаємодію між доменом застосунків та базовою мережею M2M, рівнем застосунків та функціональним рівнем домену пристроїв

M2M, а також пристроєм M2M та шлюзом M2M. На рис. 2.1 [7] показано типовий інтерфейс точок підключення елементів мережі M2M.

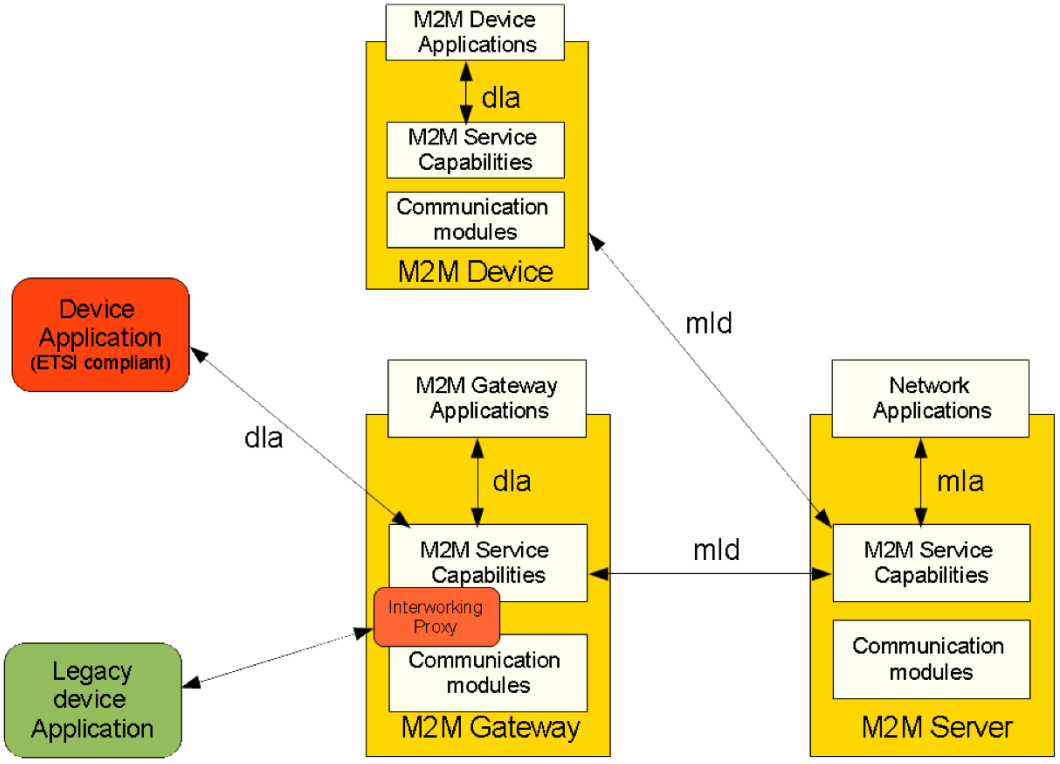


Рис. 2.1. Інтерфейси та точки інтерфейсу в мережах типу M2M

Інтерфейс mIa мережі M2M забезпечує взаємодію між застосунками M2M та функціональними модулями базової мережі M2M або домену застосунків.

Інтерфейс мережі M2M dIa забезпечує взаємодію між застосунками M2M, що працюють на пристрої M2M, та функціональними модулями пристрою M2M або шлюзу M2M, та доступ до них, а також забезпечує взаємодію між застосунками M2M, що працюють на шлюзі M2M, та застосунками на пристрої M2M, та доступ до функціональних модулів шлюзу M2M.

Мережевий інтерфейс M2M mId забезпечує взаємодію між пристроєм M2M або шлюзом M2M та основними функціональними модулями M2M у мережевому та прикладному доменах. Інтерфейс mId використовує базове мережеве розширення як базовий рівень.

Інтерфейс, який використовує платформу IMS для взаємодії з базовою мережею M2M. Підсистема мультимедійних послуг IMS має всі функціональні можливості базової мережі та дозволяє реалізувати сервісні функції. У цьому томі деякі основні функції мережевих послуг M2M (такі як функції безпеки

NSEC, функції досяжності мережевих елементів NRAR тощо) можуть бути додані до функцій IMS для забезпечення управління мережею M2M [9].

Взаємодія між основними функціональними модулями базової мережі M2M, платформою IMS, мережевими інтерфейсами M2M (mla, mld), внутрішніми інтерфейсами базової мережі M2M (ISC, Gm) та обладнанням шлюзу M2M/M2M відповідного постачальника послуг M2M показана на рис. 2.2.

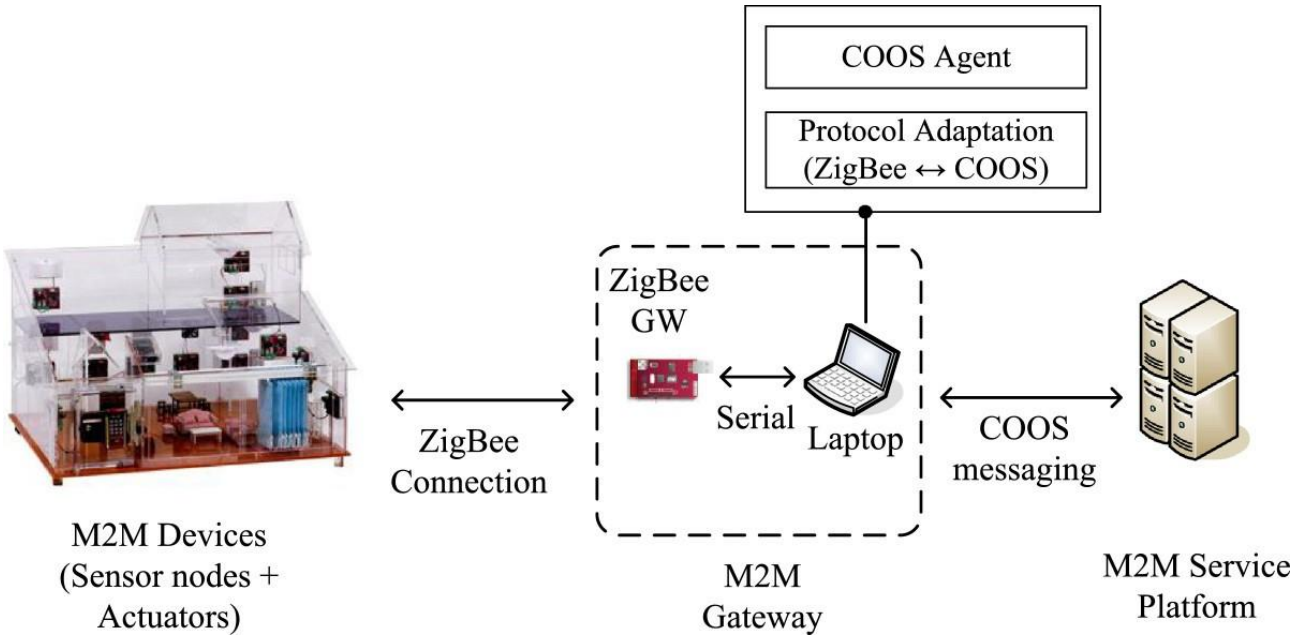


Рис. 2.2. Взаємодія між основними функціональними модулями базової мережі M2M

Інтерфейс ISC базової мережі M2M забезпечує обмін даними та підключення до серверів додатків, доступ до послуг M2M, а також доступ до інформації та використання функцій базової мережі IMS.

Інтерфейс Gm мережі M2M відповідає за автентифікацію та авторизацію різних додатків пристроїв M2M та мережевих додатків, а також реалізує багато функцій базової мережі (SC) M2M. Він також підключається до базової мережі IMS через інтерфейс ISC та взаємодіє з додатками пристроїв M2M через модуль NGC. Обмін інформацією між базовою мережею SC M2M та мережевими додатками здійснюється через модуль NAE[8].

Варіанти взаємодії пристроїв M2M включають взаємодію з використанням базової мережі M2M та шлюзу M2M, а також взаємодію без базової мережі M2M та шлюзу M2M, як показано на рисунках 2.3a та 2.3b.

У першому випадку обладнання користувача M2M також є точкою взаємодії інтерфейсу mId домену пристроїв M2M, який з'єднує пристрій M2M/шлюз M2M та основну мережу M2M.

Пристрої M2M взаємодіють через Інтернет; b – Пряма взаємодія між пристроями M2M.

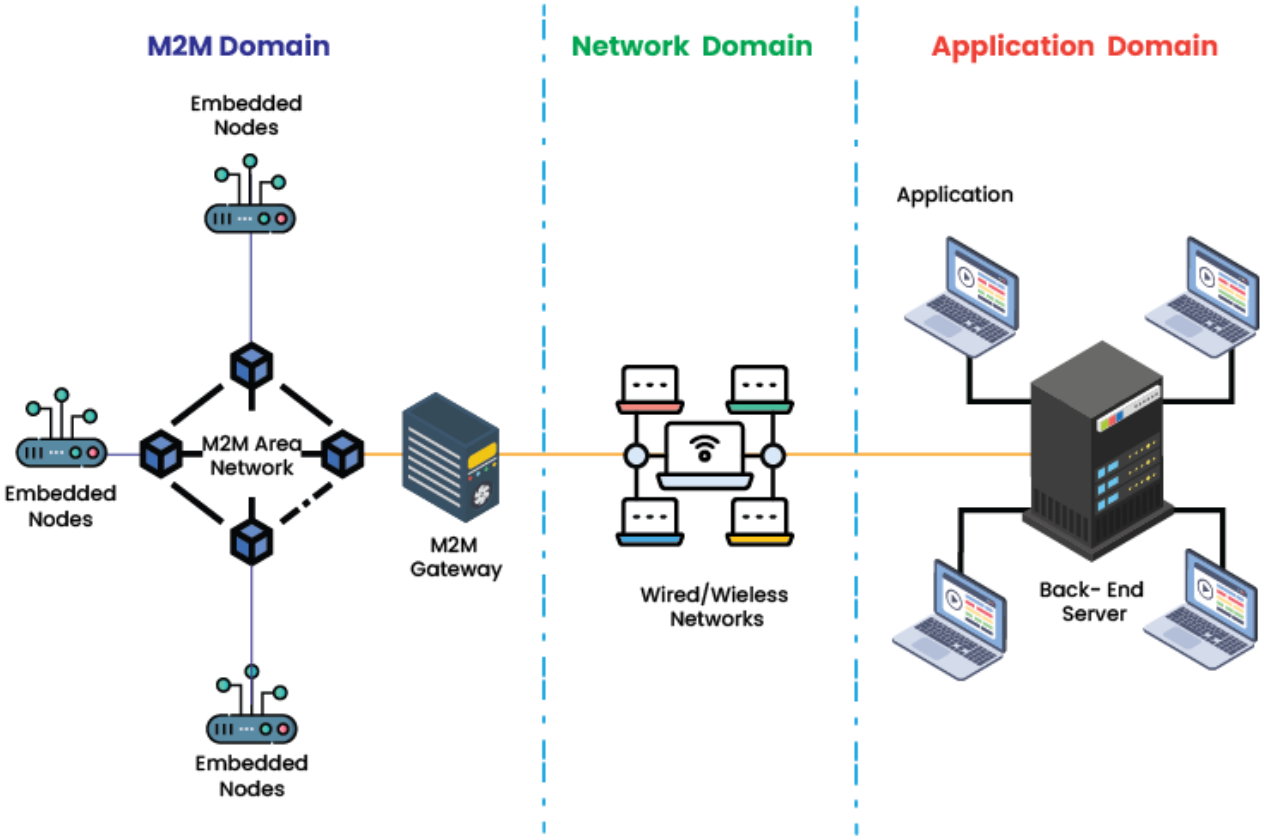


Рис. 2.3. Варіанти взаємодії між пристроями M2M

У другому випадку обладнання користувача M2M також є точкою взаємодії між додатками домену пристроїв M2M та функціональними модулями, які локально підтримують основні функції мережі M2M. У цьому випадку інтерфейс mA також використовується для взаємодії з локальною мережею пристроїв M2M [5].

2.2. Платформа мультимедійних Інтернет-сервісів та її функціональні елементи

IMS (IP Multimedia Subsystem) – це базова підсистема для реалізації мультимедійних IP-сервісів у мережах LTE. Він відповідає за керування та синхронізацію передачі пакетів даних користувача (голосу, відео, аудіо та SMS), резервування мережевих ресурсів, маршрутизацію IP-пакетів у режимі реального часу та підтримку інтерфейсів із серверами додатків, системами управління операторами та виставлення рахунків [2,9-14]. Згідно з планом проекту, IMS виконуватиме такі функції:

- Реалізація маршрутизації та адресації пакетів між UE та сервером додатків, UE та сервером онлайн-статусу на основі протоколу SIP (наразі) підсистема IMS;
- Аутентифікація та авторизація користувачів підсистеми IMS;
- Якість обслуговування (QoS);
- Стиснення SIP-повідомлень для оптимізації потоку сигналів;
- Підтримка режиму реєстрації SIP та угоди про сеанс обміну даними;
- Підготовка звітів для систем ціноутворення.

Підсистема IMS надає користувачам LTE переважно голосові повідомлення, короткі повідомлення (SMS), мультимедіа (MMS) та миттєві повідомлення (IM), забезпечуючи при цьому сумісність LTE з іншими мережами: мережею наземного мобільного зв'язку загального користування (PLMN), телефонною мережею загального користування (PSTN), мережею передачі даних загального користування (PDN) та VoIP. Підсистема IMS використовується для забезпечення безперервності голосових послуг.

Технологія SRVCC[6].

Основна підсистема IMS включає такі основні функціональні елементи:

AS (сервер додатків) - сервер додатків (наприклад, SIP);

Сервер додатків (OSA або CAMEL IM-SSF сервер додатків) містить логіку обробки сигналів та надає послуги кінцевому користувачеві;

HSS (сервер домашнього користувача) - сервер бази даних домашніх користувачів. Це набір HLR/AuC, включаючи AS, MME, S-CSCF, I-;

Панель керування SORM (панель керування SORM);

Панель керування SORM (панель керування SORM);

SLF (Subscription-Defined Function) – це сервер, який визначає базу даних HSS, де зберігаються профілі користувачів. Сервер SLF надає інформацію про адресу обслуговуючого HSS до S-CSCF та I-CSCF і використовується, коли в підсистемі IMS реалізовано кілька HSS.

LRF (Location Reference Function) – це сервер;

Визначає місцезнаходження користувача на основі загальної інформації;

Оновлює місцезнаходження мобільного терміналу (оновлює інформацію про місцезнаходження);

P-CSCF (Proxy Call Session Control Function) – це проксі-сервер і перший мережевий елемент, який встановлює з'єднання між терміналом користувача UE та підсистемою IMS;

- S-CSCF (Service Call Session Control Function) – це центральний сервісний сервер підсистеми IMS, який забезпечує автентифікацію та авторизацію користувачів, керування сеансами та керування статусом користувачів у мережі;

- I-CSCF (Interactive Call Session Control Function)

Сервер опитування є граничним елементом підсистеми IMS.

Зовнішня підсистема IMS встановлює з нею з'єднання.

- E-CSCF (Emergency Call Session Control Function) – це сервер підсистеми IMS, який надає послуги кінцевим користувачам під час виклику екстреної служби 112 (911);

- EATF (Emergency Access Transfer Function) – це сервер підсистеми IMS, який надає кінцевим користувачам можливість викликати екстрені служби;

- ATCF (Access Control Function) – це контролер, забезпечує реалізацію функцій SRVCC;

- MGCF (Media Gateway Management Function) – це контролер

Медіашлюз IMS-MGW використовує протокол H.248/MEGACO для управління ресурсами медіашлюзу;

- IMS-MGW (Media Gateway Function) – Медіашлюз,

Забезпечує передачу голосового трафіку (площина користувача) через протокол реального часу RTP, перекодування голосового сигналу (зміна голосового кодека);

- BGCF (Border Control Function) – Контролер,

Забезпечує вибір мережі PLMN (домен CS) та PSTN, а також маршрутизацію сигнальних повідомлень SIP від S-CSCF до мережі реєстрації викликаного користувача;

- SGW (Функція шлюзу сигналу) – Шлюз сигналу,

Це гранична точка, де відбувається обмін сигнальною інформацією між підсистемою IMS та мережами PLMN та PSTN. Шлюз сигналу SGW реалізує контроль безпеки та перетворення між повідомленнями SIGTRAN SCTP/IP та повідомленнями SS7 MTP.

MRB (Брокер медіа-ресурсів) – Сервер керування ресурсами на основі налаштовуваних правил, стандартів QoS та угод про рівень обслуговування;

- MRFP (Процесор функцій мультимедіа-ресурсів) – процесор мультимедійних ресурсів, який надає користувачам (відтворює) аудіо- та відеоконтент;

- MRFC (Контролер функцій мультимедіа-ресурсів) – контролер, забезпечує керування процесором мультимедійних ресурсів MRFP відповідно до команд від серверів AS та S-CSCF, генеруючи записи CDR;

- IBCF (Функція контролю межі міжмережевої взаємодії) – контролер межі сигналу, який забезпечує обмін сигналами SIP/SDP між підсистемою IMS та зовнішньою мережею VoIP та керує ресурсами медіа-шлюзу TrGW;

- TrGW (Транзитний шлюз) – транзитний шлюз, що забезпечує передачу (медіаплощина) та транскодування мультимедійного трафіку з використанням протоколу реального часу RTP. Функціональний модуль ядра мережі M2M на базі платформи IMS[10].

Підсистема мультимедійних сервісів IMS Core має всі функції ядра мережі M2M та може реалізовувати характеристики сервісних функцій мережі M2M під час взаємодії з програмами пристроїв M2M та програмами ядра мережі, що отримують доступ до мережі.

Основні функції базової мережі M2M, побудованої на платформі IMS, включають реєстрацію, автентифікацію, авторизацію, зберігання бази даних користувачів мережі, управління сеансами, управління мережевими політиками, обробку трансляції адрес мережі NAT тощо. Враховуючи функції базової мережі M2M, які не повністю охоплюються платформою IMS, функції IMS можуть бути використані для доповнення деяких бізнес-функцій базової мережі M2M (таких як функції безпеки NSEC, досяжність елементів мережі NRAR тощо) для досягнення управління мережею M2M.

Сервісні функції та можливості базової мережі M2M реалізовані у вигляді відповідних функціональних модулів, які визначені стандартом ETSI для функціональної архітектури мережі M2M. В базовій мережі M2M платформи IMS найважливішими функціональними модулями, які необхідно реалізувати, є NAE, NGC, NRAR та NSEC.

Модуль NAE (Network Application Enablement) забезпечує взаємодію з M2M-додатками на рівні мережевого домену та домену M2M-додатків, а також:

- Відкритий доступ до функціональних модулів для M2M-додатків базової мережі M2MCore через інтерфейс MLA;

- Забезпечити конфіденційність топології функціонального модуля SC та адреси NAE, та розкрити лише інформацію, необхідну для роботи M2M-додатків;

- Надати M2M-додаткам функціональний модуль SC;

- Забезпечити автентифікацію та авторизацію M2M-додатків через модуль безпеки та перевірити наявність угоди з постачальником M2M-додатків та рівень його взаємодії з функціональним модулем SC;

- Перевірити доступність функціонального модуля SC через інтерфейс MLA та повідомити про помилку, якщо маршрутизація до інших функціональних модулів неможлива.

Окрім основних функцій, модуль NAE також забезпечує взаємодію з базовою мережею IMS через інтерфейс Gm для досягнення авторизації та автентифікації мережевих додатків. Крім того, інтерфейс Gm призначений для підтримки файлів система FFS [3].

Модуль NGC (Generic Network Communication) забезпечує впорядковане встановлення та завершення транспортних сеансів без необхідності підтвердження встановлених ключів безпеки. Генерація ключів безпеки виконується модулем безпеки NSEC для створення ключів, специфічних для сеансу. Типові діалоги на рівні програми між пристроями M2M/шлюзами M2M та модулями NGC базуються на протоколі HTTP. У деяких випадках сеанс профілю безпеки може базуватися на протоколі TLS-PSK.

Крім того, модуль NGC:

- Забезпечує шифрування/наскрізний захист даних пристроїв M2M та шлюзів M2M;

- Якщо програма вимагає безпечного тунелю (наприклад, між домашнім шлюзом користувача мережі та основним функціональним модулем мережі M2M), встановлює безпечний тунель для сеансу від шлюзу M2M до пристрою M2M;

- Забезпечує засоби передачі повідомлень між такими елементами мережі M2M: пристроями M2M, шлюзами M2M, основними функціональними модулями M2M, мережевими доменами та програмами M2M, що містяться в програмах;

- Ідентифікація всіх одержувачів повідомлень, що надсилаються до модуля NGC базується на використанні унікального персонального ідентифікатора.

Модуль NRAR (Мережева досяжність, адресація та зберігання) забезпечує:

Встановлення відповідності між назвою одного або групи пристроїв M2M/шлюзів M2M та мережевою маршрутизаційною адресою пристроїв

M2M/шлюзів M2M (наприклад, у випадку мережі GPRS, кожен пристрій M2M/шлюз M2M

Можливі дві адреси: IP-адреса та MSISDN).

- Встановлення стану доступності підключеного пристрою M2M або шлюзу M2M;

- Отримання запитів від інших функціональних модулів та сповіщень про доступність пристроїв M2M або нових адрес, отриманих пристроями M2M завдяки мобільності, та зміна набору програм пристрою M2M відповідно до зареєстрованої інформації;

- Інші модулі базової мережі M2M отримують інформацію про адресу та стан доступності для підключення до пристроїв M2M або шлюзів M2M;

- Створення групи M2M, видалення та перегляд списку пристроїв M2M та шлюзів M2M, що містяться у відповідній групі.

Модуль NSEC (мережевої безпеки) забезпечує безпеку мережі M2M на рівні мережевого домену та домену додатків. Його основні функції:

- Реєстрація пристроїв M2M на рівні обслуговування за допомогою автентифікації сервісних ключів на основі протоколу;

- Керування обміном сервісними ключами між пристроями M2M/шлюзами M2M та модулями NSEC;

- Автентифікація програми перед наданням послуг;

- Взаємодія із сервером автентифікації M2M (MAS) для отримання інформації для автентифікації, необхідної для виконання автентифікації пристроїв M2M або шлюзів M2M та керування сервісними ключами.

Режими взаємодії між пристроями M2M включають: взаємодію через основну мережу M2M та шлюз M2M, а також взаємодію без проходження через основну мережу M2M та шлюз M2M[4].

Адресація та ідентифікація пристроїв M2M під час надання послуг за допомогою платформи IMS.

В основній мережі M2M, побудованій на платформі IMS[6], кожна послуга M2M ідентифікується ідентифікатором послуги IMS (ICSI). Програми M2M та

програми M2M UE в області застосувань ідентифікуються ідентифікатором програми IM (IARI).

Використовується для ідентифікації та автентифікації, реєстрації та зберігання в підсистемі основної мережі IMS (наприклад, процес реєстрації пристроїв M2M). SC основної мережі M2M також використовує ідентифікаційний код IMPU для запитів під час взаємодії з пристроями M2M.

SC основної мережі M2M використовує підсистему IMS для реєстрації мережевих програм. Для цих цілей основна мережа M2M SC підтримує зв'язок між модулями додатків M2M (використовуючи їх для додатків M2M), кожному з яких присвоюється власний ідентифікатор IMPI для ідентифікації, а також ідентифікатор IARI.

2.3. Характеристика стандартів Інтернету речей та взаємодії пристроїв в бездроьових сенсорних мережах

Існуючі варіанти використання традиційно зосереджувалися на двох частинах застосувань технології NB-IoT. По-перше, ринок IoT/M2M включає переважно дві основні сфери: промислову та споживчу, які можна розділити на чотири категорії [19-20]: домашні пристрої IoT (IoT Appliance); персональні пристрої IoT (IoT Personal); рішення IoT, що відповідають суспільним потребам (IoT Public); та промислові рішення IoT (IoT).

Найбільший попит на додатки, що використовують технологію NB-IoT, мають такі бізнес-сфери: електронна охорона здоров'я; роздрібна торгівля; безпека та оборона; автомобільні та логістичні перевезення; енергетика, житлово-комунальне господарство; промислове виробництво; розумні міста; розумні будинки тощо.

Згідно з технічними характеристиками, бюджет бездротового з'єднання, що покривається обладнанням користувача NB-IoT, становить 164 дБ, тоді як бюджет бездротового з'єднання для GPRS становить 144 дБ (45 820 турецьких

лір), а бюджет бездротового з'єднання для LTE – 142,7 дБ (36 888 турецьких лір). Як результат, технологія NB-IoT матиме набагато краще покриття (бюджет радіозв'язку на 20 дБ вищий, ніж аналогічні бюджети для стільникових мереж GPRS та LTE).

Окрім розширеного покриття, також значно покращиться ємність базових станцій LTE завдяки нижчій швидкості передачі даних пристроїв користувачів NB-IoT. Згідно з розрахунками Neul та Huawei та партнерського проекту 3GPP [6], одна макробазова станція LTE з радіусом дії 1 км може обслуговувати понад 50 000 пристроїв користувачів NB-IoT. Така базова станція мала б достатню потужність для обслуговування користувачів у густонаселених міських районах з приблизно 1500 будинками на квадратний кілометр, кожен з яких має 40 пристроїв Інтернету речей. Однак слід зазначити, що кількість обслуговуваних пристроїв користувачів стосується не кількості пристроїв, що обслуговуються одночасно, а кількості пристроїв користувачів, що обслуговуються базовою станцією на каналі 180 кГц протягом однієї години, за умови, що кожен пристрій передає 100 байт інформації. На рисунку 7.7 показано кількість пристроїв користувачів, що обслуговуються в комірці, як функцію радіуса комірки для різних рівнів додаткових втрат проникнення через будівлі. Крім того, навіть при втратах проникнення до 40 дБ через будівлі, базова станція LTE з радіусом покриття 1 км все ще може обслуговувати до 45 000 пристроїв Інтернету речей на годину [2].

Ще однією важливою перевагою пристроїв користувачів NB-IoT є значно збільшений термін служби батареї порівняно з традиційними мобільними пристроями GSM/UMTS/LTE. Згідно з рекомендаціями 3GPP, за ідеальних теоретичних умов термін служби акумулятора користувацького пристрою NB-IoT, оснащеного акумулятором ємністю 2500 мАг, становитиме 36 років. Цей показник розраховано виходячи з припущення, що користувацький пристрій NB-IoT здійснює зв'язок один раз на день, обсяг переданих даних не перевищує 50 байт, а затухання сигналу між антеною базової станції та антеною пристрою IoT не перевищує 144 дБ. Завдяки високій швидкості передачі даних пристроїв NB-

IoT (до 200 біт протягом двох годин) та великому затуханню сигналу бездротового каналу (до 164 дБ), термін служби акумулятора користувацьких пристроїв NB-IoT становитиме менше 2 років. В середньому модуль NB-IoT може працювати автономно близько 10 років від одного акумулятора.

Важливо зазначити, що ці розрахунки не враховують вплив саморозряду акумулятора, який може значно скоротити термін служби акумулятора пристроїв Інтернету речей. Вартість акумулятора з низьким коефіцієнтом саморозряду може бути в багато разів вищою за вартість самого пристрою Інтернету речей.

Враховуючи необхідність покращення (розширення) покриття NB-IoT, основною стратегією буде розгортання мереж NB-IoT у діапазонах частот 700, 800 та 900 МГц.

Використання спектру для застосувань Інтернету речей/M2M, оскільки нормативно-правова база для використання спектру в цих сферах вже існує на міжнародному, регіональному та національному рівнях управління спектром.

Другим фактором, що прискорює впровадження NB-IoT у цих діапазонах частот, є наявність (ліцензованого) спектру для операторів мереж доступу Інтернету речей/M2M. Для мобільних операторів, що працюють у діапазонах частот GSM-900 або LTE-800/700, пристрої на базі NB-IoT можуть бути розгорнуті швидко та з відносно невеликими інвестиціями.

Діапазон частот 694–790 МГц, визначений 3GPP для мереж LTE, потрапляє в діапазон, визначений у Рекомендації ITU-R M.1036-4 щодо розвитку мереж мобільного радіодоступу 4G. Резолюція ECC/DEC/(15)01[9] передбачає виділення одного каналу в смузі 694-790 МГц для парного використання в межах цієї смуги (2x30 МГц для FDD) та додаткове виділення до чотирьох блоків 5 МГц у смузі 738-758 МГц для непарного використання мережами.

Комітет CEPT ECC підготував Звіт ECC № 242 «Дослідження сумісності та спільного використання вузькосмугових програм M2M у смузі частот 733-736/788-791 МГц», у якому аналізуються проблеми сумісності вузькосмугових програм M2M у смузі частот 733-736/788-791 МГц та вплив спільного використання між машинами на національний спектр. У Звіті M2M

пропонуються альтернативні рішення щодо спільного використання спектру для мовників, що займаються виробництвом програм та проведенням спеціальних заходів (PMSE), станціями громадської безпеки та реагування на стихійні лиха (PPDR), мережами доступу M2M та мережами LTE у діапазоні 700 МГц (діапазонами B28 та B20).

Крім того, у звіті ECC 242 зроблено такі висновки щодо використання спектру:

Резолюція ECC/DEC/(09)03 від 30 жовтня 2017 року детально описує використання та частотний план цифрового дивіденду в діапазоні 790-862 МГц.

У 2009 році вони включали:

і інверсний режим FDD (використання смуг передачі та прийому у зворотному порядку) для зменшення впливу абонентських терміналів (ST) на радіоелектронні системи цифрового телебачення;

- Необхідність розділення режимів FDD та TDD та використання різних частотних планів;

- Необхідність визначення розміру частотних блоків LTE;

- Необхідність визначення кроку частотної сітки в плані (1 МГц або 2 МГц);

- Введення захисної смуги FDD (між дуплексними смугами) - більше 10 МГц (бажано 12 МГц);

- Використання додаткової фільтрації для ізоляції каналів DLUL (усунення перекиду потужності через майже дуплексний діапазон).

Згідно з цим рішенням ECC, європейські гармонізовані канали базуються на частотних блоках (каналах) шириною 5 МГц, використовуючи дві смуги частот 2x30 МГц з дуплексним інтервалом 11 МГц. Підхід, прийнятий у Європі для діапазону 790...862 МГц, подібний до підходу ITU-R та базується на зворотному принципі використання пари смуг частот для дуплексного зв'язку FDD, використовуючи дуплексну смугу (790-791 МГц) із захисним інтервалом 1 МГц.

LTE в режимі FDD використовує нижчий діапазон частот низхідного каналу, ніж діапазон частот висхідного каналу, починаючи з 791 МГц, тоді як діапазон частот висхідного каналу для FDD становить 832 МГц.

У 2016 році Комітет з електронних комунікацій (ECC) Європейського комітету зі стандартів телекомунікацій (CEPT) започаткував нову дослідницьку тему «M2M у мобільних мережах» у Робочій групі RT1. Ця тема охоплює дев'ять частотних діапазонів, визначених 3GPP для NB-IoT та M2M у мережах LTE: 700 МГц, 800 МГц, 900 МГц, 1800 МГц, 2100 МГц, 2300 МГц, 2600 МГц, 3400-3600 МГц та 3000 МГц. Це може значно розширити сфери застосування технології NB-IoT.

Таким чином, поява на ринку мереж LTE Advanced з вузькосмуговою технологією передачі даних для IoT (NB-IoT) значно посилить конкуренцію на ринку бездротового IoT порівняно зі все більш популярними технологіями UNB, LoRa, LPWAN та іншими, що використовують неліцензовані діапазони.

Технологія NB-IoT має багато переваг з точки зору швидкості, масового виробництва та низької вартості. Можливість використання ліцензованих частотних діапазонів, вже розроблених мобільними операторами 4G, та мережевого обладнання, яке вже розгорнуто для NB-IoT, призведе до подальшого розвитку сектору IoT у бізнес-структурі мобільних операторів. Для впровадження технології NB-IoT на українському ринку найближчим часом потрібні зміни в нормативно-правовій базі використання радіочастотного спектру та правилах використання нових пристроїв у мережах загального користування.

2.4. Проектування бездротової сенсорної мережі Інтернету речей при мультимодальному розподілі вузлів

Мережевою основою для реалізації концепції Інтернету речей є самоорганізуюча мережа, яка може автоматично вибирати топологію мережі,

автоматично підключати нові пристрої до мережі та автоматично вибирати маршрут для передачі пакетів даних у мережі без втручання людини. Найбільш широко використовуваними з цих мереж є бездротові персональні мережі (WPAN) або бездротові сенсорні мережі.

Бездротова персональна мережа (WPAN) – це мережа ближнього радіусу дії, зазвичай не довша за 10-20 метрів. Характерною особливістю бездротової персональної мережі (WPAN) є її низьке енергоспоживання. Тому використання автономних джерел живлення в радіообладнанні дозволяє класифікувати ці мережі як пристрої мобільного зв'язку з обмеженим радіусом дії. WPAN в основному використовується для підключення різних побутових та промислових пристроїв, включаючи комп'ютери та офісне обладнання, системи розумного дому та розумного офісу, всередині приміщень. У відповідь на це ми розробили Інтернет речей для спільнот Манхеттена.

Для впровадження бездротових персональних мереж (WPAN) Інститут інженерів з електротехніки та електроніки (IEEE) розробив серію стандартів IEEE 802.15, які описують два нижні рівні протоколу взаємодії відкритих систем (OSI): фізичний рівень (PHY) та рівень контролю доступу до середовища (MAC).

Одним з перших стандартів для бездротових персональних мереж був стандарт IEEE 802.15.1, який базувався на технології Bluetooth. Мережі IEEE 802.15.1 (Bluetooth) використовуються для обміну інформацією між такими пристроями, як персональні комп'ютери, мобільні пристрої, принтери, цифрові камери та бездротові гарнітури.

Однак для деяких пристроїв, що працюють у мережах WPAN, швидкості, що забезпечується технологією Bluetooth, недостатньо, і потрібен стандарт, який дозволяє створювати канали бездротової передачі даних з пропускною здатністю десятки або навіть сотні мегабіт на секунду. Ці стандарти утворюють сімейство стандартів IEEE 802.15.3 і забезпечують основу для мереж UWB (надширокосмугових). Ці мережі ідеально підходять для передачі великих обсягів інформації (голосу, даних, відео) на високих швидкостях.

Для пристроїв, які не потребують високої швидкості передачі даних, але потребують більшого часу роботи від батареї та менших витрат, таких як різні датчики, системи збору та управління даними, розроблено низькошвидкісний стандарт WPAN IEEE 802.15.4.

Технологія Bluetooth базується на групуванні пристроїв у пікомережі – бездротові мережі передачі даних, що складаються з невеликої кількості пристроїв, розташованих поблизу один одного (зазвичай не більше 10 метрів).

Базова пікомережа складається з двох пристроїв з підтримкою Bluetooth, один з яких називається головним, а інший – підлеглим. Крім того, головний пристрій ініціює та підтримує функцію з'єднання. Максимальна кількість підключень до головного пристрою становить сім, а загальна швидкість передачі даних не перевищує максимальну швидкість цієї версії технології. Функції головного та веденого пристроїв не призначені виключно для них і можуть змінюватися залежно від навантаження. Пристрої в різних з'єднаннях можуть грати різні ролі, а також можуть виступати в ролі ведених пристроїв для різних головних пристроїв.

Технологія Bluetooth використовує неліцензований діапазон частот 2,4...2,4835 ГГц. Радіоканали Bluetooth використовують технологію стрибкоподібної перебудови частоти (FHSS), що робить систему зв'язку стійкою до широкосмугових перешкод. Згідно з цим алгоритмом, несуча частота сигналу Bluetooth FHSS змінюється 1600 разів на секунду, і одночасно виділяється 79 робочих каналів шириною 1 МГц. Послідовність перемикання частот для кожного з'єднання є псевдовипадковою та відома лише передавачу та приймачу, які синхронно перемикаються з однієї несучої частоти на іншу кожні 625 мкс (інтервал часу). Тому, якщо поруч працюють кілька пар приймачів, вони не будуть заважати один одному. Цей алгоритм також є невід'ємною частиною системи захисту конфіденційності переданої інформації: перетворення виконується за допомогою псевдовипадкового алгоритму та визначається індивідуально для кожного з'єднання.

Технологія Bluetooth забезпечує дуплексний зв'язок з часовим поділом (TDD). Головний пристрій надсилає пакети даних через непарні інтервали часу, а ведений пристрій надсилає пакети даних через парні інтервали часу. Залежно від довжини пакета, він може охоплювати до п'яти часових інтервалів, а частота каналу не змінюється, доки пакет не буде завершено.

Технологія Bluetooth підтримує один асинхронний канал для передачі даних та до трьох синхронних каналів для передачі голосу. Вона також підтримує одночасну асинхронну передачу даних та синхронну передачу голосу. Швидкість передачі голосових даних по синхронному каналу становить 64 кбіт/с у кожному напрямку.

Для цифрових даних та аудіосигналів використовуються різні схеми кодування, оскільки цифрові дані можуть бути повторно передані, якщо пакет даних втрачено, але аудіосигнали, як правило, не повторно передаються.

Модулі, що підтримують перші версії специфікації Bluetooth, 1.0 (1998) та 1.0B (1999), виготовлялися різними виробниками та були погано сумісні один з одним. У цих версіях специфікації адреса пристрою (Bluetooth device address, BD_ADDR) повинна передаватися на етапі встановлення з'єднання, що унеможливлює досягнення анонімності з'єднань пристроїв на рівні протоколу, що є суттєвим недоліком специфікації. Максимальна швидкість передачі даних для з'єднання Bluetooth становить 721 кбіт/с.

Bluetooth 1.1, випущений у 2002 році, виправив багато помилок, виявлених у версіях 1.0 та 1.0 B; він додав підтримку незашифрованих каналів та індикацію рівня прийнятого сигналу (RSSI).

Bluetooth 1.2, випущений у 2003 році, додав технологію адаптивної перебудови частоти (AFH) для боротьби з електромагнітними перешкодами, що виникають, коли мережі Bluetooth використовуються разом з бездротовими локальними мережами, такими як Wi-Fi, що працюють в одному діапазоні частот. Ця версія Bluetooth реалізує покращену технологію ізохронних каналів.

eSCO (Enhanced Synchronous Connection-Oriented Communication) покращує якість голосу шляхом повторення пошкоджених пакетів. Додано

підтримку трипровідного інтерфейсу UART для підключення модуля Bluetooth до зовнішніх пристроїв (Універсальний асинхронний приймач/передавач).

Bluetooth 2.0 було випущено в листопаді 2004 року. Він має зворотну сумісність з попередніми версіями 1.x. Головним нововведенням є підтримка вищих швидкостей передачі даних (до 2100 кбіт/с в асиметричному режимі та до 1430 кбіт/с у симетричному режимі). Максимальний розмір мережі було збільшено з 8 пристроїв до 256, а також додано механізм контролю якості обслуговування (QoS), щоб забезпечити зв'язок пристроїв з мінімальною затримкою [6].

Bluetooth 2.1 було випущено в серпні 2008 року. Ця версія використовує технологію Sniff Subrating для зменшення споживання енергії в п'ять разів, що подовжує термін служби акумулятора пристроїв Bluetooth. Bluetooth 2.1 покращує безпеку даних та спрощує процес ідентифікації та підключення пристроїв Bluetooth.

У 2009 році вийшов Bluetooth 3.0, який підтримував швидкість передачі даних до 24 Мбіт/с, що було досягнуто завдяки використанню двох радіомодулів: звичайного модуля Bluetooth, який забезпечує швидкість передачі даних 2,1 Мбіт/с, та додаткового модуля, що працює за протоколом 802.11, який забезпечує швидкість передачі даних до 24 Мбіт/с. Вибір модуля передачі даних залежить від розміру файлу, що передається. Невеликі файли передаються по повільних каналах.

Bluetooth 4.0 був випущений у червні 2010 року. Головною метою нової специфікації є вирішення проблеми високого енергоспоживання Bluetooth 3.0. Специфікація Bluetooth 4.0 включає класичний низькошвидкісний протокол Bluetooth, заснований на попередній версії специфікації Bluetooth, високошвидкісний протокол Bluetooth, заснований на технології Wi-Fi, та протокол Bluetooth з низьким енергоспоживанням. Низьке енергоспоживання досягається завдяки використанню спеціального алгоритму роботи, згідно з яким передавач вмикається лише під час надсилання даних. Це гарантує, що пристрій Bluetooth може працювати роками від однієї батарейки CR2032. Модулі

Bluetooth 4.0 можуть бути ефективно застосовані до мікроелектронних датчиків та детекторів, а також до різних смартфонів та персональних комп'ютерів.

Стандарт IEEE 802.15.3 описує бездротову мережу, в якій кілька незалежних пристроїв можуть безпосередньо взаємодіяти один з одним. Розмір таких мереж зазвичай не перевищує 10 метрів. Основні вимоги - висока швидкість передачі даних, проста інфраструктура, легкість організації та підключення до мережі, доступні засоби захисту даних та гарантована якість обслуговування для певних типів трафіку. Діапазон частот, виділений для роботи таких персональних мереж, становить 2400...2483,5 МГц. Стандарт визначає п'ять прийнятних швидкостей передачі даних. 22 Мбіт/с - це базова швидкість, яку повинні підтримувати всі пристрої IEEE 802.15.3.

Стандарт IEEE 802.15.3 визначає два частотні плани: 1) режим користувацького пристрою високої щільності з використанням чотирьох каналів; та 2) режим, сумісний з мережами IEEE 802.11b, що використовують три канали, центральні частоти яких відповідають стандартним частотам IEEE 802.11b. Розглянемо два частотні плани із загальною кількістю 5 каналів, кожен зі смугою пропускання 15 МГц. У 2009 році було випущено новий стандарт високошвидкісної бездротової персональної мережі IEEE 802.15.3c, який використовує міліметрові радіохвилі в діапазоні 57-66 ГГц. [10] Примітною особливістю цього діапазону частот є те, що радіохвилі сильно ослаблюються атмосферними газами та гідрометеорами, тому їх можна використовувати лише для зв'язку на коротких відстанях, зазвичай до приблизно 10 метрів. Основною перевагою цієї серії є надзвичайно широкий використовуваний діапазон частот. Коротка довжина хвилі значно зменшує розмір антенної системи та розмір самого приймально-передаючого обладнання. Крім того, використання цього діапазону частот усуває проблему перешкод між різними джерелами сигналу через сильне ослаблення та вирішує проблему повторного використання частоти. Саме тому багато країн не дозволяють використання цього діапазону. В Україні для радіообладнання фіксованої служби виділено діапазон частот 58,25…63,25 ГГц.

Стандарт IEEE 802.15.3c забезпечує швидкість передачі даних до 5 Гбіт/с. Стандарт тепер включає можливість роботи в режимі формування променя. На рівні MAC різні вхідні дані можуть бути об'єднані в один пакет для підвищення ефективності системи зв'язку.

На фізичному рівні описано три режими роботи:

- Оптимізований режим передачі на одній несучій (SC) для мінімізації енергоспоживання та складності системи;

- Режим високошвидкісного інтерфейсу (HSI), призначений для двостороннього зв'язку з мінімальною затримкою;

- Режим аудіо/відео (AV) використовується для передачі нестиснених потоків відео та аудіо високої чіткості.

Іншим конкуруючим стандартом для високошвидкісних бездротових персональних мереж є стандарт Wireless Home Digital Interface (WHDI).

- Wireless Home Digital Interface. Стандарт був розроблений ізраїльською компанією Amimon та просувається консорціумом WHDI, до якого входять такі виробники побутової електроніки:

Hitachi, LG Electronics, Motorola, Samsung, Sharp та Sony.

WHDI працює в неліцензованому діапазоні частот 5,1-5,9 ГГц, використовуючи канали 40 МГц. З пропускною здатністю 3 Гбіт/с мережі WHDI забезпечують бездротову передачу нестисненого високоякісного відео та аудіо.

Стандарт IEEE 802.15.4 запроваджує низькошвидкісні бездротові персональні мережі з низьким енергоспоживанням. Стандарт був затверджений у 2003 році та призначений для створення бездротових мереж з низьким енергоспоживанням та максимальною дальністю дії від 10 до 100 метрів. Стандарт визначає такі швидкості передачі даних: 250, 100, 40 та 20 кбіт/с, і дозволяє роботу у трьох можливих неліцензованих радіочастотних діапазонах:

-868,0…868,6 МГц (Європа)

-902…928 МГц; використовується в Північній Америці;

- 2400…2483,5 МГц; використовується в Україні та інших частинах світу. Стандарт IEEE 802.15.4 розрізняє два типи вузлів бездротової мережі:

- RFD (пристрій обмеженого діапазону), який збирає інформацію в межах певного діапазону свого розташування;

- Повнофункціональний пристрій (FFD) виконує пересилання пакетів та збір інформації.

Мережі IEEE 802.15.4 можуть бути побудовані з використанням топології peer-to-peer або зірчастої топології. Кожна мережа повинна мати принаймні один повнофункціональний пристрій, який виконує роль координатора. Стандарт IEEE 802.15.4 є основою для протоколів вищого рівня (ZigBee, 6loWPAN, DigiMesh тощо).

Технологія ZigBee. У 2004 році альянс ZigBee розробив специфікації для мережі та прикладного протоколу ZigBee на основі стандарту IEEE 802.15. ZigBee Alliance – це консорціум, що складається з понад 180 компаній, які працюють над розробкою стандартів, стеків протоколів та специфікацій прикладних програм для споживчого та промислового секторів. Профілі прикладних програм зосереджені на автоматизації будівель, промисловому моніторингу, опаленні, вентиляції та кондиціонуванні повітря (HVAC), а також роботі датчиків. Специфікація ZigBee описує проектування мережі, проблеми безпеки та прикладне програмне забезпечення.

Завдяки вбудованому програмному забезпеченню пристрої мережі ZigBee можуть виявляти один одного та формувати мережу при ввімкненні, а якщо вузол виходить з ладу, вони можуть встановлювати нові маршрути для передачі повідомлень [4].

Маршрутизація мережі ZigBee складається з трьох типів логічних пристроїв: координатор ZigBee, маршрутизатор ZigBee та термінальний пристрій ZigBee. Функції координатора ZigBee включають сканування каналів для пошуку вільних каналів та встановлення мережі, генерацію мережевого ідентифікатора (PAN ID), підключення нових мережевих пристроїв (маршрутизаторів та кінцевих вузлів), а також маршрутизацію та буферизацію даних для неактивних кінцевих вузлів. У мережі ZigBee може бути лише один координатор. Функції маршрутизатора ZigBee включають ретрансляцію пакетів,

маршрутизацію та надання буферних даних для неактивних кінцевих вузлів. Кінцеві вузли ZigBee виконують лише прикладні операції (збір інформації та дистанційне керування) та не передають дані.

Протокол ZigBee може бути використаний для реалізації простих з'єднань "точка-точка" та "зірка", або для формування складних мереж з деревоподібною та сітчастою топологією.

Дальність, на якій вузли мережі ZigBee можуть надійно передавати радіосигнали, залежить від багатьох параметрів (перш за все, чутливості приймача та потужності передавача), але в середньому відстань між вузлами мережі ZigBee становить сотні метрів на відкритому просторі та десятки метрів у приміщенні.

Усі пристрої, що працюють у мережі ZigBee будь-якої топології, мають унікальну 16-бітну або 64-бітну адресу, яку можна використовувати для прямого зв'язку в персональній мережі (PAN). Під час процесу організації координатор мережі відповідає за призначення унікальних адрес пристроям.

Технологія ZigBee дозволяє вирішувати багато різних, не пов'язаних між собою прикладних завдань в межах однієї мережі. Для забезпечення розділення пакетів між різними програмами використовуються 8-бітні ідентифікатори кінцевих точок.

Для забезпечення повної сумісності між пристроями різних виробників та їх взаємодії в межах однієї розподіленої програми технологія ZigBee використовує концепцію профілів, які розрізняються в пакетах даних за допомогою 16-бітних ідентифікаторів. Специфікація описує набір технічних параметрів, домовленостей щодо структури даних та форматів повідомлень, яких виробники повинні суворо дотримуватися, щоб забезпечити відповідність своєї продукції специфікації. Поточний список профілів застосувань, опублікований ZigBee Alliance, включає: домашню автоматизацію, автоматизацію комерційних будівель, роздрібну торгівлю, інтелектуальні мережі, телекомунікації, охорону здоров'я, дистанційне керування, пристрої введення та пристрої керування освітленням.

Технологія Z-Wave використовує неліцензовані частоти нижче 1 ГГц, які відрізняються залежно від регіону. У США частота становить 908,42 МГц, у Європі – 868,42 МГц, у Росії діапазон частот для технології Z-Wave становить 868,7…869,2 МГц, виділений Постановою Державного комітету з радіочастот № 08-24-01-001 від 28 квітня 2008 року.

Швидкість передачі даних у мережі Z-Wave залежить від використовуваних пристроїв і може досягати 100 кбіт/с. Технологія розроблена для передачі команд керування (наприклад, увімкнення/вимкнення пристрою або зміни яскравості з низькою затримкою світло). Технологія Z-Wave не підходить для потокової передачі даних. Максимальна дальність зв'язку між двома безпосередньо підключеними пристроями Z-Wave становить від 10 до 30 метрів (залежно від середовища)[6].

Технологія Z-Wave забезпечує підтвердження доставки пакета - якщо команда не досягає одержувача, пристрій повторно передає дані.

Мережа Z-Wave використовує сітчасту топологію, де кожен пристрій у мережі Z-Wave є одночасно приймачем і передавачем. Це підвищує надійність мережі - якщо один пристрій вийде з ладу, сигнал буде передаватися через сусідні пристрої, а покриття можна розширити, просто додавши нові пристрої, які можуть виступати в ролі ретрансляторів сигналу, передаючи сигнал по каналу зв'язку. Мережа Z-Wave не потребує додаткових ретрансляторів або підсилювачів сигналу; достатньо, щоб будь-який пристрій у мережі Z-Wave знаходився в межах дії сусідніх пристроїв.

Мережі Z-Wave складаються з двох різних типів вузлів:

- Вузли керування (контролери), які виконують маршрутизацію в мережі та забезпечують взаємодію з іншими мережами;

- Вузли виконавчих механізмів можуть надсилати, отримувати та виконувати команди, але не мають можливостей маршрутизації; Водночас виконавчі механізми можуть виступати в ролі повторювачів сигналів у мережі Z-Wave.

Обидва типи вузлів можуть використовуватися для різноманітних пристроїв. Максимальна кількість вузлів мережі, визначена технологією Z-Wave, становить 232 вузли. Пристрої керування та виконавчі механізми бувають різних типів залежно від їх призначення та області застосування. Ідентифікатор мережі (також званий домашнім ідентифікатором) та ідентифікатор вузла використовуються для ідентифікації пристроїв у мережі та розрізнення мереж Z-Wave.

Система BreezeMAX™ – це найновіша система Alvarion, розроблена для підтримки передових платформ WiMAX. Система використовує найсучаснішу технологію OFDM з адаптивною модуляцією (до 64QAM) та працює в умовах відсутності прямої видимості (NLOS). Висока спектральна ефективність системи BreezeMAX™ дозволяє операторам негайно розпочати побудову мереж WiMAX. BreezeMAX™ працює в діапазоні частот 3,5 ГГц, а її платформа підтримує стандарти WiMAX: IEEE 802.16 та HiperMAN, задовольняючи потреби користувачів в економічно ефективних системах BWA наступного покоління. Ми обрали систему BreezeMAX™ для нашого проекту Інтернету речей у багатоквартирному будинку на Мангеттені.

Характеристики системи BreezeMAX (Рисунок 2.4):

Рис. 2.4. Широкосмуговий бездротовий доступ для Інтернету речей

- Розроблена для різних ринків - Підходить для обслуговування житлових користувачів, комерційних користувачів, MDU/MTU, точок доступу, транспортних мереж та бездротових домашніх мереж;

- Низька вартість - легке встановлення, оплата за використання;

- Системи операторського класу (висока продуктивність та доступність, резервування компонентів, гнучка система управління мережею);

- Масштабована конфігурація обладнання базових станцій. Базові станції на базі шасі (висока щільність) найкраще підходять для масштабного розгортання в міських та приміських районах. Мікросоти є ідеальним та економічно ефективним рішенням для сільських та малонаселених районів;

- Висока продуктивність та пропускна здатність - Можливості повнодуплексної та багатоканальної базової станції дозволяють одній базовій станції підтримувати велику кількість користувачів;

- Покриття NLOS - Модуляція OFDM покращує продуктивність в умовах майже прямої видимості;

- Система управління AlvariSTAR - Платформа NMS операторського класу, що підтримує всі функції 2.3 Основні принципи та характеристики обладнання BreezeMAX

Система BreezeMAX™ - це найновіша система Alvarion, розроблена для підтримки передових платформ WiMAX. Система використовує найсучаснішу технологію OFDM з адаптивною модуляцією (до 64QAM) та працює в умовах відсутності прямої видимості (NLOS). Висока спектральна ефективність системи BreezeMAX™ дозволяє операторам негайно розпочати побудову мереж WiMAX. BreezeMAX™ працює в діапазоні частот 3,5 ГГц та відповідає потребам користувачів у наступному поколінні економічно ефективних систем BWA. Її платформа підтримує стандарти WiMAX: IEEE 802.16 та HiperMAN (Рисунок 2.3).

Основними архітектурами WiMAX є IEEE 802.16 та ETSI HiperMAN.

Розроблена для різних ринків – ідеально підходить для житлових та комерційних будівель, багатоквартирних комплексів, точок доступу, магістральних та бездротових домашніх мереж.

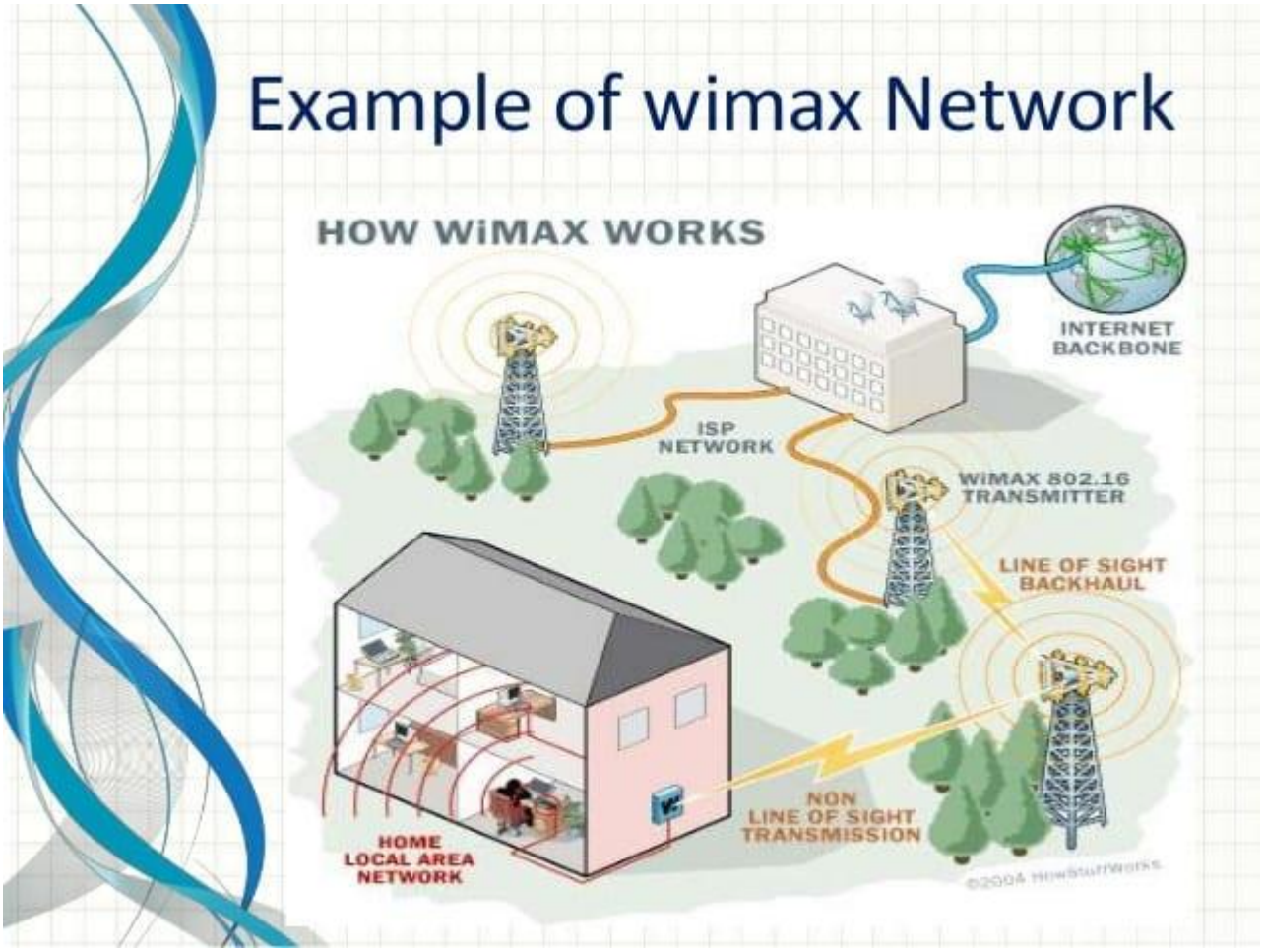


Рис. 2.5. Організація бездротової сенсорної мережі Інтернету речей житлового комплексу при мультимодальному розподілі вузлів

Низька вартість, легке встановлення та підтримка оплати за використання. Система операторського класу, висока продуктивність, висока доступність, резервування компонентів, гнучка система управління мережею.

Масштабована конфігурація обладнання базової станції. Базові станції на базі шасі (високої щільності) найкраще підходять для масштабного розгортання в міських та приміських районах.

Мікростільники – ідеальне та економічно ефективне рішення для сільських та малонаселених районів.

Висока продуктивність та пропускна здатність – повнодуплексні та багатоканальні можливості базових станцій дозволяють одній базовій станції підтримувати велику кількість користувачів.

Покриття NLOS – модуляція OFDM покращує продуктивність прямої видимості.

Технологія адаптивної модуляції. Система управління AlvariSTAR – це платформа NMS операторського класу, яка підтримує повну функціональність FCAPS.

Апаратне забезпечення базових станцій BreezeMAX доступне у двох основних конфігураціях: базові станції високої щільності для масштабного розгортання в міських та приміських районах, а також мікросоти для сільських та малонаселених районів.

Таблиця 2.1 Компоненти базової станції

Тип продукту	Назва продукту	Опис продукту
Для великомасштабних розгортань (місто, передмістя)	BMAX-BST-SH	BreezeMAX 3500 base station shelf
	BMAX-BST-NPU	BreezeMAX 3500 base station
		network processor unit
	BMAX-BST-AU-IDU-	BreezeMAX 3500 base station
	2CH	access unit interface module
	BMAX-BST-PSU	BreezeMAX 3500 base station power supply
		unit
	BMAX-BST-PIU	BreezeMAX 3500 base station power interface
		unit
Мініатюрна (для сільських місцевостей)	BMAX-MBST-IDU-	BreezeMAX 3500 micro base station
	2CH-AC	indoor unit, AC power
	BMAX-MBST-IDU-	BreezeMAX 3500 micro base station
	2CH-DC	indoor unit, DC power

Платформа BreezeMAX пропонує різноманітні економічно ефективні типи пристроїв кінцевих користувачів, що надає операторам гнучкість для обслуговування широкого кола житлових та комерційних користувачів (Таблиця 2.2).

Таблиця 2.2. Компоненти користувацьких станцій

Продукт	Ім’я продукту	Опис продукту
CPE Indoor (внутрішні)	BMAX-CPE-IDU-1D	BreezeMAX 3500 broadband data CPE indoor module with one 10/100 BaseT
	BMAX-CPE-IDU-VG-1D1V	BreezeMAX 3500 broadband voice gateway CPE indoor module with one 10/100 BaseT data port + one RJ11

	BMAX-CPE-IDU-VG-4D2V	BreezeMAX 3500 broadband voice gateway CPE indoor module with four 10/100 BaseT data ports + two RJ11
	BMAX-CPE-IDU-NG-4D1WLAN	BreezeMAX 3500 networking gateway CPE indoor module with four 10/100 BaseT data ports + one 802.11b/g
CPE Outdoor (зовнішні)	BMAX-CPE-ODU-AV-3.5	BreezeMAX 3500 subscriber outdoor radio unit with integrated vertical antenna, frequency band 3.5a+b
	BMAX-CPE-ODU-AH-3.5	BreezeMAX 3500 subscriber outdoor radio unit with integrated horizontal antenna, frequency band 3.5a+b
	BMAX-CPE-ODU-E-3.5	BreezeMAX 3500 subscriber outdoor radio unit with connnector for external antenna,

Система BreezeMAX є найновішою розробкою системи Alvarion, яка підтримує передові платформи WiMAX. На рис. 2.6 показано типову схему WiMAX.

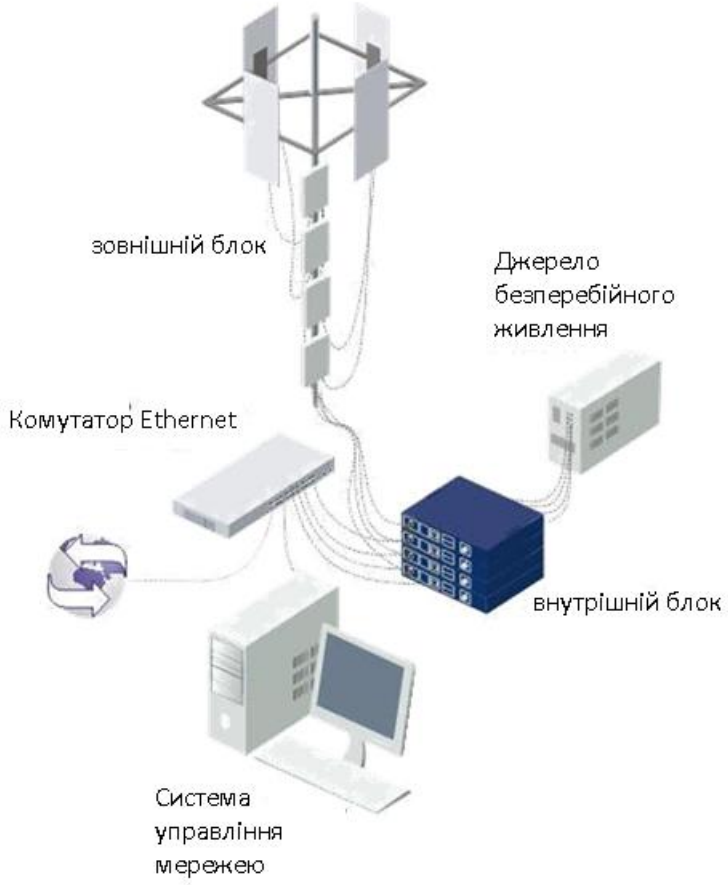


Рис. 2.6. Схема базової станції WiMAX

Система використовує найсучаснішу технологію OFDM з адаптивною модуляцією (до 64QAM) та працює в умовах майже прямої видимості.

BreezeMAX™ працює в діапазоні частот 3,5 ГГц, а її платформа підтримує стандарти WiMAX: IEEE 802.16 та HiperMAN, задовольняючи потреби користувачів у економічно ефективних системах BWA наступного покоління.

Використовуйте секторну антену. Кількість секторів змінна.

Кожен внутрішній модуль має інтерфейс Ethernet 10/100 Base TX.

Платформа BreezeMAX™ пропонує різноманітні варіанти пристроїв кінцевих користувачів, що дозволяє операторам ефективно обслуговувати широке коло користувачів як на комерційному, так і на житловому ринку [6].

Пристрій користувача BreezeMAX™ має високоінтегрований дизайн, який забезпечує високу надійність та служить ефективною платформою для широкого спектру послуг (Рис. 2.7).

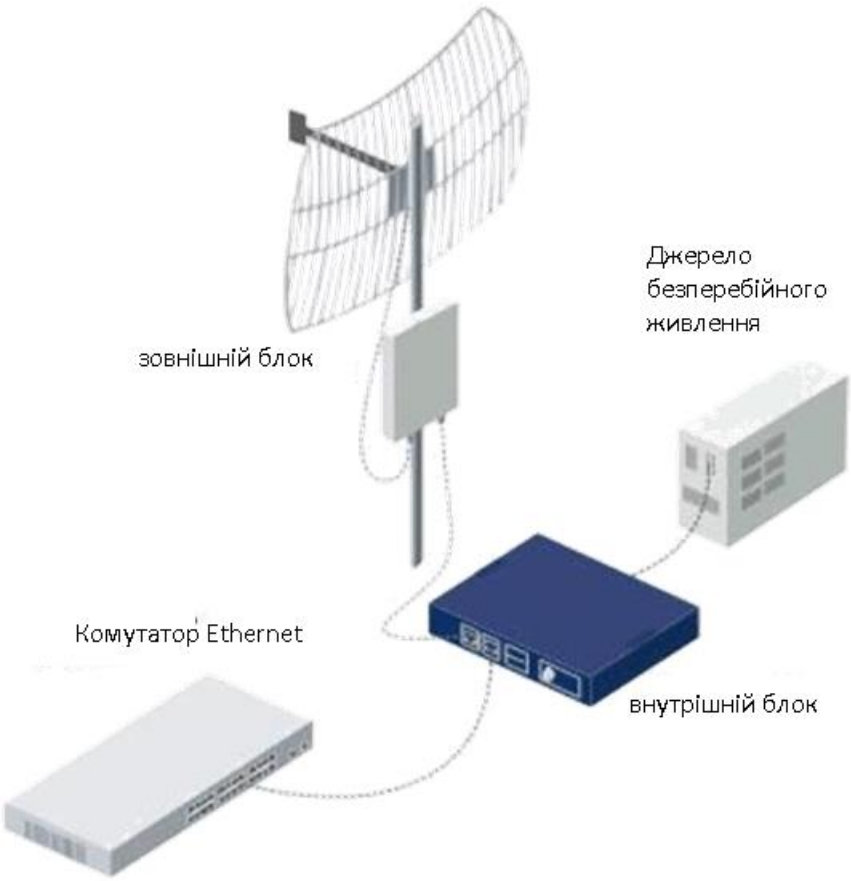


Рис. 2.7. Типова схема станції користувача WiMAX

Система BreezeMAX™ забезпечує користувачам високошвидкісний доступ зі швидкістю передачі даних до 12,7 Мбіт/с на каналі 3,5 МГц.

Клієнтський пристрій BreezeMAX™ підтримує такі основні програми:

Широкосмуговий доступ до даних та голосу, домашній Інтернет та точки доступу.

Обладнання користувача BreezeMAX™ складається з внутрішнього та зовнішнього модулів[8].

Зовнішній модуль містить усі активні компоненти та інтегровану планарну антену з високим коефіцієнтом посилення. Внутрішній блок підключено до зовнішнього блоку за допомогою кабелю Ethernet категорії 5. Цей кабель передає дані Ethernet, сигнали моніторингу стану, керування та скидання для внутрішнього блоку, а також живлення (54 В постійного струму) для зовнішнього блоку.

Як згадувалося раніше, у багатьох практичних задачах розподіл вузлів мережі відрізняється від поля Пуассона (рис. 2.8).

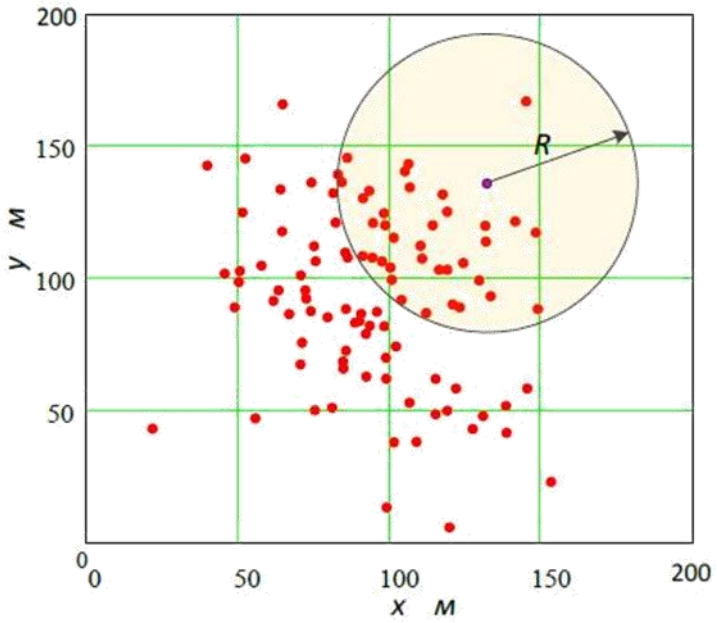


Рис. 2.8. Графічне представлення моделі аналізу бездротової сенсорної мережі при мультимодальному розподілі вузлів

Загалом, вона може бути унімодальною або мультимодальною, з областями високої та низької щільності вузлів. Для вивчення властивостей полів, відмінних від полів Пуассона, розглянемо мережу, що складається з вузлів.

Вона розташована в зоні обслуговування за звичайними правилами, тобто утворює гауссове поле в певній точці на площині. Ця модель зазвичай

використовується, коли вузли мережі нерівномірно розподілені в зоні обслуговування.

2.5. Висновок до розділу 2

Технологія ZigBee дозволяє вирішувати багато різних, не пов'язаних між собою прикладних завдань в межах однієї мережі. Для забезпечення розділення пакетів між різними програмами використовуються 8-бітні ідентифікатори кінцевих точок.

Для забезпечення повної сумісності між пристроями різних виробників та їх взаємодії в межах однієї розподіленої програми технологія ZigBee використовує концепцію профілів, які розрізняються в пакетах даних за допомогою 16-бітних ідентифікаторів. Специфікація описує набір технічних параметрів, домовленостей щодо структури даних та форматів повідомлень, яких виробники повинні суворо дотримуватися, щоб забезпечити відповідність своєї продукції специфікації. Поточний список профілів застосувань, опублікований ZigBee Alliance, включає: домашню автоматизацію, автоматизацію комерційних будівель, роздрібну торгівлю, інтелектуальні мережі, телекомунікації, охорону здоров'я, дистанційне керування, пристрої введення та пристрої керування освітленням.

Щільність вузлів у кожній точці поверхні є випадковою величиною, що задається випадковими незалежними координатами x та y. Функція щільності ймовірності тоді визначається спільною функцією розподілу випадкових x та y

3. РЕАЛІЗАЦІЯ МОДЕЛІ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ ПРИ МУЛЬТИМОДАЛЬНОМУ РОЗПОДІЛІ ВУЗЛІВ

3.1. Архітектура беспровідної сенсорної мережі

У графічному редакторі OMNET++ бездротова сенсорна мережа Castalia представлена наступним чином, що описує бездротову сенсорну мережу (WSN):

- SN - назва мережі, яка використовується для моделювання;
- Wireless Channel - модуль бездротового каналу;
- Node [кількість вузлів] - модуль елемента мережі;
- Physical Trip [кількість фізичних поїздок] - модуль фізичної поїздки.

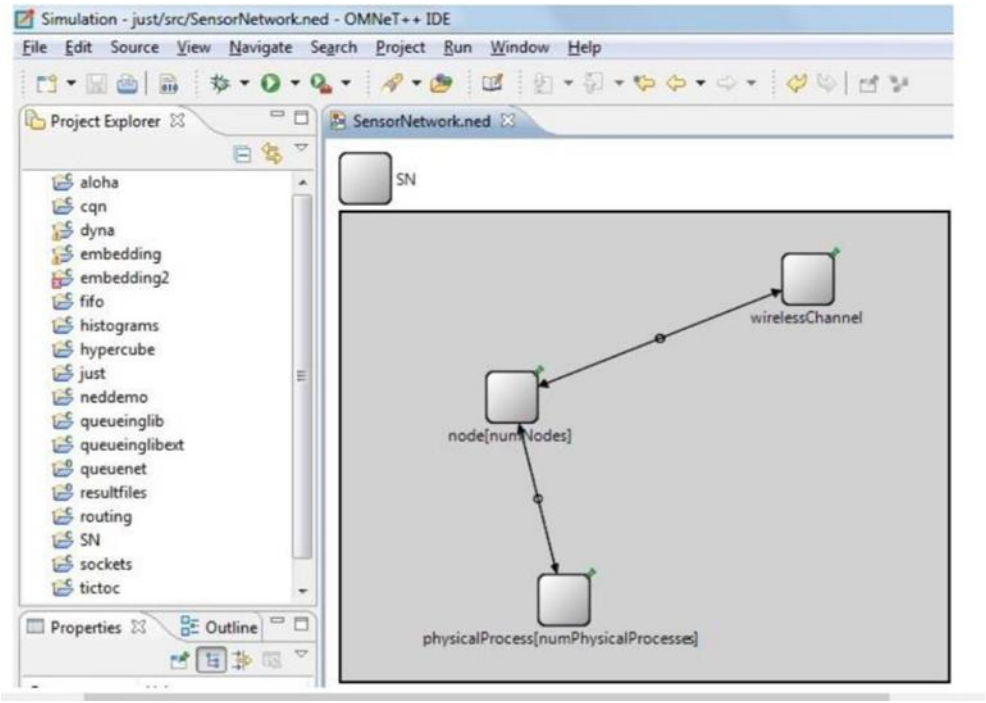


Рис. 3.1. Структура бездротової сенсорної мережі

Node - елемент, що описує кожну станцію, його параметри налаштовуються відповідно до кількості вузлів, що визначає кількість станцій у мережі.

Модулі, що складають станції, що описують модулі вузлів:

- Node - назва мережі (використовується для моделювання);
- Communication - модуль зв'язку;
- Sensor Manager - модуль, що описує кількість датчиків;
- Resource Manager - модуль споживання ресурсів;
- Application - модуль програми;

- Mobility Manager - модуль мобільності вузлів.

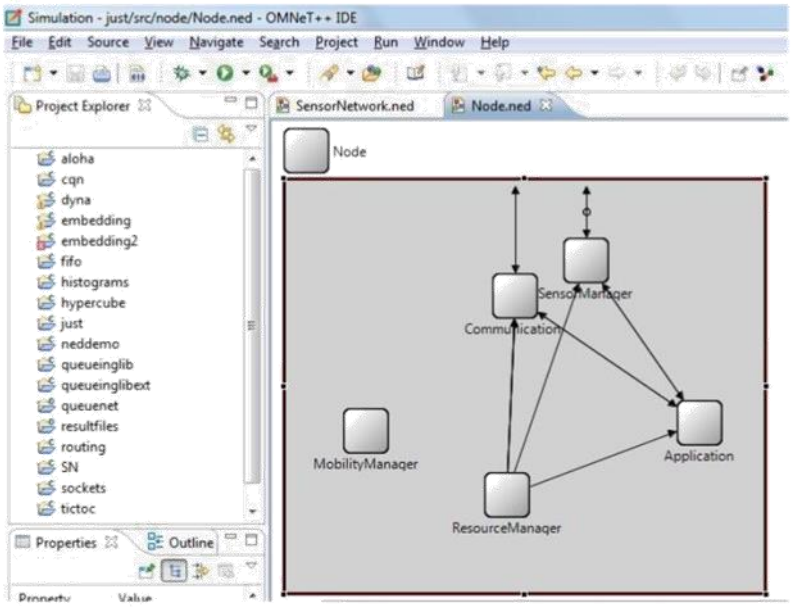


Рис. 3.2. Node Module в структура бездротової сенсорної мережі

Структура модуля зв'язку, що описує комунікацію:

- Радіо - Модуль радіоканалу;

- MAC - Модуль фізичного рівня;

- Маршрутизація - Модуль маршрутизації.

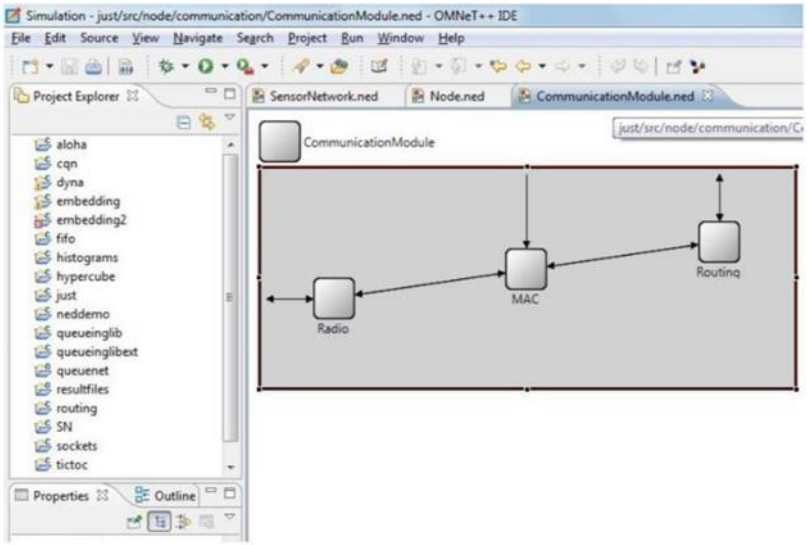


Рис. 3.3. Модуль зв'язку в структура бездротової сенсорної мережі

Зміна або видалення будь-якого елемента може призвести до помилок та неправильного моделювання мережі; всі елементи мережі важливі.

У графічному режимі топологія мережі виглядатиме так:

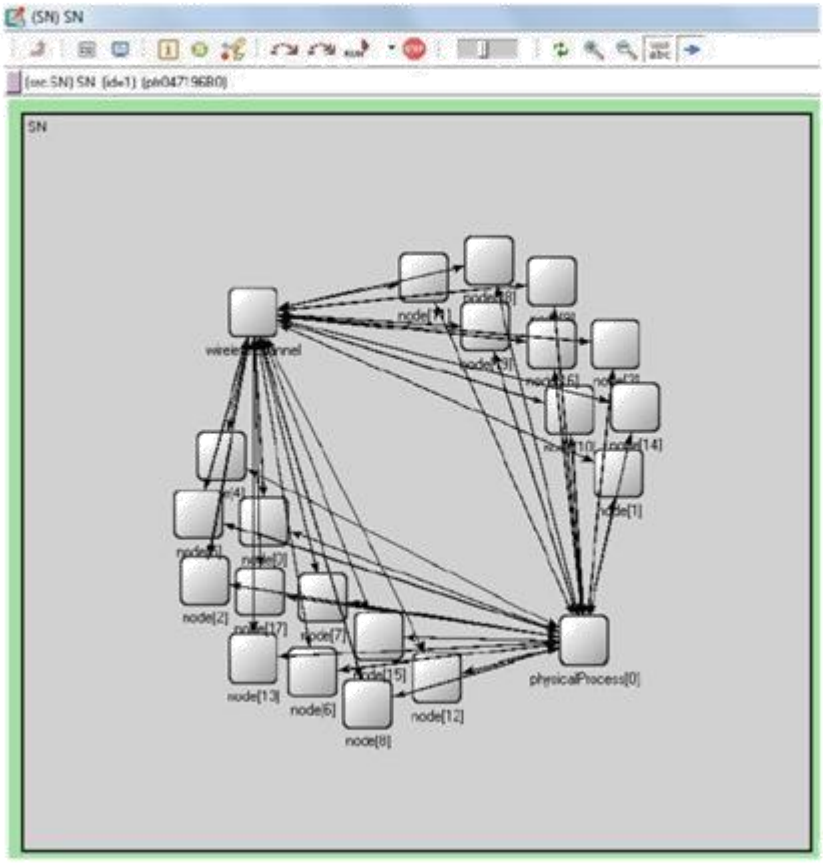


Рис. 3.4. Топологія мережі

Щоб переглянути зібрану статистику, запускаємо скрипт Castalia Results: Castalia Results -igen.txt

Таблиця 3.1. Статистика мережі

Module	**Output**	**Dimensions**
Communication.MAC	Fraction of time with out PAN connection	19x1(3)
	Number of bea consreceived	19x1
	Number of bea conssent	1x1
Communication.Radio	RX pktbreakdown	20x1(5)
	Txedpkts	20x1
ResourceManager	Consumed Energy	20x1
wirelessChannel	Fade depthdistribution	1x1(14)

Після завершення моделювання мережі ми проаналізуємо споживання енергії кожною станцією. Щоб переглянути статистику, введіть у терміналі таку команду: *Castalia -igen.txt -senergy -n*

Таблиця 3.2. Споживання енергії за годину. Менеджер ресурсів: Споживання енергії

node=0	32,756	node=10	24,632
node=1	24,991	node=11	24,632
node=2	24,565	node=12	24,631

node=3	26,5	node=13	24,632
node=4	24,589	node=14	24,632
node=5	25,772	node=15	24,631
node=6	24,632	node=16	24,632
node=7	24,632	node=17	24,632
node=8	24,632	node=18	24,631
node=9	24,631	node=19	24,632

Для зручності ми представимо отримані дані у вигляді графіка:

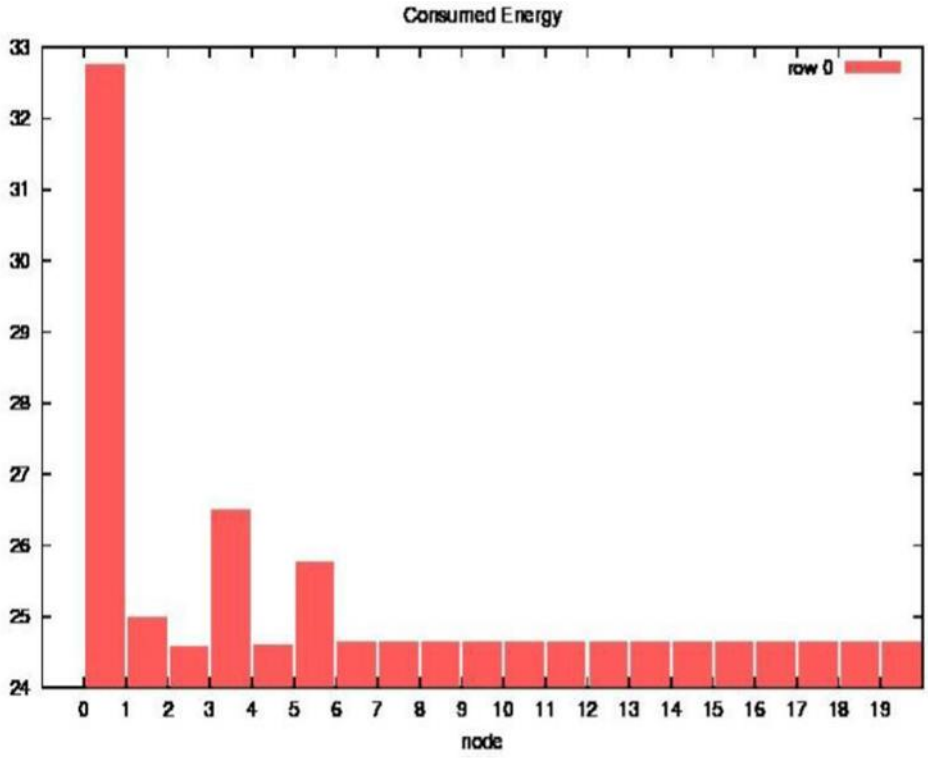


Рис. 3.5. Енергоспоживання бездротової сенсорної мережі при мультимодальному розподілі вузлів

Розрахуємо максимальний час роботи кожного пристрою. Ємність батареї типу AA становить 2122 мАг. Отже, максимальний час роботи (у годинах) кожної станції з використанням двох батарейок типу AA становить:

Таблиця 3.3: Максимальний час роботи

node=0	130	node=10	172
node=1	170	node=11	172
node=2	173	node=12	172
node=3	160	node=13	172
node=4	173	node=14	172
node=5	165	node=15	172
node=6	172	node=16	172
node=7	172	node=17	172
node=8	172	node=18	172

node=9	172	node=19	172

У наших аналітичних моделях і для того, щоб помітити переваги Wake-up Radio Receivers (WuRx) і конфігурації LDC для мультимодального бездротового датчика, зроблені деякі основні припущення:

1. WuRx і основне радіо використовують один канал. Які наслідки передачі з головного радіо виявлені по WuRx. Там, усі SN потребують, крім основного радіо, тільки WuRx, і не передавач пробудження.

2. Обидві радіостанції мають однакову дальність зв’язку.

3. Нам не важлива топологія мережі та протоколи маршрутизації. Ми вважаємо, що SN знає адресу Next Hop для знищення пакетів даних у приймачі.

4. Передане повідомлення даних дуже мало. Там, наскільки це казалося, це входить в пакет пробудження.

. 5. Для того, щоб задовольнити ймовірність, ми розуміємо, що енергетика (Pnode) основного радіо є саме для періодів пробудження та простою, прийому та передачі пакету та перемикання між станами.

6. Для енергетичної оцінки ми припускаємо відсутність втрат пакетів під час зв’язку, тобто безпомилковий канал.

7. Усі SN сплять у режимі LPM4, тобто глибоко функціонуючий режим сну, який не завжди є пробудженим на їх активний період.

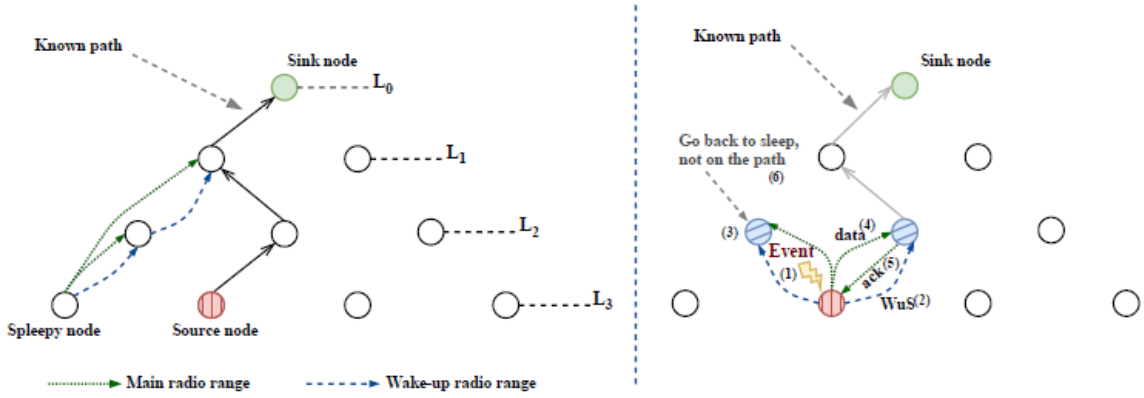


Рис. 3.6. Діаграма багатострибкового зв'язку двох радіоканалів у деревоподібній топології бездротової сенсорної мережі при мультимодальному розподілі вузлів

На правій частині рисунку показано багатострибкову роботу запропонованого протоколу пробудження. Пакети подій поширюються від джерела до приймача через попередньо визначені відомі шляхи маршрутизації.

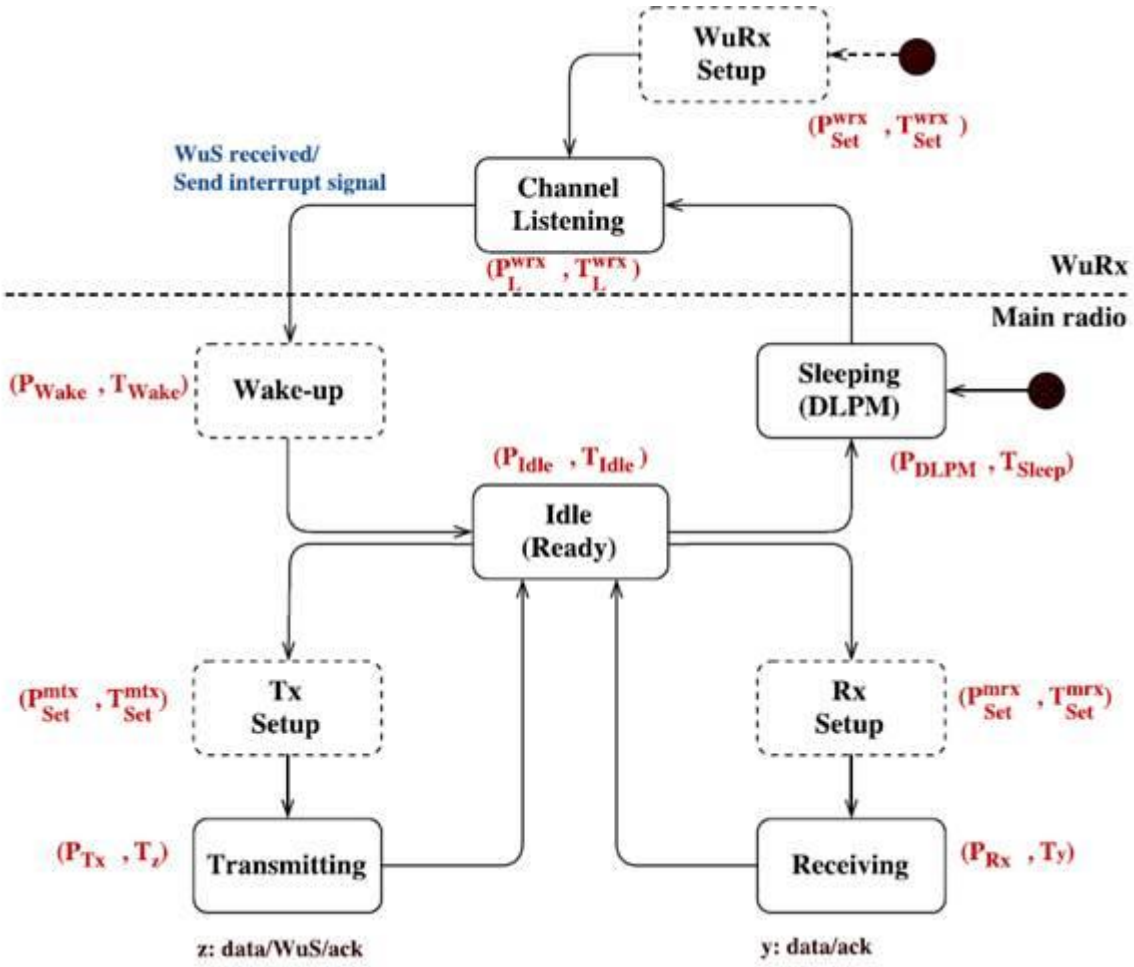


Рис. 3.7. Структура двостанційного радіоканалу у бездротової сенсорної мережі

3.2. Технічна підтримка бездротової сенсорної мережі при мультимодальному розподілі вузлів

Житловий комплекс Мангеттен складається з шести яскраво-помаранчевих 18-, 19- та 20-поверхових багатоквартирних будинків з блакитними пірамідальними дахами. Кожен будинок має вхід. Зовнішні стіни комплексу прикрашені вітражами та стильним декором.

Для нашого дипломного проекту ми обрали модуль Jennic JN5139-Z01-M02 ZigBee, який має вбудований регульований підсилювач потужності для бездротової передачі.

Модулі Jennic, що використовуються для побудови бездротової сенсорної мережі JN513x, являють собою серію недорогих, малопотужних бездротових мікроконтролерів, що відповідають стандартам 802.15.4 та ZigBee. Використання цих модулів дозволяє уникнути дорогого та трудомісткого проектування та тестування друкованих плат. Ці модулі можна підключити до бездротового мікроконтролера Jennic JN5139, щоб забезпечити вам повне та високопродуктивне рішення. Модуль доступний у п'яти апаратних версіях: JN5139-xxx-M00 з вбудованою антеною, JN5139-xxx-M01/M03 з роз'ємом антени та JN5139-xxx-M02/M04 з вбудованим підсилювачем потужності та малошумним підсилювачем (LNA) для зв'язку на великі відстані. Кожну версію можна запрограмувати за допомогою мережевого протоколу ZeeBee (JN5139-xxx-Z01/Myy) [8].

Технічні характеристики модуля далекого радіусу дії: - Діапазон частот: 2,4 ГГц; - Апаратний процесор протоколу MAC; - Дальність зв'язку до 4 км; - Чутливість прийому: -100 дБмВт; - Вихідна потужність передачі: +19 дБмВт; - Розмір модуля: 18x41 мм; - Промисловий діапазон температур: від -20 до +70 °C. Ці модулі встановлені на платі датчиків маршрутизатора DR1048, яка інтегрує датчики температури, вологості та освітлення та має виходи UART0 та UART1, які можна підключити до комп'ютера за допомогою кабелю TTL-232R-3V3 (Рис. 3.8) [8]

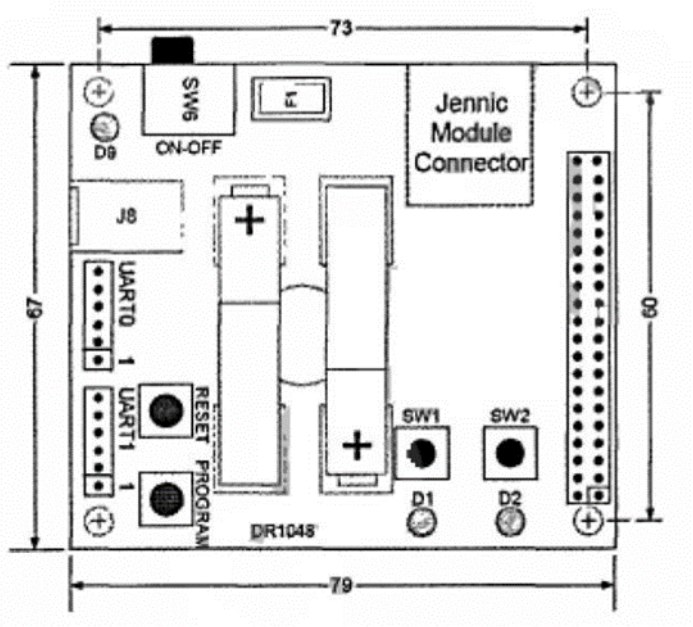


Рис. 3.8. Плата датчиків DR1048

Оцінювальний комплект IEEE802.15.4/Jen Net забезпечує повне середовище для швидкої розробки бездротових комунікаційних програм на основі бездротового мікроконтролера JN5139. Комплект включає все необхідне апаратне та програмне забезпечення для розробки продукту, включаючи п'ять мережевих вузлів, комплект розробки програмного забезпечення, тестові програми та приклади. Бібліотеки, що надаються мережевими рівнями IEEE802.15.4 та Jen Net, підтримують топології типу «зірка», «дерево» та «лінія» до 1000 вузлів та забезпечують самовідновлювальні мережеві функції для надійного зв'язку.

Комплект включає плату контролера, яка виконує роль координатора мережі, та чотири маршрутизовані плати датчиків. Кожна плата розробки містить інтегральну схему JN5139 у компактному модулі підтримки.

3.3. Моделювання бездротової сенсорної мережі при мультимодальному розподілі вузлів

Дах було обрано місцем для розгортання бездротової сенсорної мережі. Ця мережа призначена для використання як мережа доступу, тобто для передачі

даних від базової системи технічного обслуговування до центру управління через командний пункт. Командний пункт оснащений обладнанням супутникового зв'язку SE2Pro, тобто антенами самонаведення. Тобто, дані будуть передаватися від базової системи технічного обслуговування (СТО) до центру управління через супутниковий зв'язок, оскільки це найшвидший спосіб організації зв'язку в складних бойових умовах. Затримка каналу становить 600-800 мілісекунд, швидкість каналу – 4 Мбіт/с (передача), 8 Мбіт/с (прийом). SE2Pro має 4 порти Ethernet для доступу до Інтернету. Два з них використовуються для передачі даних, а два – для телефонного зв'язку. Один з портів передачі даних SE2Pro використовується для організації відеоконференцій, для яких виділяється окремий носій, наприклад, 1 Мбіт/с (передача), 1 Мбіт/с (прийом). Другий порт для передачі даних підключено до 8-портового Microtik. Microtik виділяє окремі порти та окремі VLAN для доступу до Інтернету та передачі даних. Бездротовій сенсорній мережі також призначено окремий порт та VLAN. WSN має швидкість прийому/передачі 512 кбіт/с. Координатор мережі буде встановлено в GSM та підключено до Microtik. Потім усі дані передаються від радіомодулів до координатора, а потім надсилаються в мережу. Радіомодулі з'єднані за допомогою сітчастої топології. Сітчаста топологія дозволяє передавати дані на великі відстані, розділяючи довгі шляхи на кілька коротких шляхів між вузлами. Ця топологія є гнучкою та адаптивною. Тому що, якщо один радіомодуль вийде з ладу, система перебудується на основі поточної ситуації та продовжить роботу (Рис. 3.9).

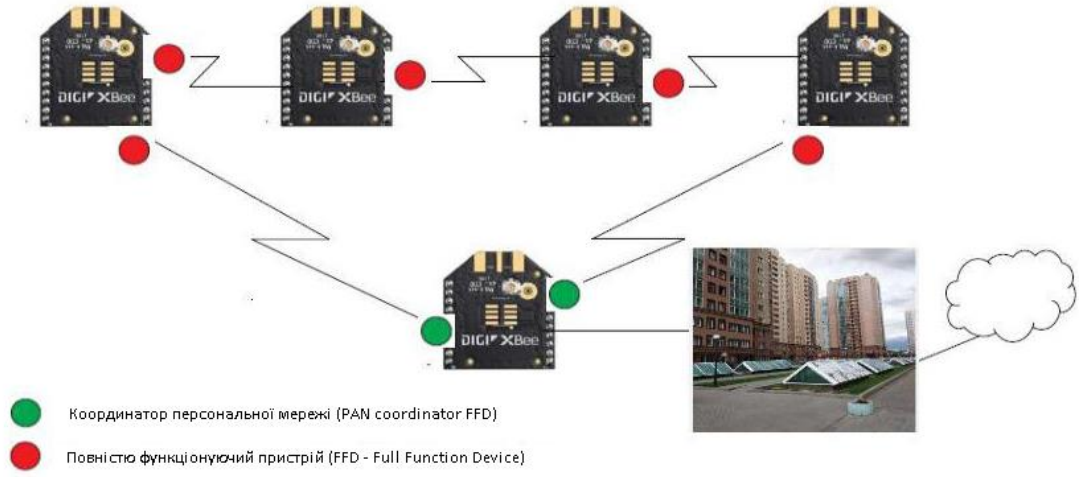


Рис. 3.9. Схема структури бездротової сенсорної мережів в житловому кварталі Манхеттен

Споживання енергії під час передачі даних безпосередньо пов'язане з розміром пакета. Виробник JN5139-Z01-M02 вказує, що струм передачі становить 26,9 мА. При використанні батареї 3 В споживання потужності передачі становить

$$P = UI \tag{3.1}$$

$P=26{,}9*10^{-3}=80{,}7мВт.$

Виробник JN5139-Z01-M02 вказує, що струм прийому становить 26,7 мА. Згідно з рівнянням (4.1), споживання потужності прийому становить

$P=26{,}7*10^{-3}*3=80{,}1мВт$

Струм сну пристрою ZigBee становить 0,5 мкА, а споживання потужності в режимі сну становить

$P=0{,}5*10^{-6}*3=1{,}5мкВт$

Антена, що використовується JN5139-Z01-M02, є чвертьхвильовою антеною з коефіцієнтом посилення 2,2 дБ. Ми використовуємо наступні формули для розрахунку коефіцієнтів посилення передачі та прийому антени (виражених у натуральних числах).

$$G = 10^{\frac{G_{ldd}}{10}} \tag{3.2}$$

$$G = 10^{\frac{2.2}{10}} = 1.667$$

Чутливість приймача визначається як мінімальний вхідний сигнал, який можна успішно декодувати. Чутливість приймача JN5139-Z01-M02 становить -95 дБм. Щоб розрахувати коефіцієнт підсилення (у ватах), використовуйте наступну формулу.

$$P_r = \frac{10^{\frac{P_{дБм}}{10}}}{1000} \quad (3.3)$$

$$P_r = \frac{10^{\frac{-95}{10}}}{1000} = 3{,}1623 \cdot 10^{=13}\text{Вт}$$

Для будь-якої передачі даних вірним є наступне твердження: прийнятий сигнал складається з переданого сигналу, різних спотворень, внесених самою системою передачі, та інших сигналів перешкод, які взаємодіють з вихідною хвилею під час поширення від точки передачі до точки прийому. Ці сигнали перешкод зазвичай називають шумом. Шум є основним фактором, що обмежує продуктивність систем зв'язку.

Верхня межа продуктивності системи зв'язку встановлюється тепловим шумом. Тепловий шум розподіляється по всьому спектру та впливає на передавальні та приймальні пристрої електромагнітних сигналів, а також на середовище передачі.

Спектральна щільність теплового шуму не залежить від частоти, тому його можна розглядати як білий шум у широкому діапазоні частот. Тепловий шум не залежить від частоти, тому щільність потужності шуму на одиницю ширини каналу становить

$$N = kTB[\text{Вт}] \quad (3.4)$$

де k = 1,3803 * 10−23 Дж/К - стала Больцмана;

Т - абсолютна температура в Кельвінах; В - ширина каналу в герцах.

Запишемо формулу для щільності потужності шуму в децибел-ватах.

$$N = 10lgk + 10lgT + 10lgB.[\text{дБВт}] \quad (3.5)$$

Ширина смуги пропускання каналу ZigBee становить 5 МГц. Ми розрахували щільність потужності шуму для стандартного каналу зв'язку ZigBee за стандартних умов, 298K, низьких та високих температур.

$$N = 10\lg(1{,}38 * 10^{-23}) + 10\lg 298 + 10\lg 5 * 10^{6} = -136{,}3[\text{дБВт}]$$
$$N = 10\lg(1{,}38 * 10^{-23}) + 10\lg 323 + 10\lg 5 * 10^{6} = -136[\text{дБВт}]$$
$$N = 10\lg(1{,}38 * 10^{-23}) + 10\lg 223 + 10\lg 5 * 10^{6} = -138[\text{дБВт}]$$

Слід зазначити, що ймовірність імпульсних перешкод висока, а виникнення таких перешкод є випадковим процесом.

Модель вільного простору та модель двопроменевої передачі найкраще підходять для опису рівня сигналу та поширення ліній зв'язку ближньої дії. Однак під час передачі на великі відстані переданий сигнал піддається різним впливам, таким як завмирання та багатопроменевість, які не враховуються першими двома моделями. Тому в цьому випадку більш доречна модель "тінь". Ця модель враховує фактори навколишнього середовища під час передачі даних. У районах з поганою видимістю, якщо є багато перешкод, радіосигнал буде схильний до багатопроменевості.

Під час опису внутрішніх каналів зв'язку ZigBee в зонах з поганою видимістю необхідно враховувати два важливі фактори, що впливають на поширення радіосигналів:

a) Зона покриття мережі ZigBee значно менша, ніж на відкритих майданчиках;

b) Умови поширення радіохвиль у цій зоні більш різноманітні.

Поширення радіохвиль у приміщенні визначається переважно такими параметрами:

- планування будівлі;

- будівельні матеріали;

- тип будівлі.

Потужність сигналу залежить від розташування антени та від того, чи відкриті чи закриті двері. У приміщенні зазвичай є багато перегородок, стін та різних предметів, які суттєво впливають на поширення радіосигналів.

Внутрішні стіни та перегородки зазвичай поділяються на дві категорії: a) «жорсткі» стіни, які є частиною конструкції будівлі; b) «м'які» стіни, які є рухомими перегородками.

Модель «тінь» складається з двох частин. Перша частина називається моделлю втрат на трасі та використовується для прогнозування середнього значення прийнятої потужності відносно потужності на контрольній відстані.

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{\text{дБ}} = -10\beta * log(\frac{d}{d_0}) \quad (3.6)$$

β - коефіцієнт втрат на трасі дорівнює , що визначається експериментально.

Значення коефіцієнта втрат на трасі залежить від зовнішнього середовища. У зонах з поганою видимістю його максимальне значення можна вибрати в діапазоні від 4 до 6. Мінімальне значення дорівнює 2, що вказує на зону без перешкод (табл. 3.4).

Таблиця 3.4. Значення постійної втрат на трасі

Зовнішнє середовище		(постійна втрата)
Відкрита місцевість	Вільне від перешкод	2
	Забудована міська	2,7-5
Закрите приміщення	Прямої видимості	1,6-1,8
	Утруднений	4-6

Розрахуємо значення прийнятої потужності для складних внутрішніх передач, де константа знаходиться в діапазоні від 4 до 6.

Для оцінки якості тракту передачі датчиків ZigBee при розміщенні обладнання підстанції ми розрахували відношення прийнятої потужності до опорної потужності, що відповідає комплексній зоні видимості та зоні прямої видимості.

Використовуючи мережу ZigBee в житлових будівлях передача даних можлива в зоні прямої видимості та комплексній зоні видимості, оскільки ці будівлі можуть отримувати дані від центрального координатора.

На основі розрахованого відношення прийнятої потужності до опорної потужності побудовано графік залежності цього показника від відстані.

З рис. 3.10 видно, що відношення прийнятої потужності до опорної потужності в комплексній зоні видимості більше, ніж у зоні прямої видимості. Для зони з поганою видимістю значення загасання на відстані 40 метрів

становить -90 дБм, тоді як значення загасання в зоні прямої видимості становить -30 дБм.

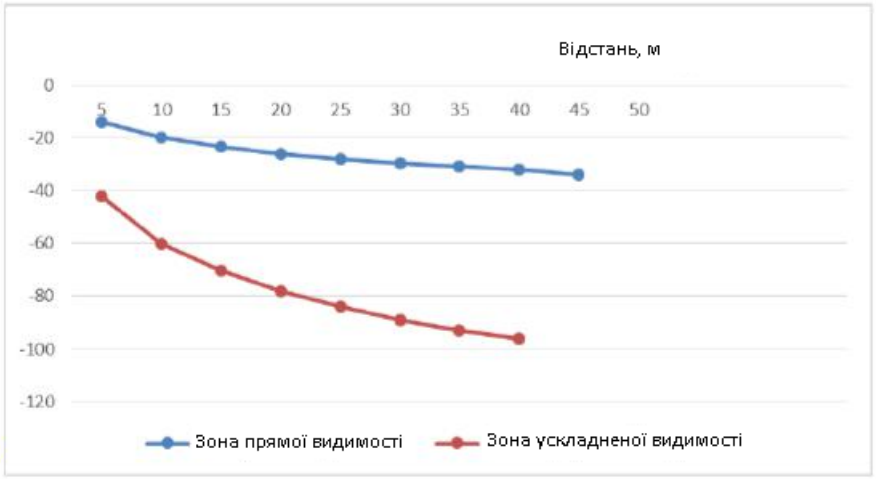


Рис. 3.10. Залежність прийнятої потужності від потужності на контрольній відстані

Затухання радіосигналу під час його поширення від передавача до приймача залежить від частоти передачі, відстані між модулями та значення нульової гаусової змінної.

Ми розраховуємо затухання за такою формулою:

$$\overline{P_L(d_0)} = 20log_{10}(f_{MHz}) + 10\beta log(d) - 28 + N(0, \sigma_{ch}^2) \quad (3.7)$$

де f_{MHz} представляє частоту модуля, що еквівалентно -2400 МГц;

Допустима відстань між внутрішніми модулями становить 50 метрів.

$$\overline{P_L(d_0)} = 20log_{10}(2405) + 10 * 2log(1) - 28 + 1 = 40(\text{дБ})$$

Вважаючи нульову гаусову змінну (0, $h2$) рівною 1 (заводська, обмежена видимість), = 2, затухання на контрольній відстані можна розрахувати за такою формулою:

$$P_L(d) = \overline{P_L(d_0)} + 10\beta log\left(\frac{d}{d_0}\right) - 28 + N(0, \sigma_{ch}^2) \quad (3.8)$$

Після врахування затухання, спричиненого перешкодами, ми використовуємо таку формулу для розрахунку логарифмічно-нормального розподілу втрат на маршруті.

Цей розрахунок дає лише приблизне значення втрат на трасі, оскільки характеристики шляху поширення радіосигналу, тип перешкод та їх розмір не

враховуються. Тому під час передачі даних необхідно враховувати багатопроменеве поширення.

Розрахунок затухання на трасі передачі (з урахуванням затухання, спричиненого перешкодами) чітко показує, що при поширенні в зонах з поганою видимістю сигнал зазнає багаторазових відбиттів та поглинань. Тому на відстані 30 м затухання сигналу досягає 70 дБ (Таблиця 3.5).

Таблиця 3.5. Затухання на мкршруті передачі сигналу

Відстань між передавачем та приймачем, м	**Згасання на маршруті з урахуванням послаблень за рахунок перешкод, дБ**
5	55
10	61
15	64,52
20	67
25	68,96
30	70,54
35	71,88
40	73,04
45	74,06

Як видно з графіка на рисунку 3.9, затухання на тракті передачі з урахуванням затухання, спричиненого перешкодами, досягає 75 дБ на відстані 45 метрів. При використанні системи передачі даних ZigBee на підстанції з поганою видимістю рівень прийнятої потужності може бути низьким навіть на відстані 10-15 метрів.

Рис. 3.11. Затухання на тракті після врахування затухання, спричиненого перешкодами

Для розрахунку співвідношення сигнал/шум (SNR) на вході приймача використовуємо наступну формулу.

$$\gamma(d) = N(\overline{P_t}, \sigma_t^2) - P_L(d) - N(\overline{P_n}, \sigma_n^2), \text{дБ} \quad (3.9)$$

де $\overline{P_t}$ - середня (номінальна) вихідна потужність передавача (дБм);

σ_t^2 - дисперсія вихідної потужності;

$\overline{P_n}$ - середній (номінальний) рівень шуму приймача (дБм);

σ_n^2 - дисперсія рівня шуму

У таблиці 3.6 наведено значення, отримані при розрахунку співвідношення сигнал/шум на вході приймача на різних відстанях між модулями.

Таблиця 3.6. Значення співвідношення сигнал/шум на вході приймача

Відстань між передавачем та приймачем, м	**Відношення сигнал-шум (ВСШ) на вході приймача, дБ.**
5	41,5
10	35,5
15	31,98
20	29,5
25	27,54
30	25,96
35	24,62
40	23,46
45	22,5

На рис. 3.12 показано зв'язок між співвідношенням сигнал/шум та відстанню. Як видно з рисунка, співвідношення сигнал/шум різко падає зі збільшенням відстані та становить близько 22 дБ на 45 метрах, що відповідає нижчій якості зв'язку.

Ми побудували модель бездротової сенсорної мережі ZigBee у графічному редакторі Manhattan LCD OMNET++ та розрахували споживання енергії кожною станцією. Як радіомодуль ZigBee було обрано Jennicc JN5139-Z01-M02, а як координатор мережі – JN5139. Ми розглянули його основні технічні характеристики та функції архітектуру бездротової сенсорної мережі IoT. Ця топологія мережі є mesh-мережею. Унікальність сітчастої топології полягає в тому, що радіомодулі можуть взаємодіяти один з одним без координатора, тобто без центрального шлюзу, що робить мережу гнучкою та адаптивною в реальних

умовах експлуатації. Якщо один з радіомодулів вийде з ладу, мережа продовжить роботу та оновлювати канали маршрутизації.

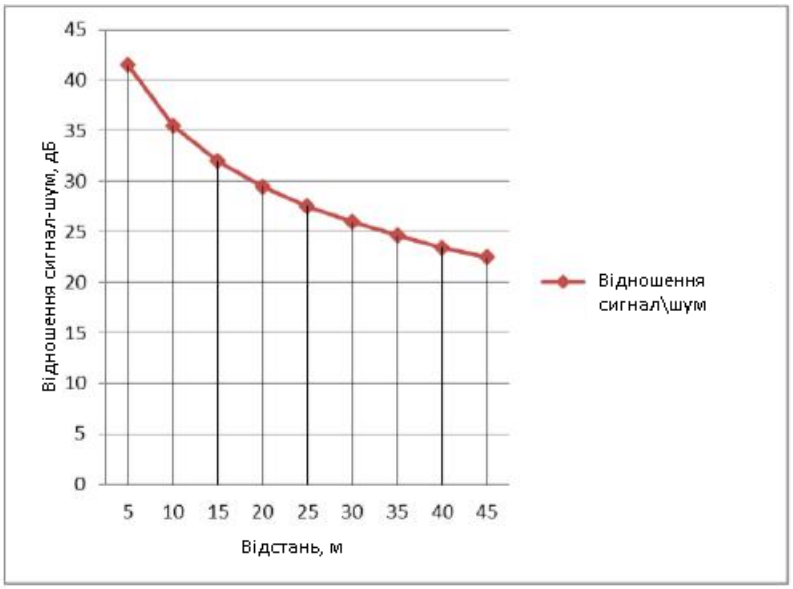


Рис. 3.12. Зв'язок між співвідношенням сигнал/шум та відстанню

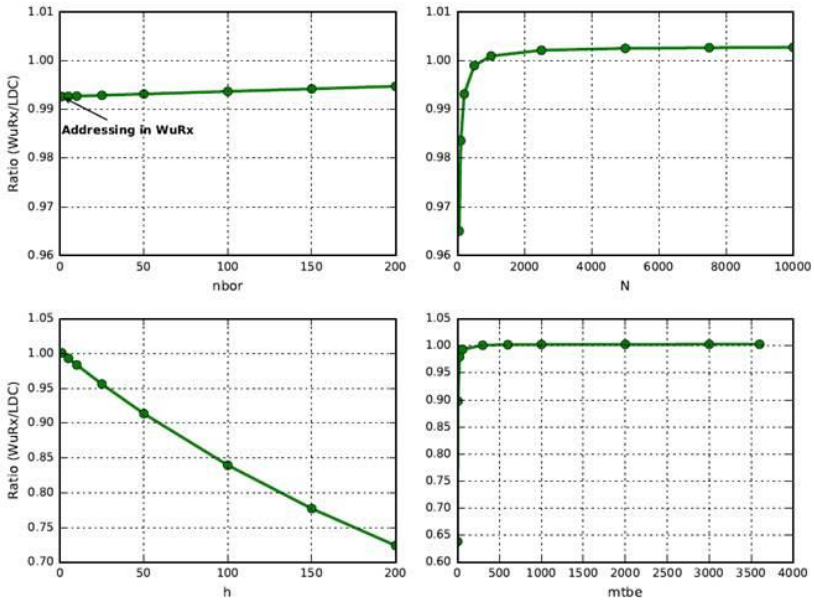


Рис. 3.13. Загальний коефіцієнт споживання енергії при двох рішеннях бездротових сенсорних мереж та використанні різних ресурсів

Криві на рис. 3.13 отримані шляхом зміни тих самих параметрів в обох моделях. Крім того, це дослідження базується на третьому сценарії, тобто mtbe = 60 секунд, Tsleep = 10 секунд. Для кожного значення параметра розраховується споживання енергії кожною моделлю, а вісь у представляє співвідношення, тобто споживання енергії моделлю на основі WuRx/споживання енергії моделлю

на основі LDC. Отже, якщо співвідношення менше за 1, споживання енергії моделлю на основі WuRx менше, ніж моделлю на основі LDC, і навпаки.

3.5. Висновок до розділу 3

У розрахунковій частині ми розрахували споживання енергії радіомодулями в режимі прийому та передачі, режимі сну, а також розрахували шум під час поширення сигналу, щоб отримати співвідношення сигнал/шум, яке відображає фактичний рівень сигналу на певній відстані. Для розрахунку дальності зв'язку ми обрали модель "тінь", яка враховує різні ефекти, такі як завмирання та багатопроменеве поширення.

ВИСНОВКИ

У бакалаврській кваліфікаціній роботі досліджується можливість використання бездротових мереж ZigBee для передачі даних з різних датчиків у житловому районі на Мангеттені з базової станції системи моніторингу параметрів.

Для досягнення цієї мети ми вибрали бездротові модулі, координатори мережі та точки доступу до мережі, побудували модель бездротової сенсорної мережі (WSN) ZigBee та намалювали схему підключення бездротових модулів.

У розрахунковій частині ми розрахували споживання енергії бездротовим модулем в режимі передачі/прийому, режим сну та шум під час процесу поширення сигналу, щоб отримати співвідношення сигнал/шум, яке відображає фактичну силу сигналу на певній відстані. Для розрахунку дальності зв'язку ми обрали модель "тінь", яка враховує різні ефекти, такі як завмирання та багатопроменеве поширення.

Впровадження технології Інтернету речей принесло великі переваги для збору інформації. У військовій галузі Інтернет речей - це мережа взаємопов'язаних об'єктів або "речей", які безперервно спілкуються, координують, навчаються та взаємодіють з фізичним середовищем для виконання різних операцій більш ефективним та інтелектуальним способом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Belej O., Lohutova T., Halkiv L. (2021) Development of Evaluation Templates for the Protection System of Wireless Sensor Network. In: Ageyev D., Radivilova T., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham. https://doi.org/10.1007/978-3-030-71892-3_10

2. O. Belej, N. Nestor, I. Artyshchuk, K. Pytel, N. Spas and M. Polietaiev, "The Formation of Computer Cluster with Limited Computing Resources Based on an Arbitrary Neural Network," 2024 IEEE 19th International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), Zozuli, Ukraine, 2024, pp. 132-136, doi: 10.1109/MEMSTECH63437.2024.10620061.

3. O. Belej, Y. Fedirko, O. Markelov, I. Yurchak, M. Lobur and O. Peretiatko, "The Monitoring of Automated Platforms for Testing Internet of Things Devices," 2024 IEEE 19th International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), Zozuli, Ukraine, 2024, pp. 137-141, doi: 10.1109/MEMSTECH63437.2024.10620012.

4. Belej, O., Fedirko, Y., Markelov, O. Ensuring accuracy of personal data processed in blockchain systems. (2024) CEUR Workshop Proceedings, 3723, pp. 13-41. - CEUR Workshop Proceedings, Volume 3723, Pages 13 – 41, 2024, 6th International Workshop on Modern Data Science Technologies Workshop, MoDaST 2024, Lviv, 31 May 2024 through 1 June 2024, Code 200872 –https://ceur-ws.org/Vol-3723/paper2.pdf – Scopus

5. O. Belej, N. Nestor and N. Spas, "Building a Model of Fault Tolerance of Serial-Parallel Ports in a Self-Synchronous Microkernel," 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/TCSET64720.2024.10755721. - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10755721&isnumber=10755510

6. O. Belej, I. Artyshchuk and M. Kutelmakh, "The Technology for Countering the Threats of Violation in the Information Security of Cloud Infrastructure," 2024 IEEE 19th International Conference on Computer Science and Information Technologies (CSIT), Lviv, Ukraine, 2024, pp. 1-5, doi: 10.1109/CSIT65290.2024.10982655

7. O. Belej FORMATION OF WIRELESS SENSOR NETWORK PROTECTION SYSTEM PARAMETERS FOR INTRUSION DETECTION IN THE FORM OF FALSE EVENT FLOWS - Artificial Intelligence. 2023. № 1: c. 123-137 - DOI: 10.15407/jai2023.01.123 - http://jai.in.ua/index.php/en/issues?paper_num=1574 - https://orcid.org /0000-0003-4150-7425

8. O. Belej, N. Nestor, I. Artyshchuk and N. Spas, "Modeling of Wireless Sensor Network Based on Functioning Parameters of Unevenly Distributed Nodes," 2023 17th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Jaroslaw, Poland, 2023, pp. 23-27, doi: 10.1109/CADSM58174.2023.10076512

9. F. Z. Djiroun and D. Djenouri, “MAC protocols with wake-up radio for wireless sensor networks: A review,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 587-618, 2017.

10. R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, “Ultra low power wake-up radios: A hardware and networking survey,” *IEEE Communications Surveys Tutorials* , vol. PP, no. 99, pp. 1-1, 2017.

11. J. Aranda, H. Carrillo, and D. Mendez, “Enhanced multimodal switching mechanisms for node scheduling and data gathering in wireless sensor networks,” in *2017 IEEE Colombian Conference on Communications and Computing (COLCOM),* Aug 2017, pp. 1-6.

12. J. Aranda , M. Schölzel, D. Mendez , andH. Carrillo , “An energy consumption model for multimodal wireless sensor networks based on wake-up radio receivers,” in *2018 IEEE Colombian Conference on Communications and Computing (COLCOM),* May 2018, pp. 1-6.

13. T. Kumberg, M. Schink, L. M. Reindl, and C. Schindelhauer, “T-ROME: A simple and energy efficient tree routing protocol for low-power wake-up receivers,” *Ad Hoc Networks*, vol. 59, pp. 97-115, 2017.

14. J. Oller, I. Demirkol, J. Casademont, J. Paradells, G. U. Gamm, and L. Reindl, “Has Time Come to Switch from Duty-Cycled MAC Protocols to Wake-Up Radio for Wireless Sensor Networks?” *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 674-687, 2016.

15. N. Seyed Mazloum and O. Edfors, “Influence of Duty-Cycled Wake-Up Receiver Characteristics on Energy Consumption in Single-Hop Networks,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3870-3884, 2017.

16. M. Lont, D. Milosevic, P. G. M. Baltus, A. H. M. Van Roermund, and G. Dolmans, “Analytical models for the wake-up receiver power budget for wireless sensor networks,” *GLOBECOM - IEEE Global Telecommunications Conference*, 2009.

17. Y. Zhang, L. Huang, G. Dolmans , and H. de Groot, “An analytical model for energy efficiency analysis of different wakeup radio schemes,” *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications,* 2009, pp. 1148-1152.

18. M. Zhang, D. Ghose, and F. Y. Li, “Does wake-up radio always consume lower energy than duty-cycled protocols?” in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall),* Sept 2017, pp. 1-5.

19. R. Piyare , T. Istomin, andA. L. Murphy , “WaCo: A Wake-Up Radio COOJA Extension for Simulating Ultra Low Power Radios,” in *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. USA: Junction Publishing, 2017, pp. 48-53.

20. M. Al Ameen, N. Ullah, M. S. Chowdhury, S. R. Islam, and K. Kwak, “A power efficient MAC protocol for wireless body area networks,” EURASIP *Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 33, 2012.

21. M.-P. Uwase, M. Bezunartea, J. Tiberghien, J.-M. Dricot, and K. Steenhaut, “Experimental Comparison of Radio Duty Cycling Protocols for Wireless Sensor Networks,” *IEEE Sensors Journal*, vol. 17, no. 19, pp. 6474-6482, 2017.

22. Kareemulla S, Khasim S. 2024. IOT communication technologies. In: AI for Climate Change and Environmental Sustainability. Boca Raton, Florida, USA: CRC Press, 75–87.

23. Kasat K, Shaikh N, Rayabharapu VK, Nayak M, Liyakat KKS. 2023. Implementation and recognition of waste management system with mobility solution in smart cities using Internet of Things. In: 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). Piscataway: IEEE, 1661–1665.

24. Khalique A, Siddiqui F, Ahad MA, Hussain I. 2024. Towards trustworthy urbanization: security and privacy objectives for sustainable smart city. In: International Conference on ICT for Digital, Smart, and Sustainable Development. Cham: Springer, 349–365.

25. Krishnan SR, Nallakaruppan M, Chengoden R, Koppu S, Iyapparaja M, Sadhasivam J, Sethuraman S. 2022. Smart water resource management using artificial intelligence—a review. Sustainability 14(20):13384 DOI 10.3390/su142013384.

26. Kumar A. 2024. A novel framework for waste management in smart city transformation with industry 4.0 technologies. Research in Globalization 9:100234 DOI 10.1016/j.resglo.2024.100234.

27. Kumar A, Sharma S, Singh A, Alwadain A, Choi B-J, Manual-Brenosa J, Ortega-Mansilla A, Goyal N. 2022. Revolutionary strategies analysis and proposed system for future infrastructure in Internet of Things. Sustainability 14(1):71 DOI 10.3390/su14010071.

28. Kurniawan TA, Othman MHD, Liang X, Goh HH, Gikas P, Kusworo TD, Anouzla A, Chew KW. 2023. Decarbonization in waste recycling industry using digitalization to promote net-zero emissions and its implications on sustainability. Journal of Environmental Management 338(12):117765 DOI 10.1016/j.jenvman.2023.117765.

29. Linke IHJ. Full speed towards transport transition? Sustainability assessment of urban transport developments in Vienna and Berlin M.Sc. Audrey Bourgoin Master thesis. Technical University of Darmstadt.

30. Mahbub M. 2020. A smart farming concept based on smart embedded electronics, internet of things and wireless sensor network. Internet of Things 9(1):100161 DOI 10.1016/j.iot.2020.100161.

31. Mahor V, Rawat R, Kumar A, Garg B, Pachlasiya K. 2023. IoT and artificial intelligence techniques for public safety and security. In: Smart Urban Computing Applications. River Publishers, 111–126. Manickam S, Kooy A. 2020. Internet of things for smart cities: challenges, security and privacy issues. Security and Privacy Issues (October 17, 2020).

32. Masood F, Khan WU, Jan SU, Ahmad J. 2023. AI-enabled traffic control prioritization in software-defined IoT networks for smart agriculture. Sensors 23(19):8218 DOI 10.3390/s23198218.

ДОДАТОК А

```
[General]
network = WiredAndWirelessHostsWithAP
sim-time-limit = 400s
tkenv-plugin-path = ../../../etc/plugins

**.addDefaultRoutes = false

**.*Host*.numUdpApps = 3

**.*Host*.udpApp[0].typename = "UDPEchoApp"
**.*Host*.udpApp[0].localPort = 1000

**.*Host*.udpApp[*].typename = "UDPBasicApp"
**.wiredHost1.udpApp[1].destAddresses = "wirelessHost1"
**.wiredHost1.udpApp[2].destAddresses = "wiredHost2"
**.wiredHost2.udpApp[1].destAddresses = "wirelessHost1"
**.wiredHost2.udpApp[2].destAddresses = "wiredHost1"
**.wirelessHost1.udpApp[1].destAddresses = "wiredHost1"
**.wirelessHost1.udpApp[2].destAddresses = "wiredHost2"
**.*Host*.udpApp[1..].destPort = 1000
**.*Host*.udpApp[1..].messageLength = 100B
**.*Host*.udpApp[1..].sendInterval = 1s
**.*Host*.udpApp[1..].stopTime = 300s

**.initialZ = 0



//
// This program is property of its copyright holder. All rights reserved.
//

package inet.examples.wireless.wiredandwirelesshostswithap;

import inet.networklayer.configurator.ipv4.IPv4NetworkConfigurator;
import inet.node.ethernet.Eth100M;
import inet.node.inet.Router;
import inet.node.inet.StandardHost;
import inet.node.inet.WirelessHost;
import inet.node.wireless.AccessPoint;
import inet.physicallayer.ieee80211.packetlevel.Ieee80211ScalarRadioMedium;
import inet.visualizer.integrated.IntegratedCanvasVisualizer;

network WiredAndWirelessHostsWithAP
{
    @display("bgb=500,300");
    submodules:
        visualizer: IntegratedCanvasVisualizer {
            parameters:
```

```
            @display("p=100,50");
        }
        configurator: IPv4NetworkConfigurator {
            parameters:
                assignDisjunctSubnetAddresses = false;
                @display("p=100,150");
        }
        radioMedium: Ieee80211ScalarRadioMedium {
            parameters:
                @display("p=100,250");
        }
        wirelessHost1: WirelessHost {
            parameters:
                @display("p=62,69");
        }
        wiredHost1: StandardHost {
            parameters:
                @display("p=296,134");
        }
        wiredHost2: StandardHost {
            parameters:
                @display("p=412,70");
        }
        router: Router {
            parameters:
                @display("p=296,69");
        }
        accessPoint: AccessPoint {
            parameters:
                @display("p=205,69");
        }
    connections:
        accessPoint.ethg++ <--> Eth100M <--> router.ethg++;
        wiredHost1.ethg++ <--> Eth100M <--> accessPoint.ethg++;
        wiredHost2.ethg++ <--> Eth100M <--> router.ethg++;
}
```

```
        #!/bin/sh
        # the next line restarts using wish (on cygwin, use wish84 or the like) \
        exec wish "$0" "$@"

#==========================================================================
        #  DEMO
        #  part of OMNeT++
#==========================================================================

        #----------------------------------------------------------
        #  Copyright (C) 1992-2003 Andras Varga
        #
        #  This file is distributed WITHOUT ANY WARRANTY. See the file
        #  `license' for details on this and other legal matters.
        #----------------------------------------------------------


        #
        # Configuration
        #
        set wantScrollbar 1
        set unixbrowser "firefox"
        #set unixbrowser "mozilla"
        #set unixbrowser "konqueror"
        #set unixbrowser "netscape"

        #
        # title line:   {"title"}
        # program line: {"name" "directory" "unix-command" "windows-command"}
        # readme line:  {"name" "readme-file"}
        # docu line:    {"name" "readme-file"  "html-file"}
        # separator:    {}
        #
        set i 0
        set first ""
        foreach line {
          {"INET Framework"}
          {"About..."              "README"              "../doc/index.html"}

          {"Ethernet"}
          {"ARP Test"              "ethernet/arptest"     "./run"              "run"}
          {"ARP Test 2"            "ethernet/arptest2"    "./run"              "run"}
          {"LANs: mixed Ethernet"  "ethernet/lans"        "./run mixed.ini"    "run mixed.ini"}
          {"LANs: Ethernet bus"    "ethernet/lans"        "./run bus.ini"      "run bus.ini"}
          {"LANs: hub"             "ethernet/lans"        "./run hub.ini"      "run hub.ini"}
          {"LANs: switch"          "ethernet/lans"        "./run switch.ini"   "run switch.ini"}
          {"LANs:  duplexswitch"           "ethernet/lans"                 "./run  duplexswitch.ini"  "run
duplexswitch.ini"}
          {"LANs: two hosts"       "ethernet/lans"        "./run twoHosts.ini"  "run twoHosts.ini"}
          {"LANs: very large LAN"  "ethernet/lans"        "./run largeNet.ini"  "run largeNet.ini"}

          {"INET"}
          {"NClients/Telnet"       "inet/nclients"        "./run"              "run"}
```

```
  {"NClients/HTTP"          "inet/nclients" "./run basicHTTP.ini"       "run basicHTTP.ini"}
  {"NClients/file transfer" "inet/nclients" "./run filetransfer.ini"    "run filetransfer.ini"}
  {"FlatNet"               "inet/flatnet"        "./run"              "run"}
  {"KIDSNw1"                "inet/kidsnw1"        "./run"              "run"}
  {"Multicast"             "inet/multicast"      "./run"              "run"}
  {"RouterPerf"             "inet/routerperf"     "./run"              "run"}
  {"BulkTransfer"           "inet/bulktransfer"   "./run"              "run"}
  {"RedTest"               "inet/redtest"        "./run"              "run"}
  {"TcpSack"                "inet/tcpsack"        "./run"              "run"}
  {"TcpTimestamps"          "inet/tcptimestamps"  "./run"              "run"}
  {"TcpWindowScale"         "inet/tcpwindowscale" "./run"              "run"}
  {"TcpClientServer"        "inet/tcpclientserver" "./run"             "run"}
  {"BER"                   "inet/ber"            "./run"              "run"}

  {"IPv6 (work in progress)"}
  {"NClients"               "ipv6/nclients"       "./run"              "run"}
  {"DemoNetworkEth"         "ipv6/demonetworketh" "./run"              "run"}
  {"Mobile IPv6"            "ipv6/mobileipv6"     "./run"              "run"}

  {"SCTP"}
  {"NClients"               "sctp/nclients"       "./run"              "run"}
  {"Multi-homing"           "sctp/multihomed"     "./run"              "run"}

  {"Emulation"}
  {"Traceroute"             "emulation/traceroute" "./run"             "run"}
  {"ExtClient"              "emulation/extclient" "./run"              "run"}
  {"ExtServer"              "emulation/extserver" "./run"              "run"}

  {"Ad-hoc"}
  {"Mobility models"        "adhoc/mobility"      "./run"              "run"}
  {"802.11b ad-hoc"         "adhoc/ieee80211"     "./run"              "run"}
  {"802.11b ad-hoc (MF impl.)" "adhoc/mf80211"    "./run"              "run"}

  {"Wireless"}
  {"802.11 AP and hosts"    "wireless/lan80211"   "./run"              "run"}
  {"802.11 handover"        "wireless/handover"   "./run"              "run"}
  {"802.11 thruput test"    "wireless/throughput" "./run"              "run"}
  {"802.11 thruput test 2" "wireless/hosttohost"  "./run"              "run"}

  {"MPLS/RSVP-TE"}
  {"TestTE/failure"         "mpls/testte_failure" "./run"              "run"}
  {"TestTE/reroute"         "mpls/testte_reroute" "./run"              "run"}
  {"TestTE/routing"         "mpls/testte_routing" "./run"              "run"}
  {"TestTE/tunnel "         "mpls/testte_tunnel"  "./run"              "run"}
  {"LDP/test"               "mpls/ldp"            "./run"              "run"}
  {"Net37"                 "mpls/net37"          "./run"              "run"}

  {"OSPFv2"}
  {"SimpleTest"             "ospfv2/simpletest"   "./run"              "run"}
  {"Areas"                 "ospfv2/areas"        "./run"              "run"}
  {"Backbone"               "ospfv2/backbone"     "./run"              "run"}
  {"FullTest"               "ospfv2/fulltest"     "./run"              "run"}
} {
```

```
            lappend samples $i
            if {[llength $line]==0} {
               set db($i,type) "spacer"
            } elseif {[llength $line]==1} {
               set db($i,type) "heading"
               set db($i,title) [lindex $line 0]
            } elseif {[llength $line]==2} {
               set db($i,type) "readme"
               set db($i,title) [lindex $line 0]
               set db($i,readme) [lindex $line 1]
               if {$first==""} {set first $i}
            } elseif {[llength $line]==3} {
               set db($i,type) "docu"
               set db($i,title) [lindex $line 0]
               set db($i,readme) [lindex $line 1]
               set db($i,docu) [lindex $line 2]
               if {$first==""} {set first $i}
            } elseif {[llength $line]==4} {
               set db($i,type) "program"
               set db($i,title) [lindex $line 0]
               set db($i,dir)   [lindex $line 1]
               set db($i,uprog) [lindex $line 2]
               set db($i,wprog) [lindex $line 3]
               if {$first==""} {set first $i}
            } else {
               tk_messageBox -title {Error} -type ok -icon error -message "Error in table: wrong #items
in {$line}"
               exit
            }
            incr i
         }


         proc createWindow {} {
            global wantScrollbar samples first db fonts colors

            wm focusmodel . passive
            wm minsize . 1 1
            wm overrideredirect . 0
            wm resizable . 1 1
            wm deiconify .
            wm title . "OMNeT++ Demo Simulations"
            wm protocol . WM_DELETE_WINDOW {exit}
            wm geometry . "650x400"

            ###################################
            # Menu bar
            ###################################

            menu .menubar
            . config -menu .menubar

            # Create menus
```

```
foreach i {
   {filemenu     -label File -underline 0}
   {helpmenu     -label Help -underline 0}
} {
   eval .menubar add cascade -menu .menubar.$i
   menu ".menubar.[lindex $i 0]" -tearoff 0
}

# File menu
foreach i {
  {command -command exit -label Exit -underline 1}
} {
  eval .menubar.filemenu add $i
}

# Help menu
foreach i {
  {command -command helpAbout -label {About OMNeT++} -underline 0}
} {
  eval .menubar.helpmenu add $i
}

###################################
# Create main display area
###################################

frame .sel -bd 2 -relief groove
frame .main -bd 2 -relief groove
pack .sel -expand 0 -fill y  -side left -padx 2
pack .main -expand 1 -fill both  -side right  -padx 2

frame .main.up
frame .main.lo
frame .main.mid
pack .main.up -expand 0 -fill x  -side top
pack .main.lo -expand 0 -fill x  -side bottom
pack .main.mid -expand 1 -fill both -side top

label .main.up.banner -bg $colors(banner) -relief groove  -font $fonts(bold)
pack .main.up.banner -fill x -side top

text .main.mid.text -yscrollcommand ".main.mid.sb set" -width 80 -height 20  -wrap none
scrollbar .main.mid.sb -command ".main.mid.text yview"
pack .main.mid.sb -anchor center -expand 0 -fill y  -side right
pack .main.mid.text -anchor center -expand 1 -fill both -side left

button .main.lo.start -font $fonts(bold) -bg $colors(startbutton)
pack .main.lo.start -expand 1 -fill x  -padx 10 -pady 6

canvas .sel.c -width 200
pack .sel.c -side left -expand yes -fill both
if {$wantScrollbar} {
    .sel.c config -yscrollcommand ".sel.s set"
```

```
            scrollbar .sel.s -command ".sel.c yview"
            pack .sel.s -side right -fill y
          }
          frame .sel.c.f
          .sel.c create window 0 0 -anchor nw -window .sel.c.f
          set f .sel.c.f

          #label $f.banner -text "Sample simulations:" -bg $colors(banner) -relief groove -font
$fonts(bold)
          #pack $f.banner -fill x -side top
          foreach i $samples {
            if {$db($i,type)=="spacer"} {
              frame $f.$i -relief flat
              pack $f.$i -fill x -side top -pady 5
            } elseif {$db($i,type)=="heading"} {
              label $f.$i -text $db($i,title) -bg $colors(banner) -relief groove  -font $fonts(bold)
              pack $f.$i -fill x -side top -padx 5 -pady 5
            } elseif {$db($i,type)=="readme" || $db($i,type)=="docu" || $db($i,type)=="program"}
{
              button $f.$i -text $db($i,title) -bd 1 -command "showDemo $i"
              pack $f.$i -fill x -side top -padx 5 -pady 2
            } else {
              tk_messageBox -title {Error} -type ok -icon error -message "internal error: wrong type
'$db($i,type)'"
              exit
            }
          }

          update
          .sel.c config -width [winfo width .sel.c.f]
          .sel.c config -scrollregion "0 0 0 [winfo height .sel.c.f]"
          showDemo $first
        }

        proc helpAbout {} {
          tk_messageBox -title {About} -type ok -icon info -message {Demo simulations for
OMNEST/OMNeT++.}
        }

        proc showDemo {sample} {
          global samples db colors tcl_platform

          set f .sel.c.f
          foreach i $samples {
            if {$db($i,type)=="readme" || $db($i,type)=="docu" || $db($i,type)=="program"} {
              $f.$i config -relief raised -bg $colors(unselbutton)
            }
          }

          $f.$sample config -relief sunken -bg $colors(selbutton)

          if {$db($sample,type)=="readme"} {
```

```
            .main.up.banner config -text "$db($sample,title)"
            pack forget .main.lo
            loadFile .main.mid.text $db($sample,readme)

          } elseif {$db($sample,type)=="docu"} {
            .main.up.banner config -text "$db($sample,title)"
            .main.lo.start config -text "Open documentation\n($db($sample,docu))"
            .main.lo.start config -command "openDocu $sample"
            pack forget .main.lo
            pack .main.lo -expand 0 -fill x -side bottom -before .main.mid
            loadFile .main.mid.text $db($sample,readme)

          } elseif {$db($sample,type)=="program"} {

            if {$tcl_platform(platform)=="unix"} {
              set cmd "cd $db($sample,dir); $db($sample,uprog)"
            } else {
              set cmd "cd $db($sample,dir); $db($sample,wprog)"
            }
            .main.up.banner config -text "$db($sample,title) README"
            .main.lo.start config -text "Launch $db($sample,title)\n($cmd)"
            .main.lo.start config -command "runSample $sample"
            pack forget .main.lo
            pack .main.lo -expand 0 -fill x -side bottom -before .main.mid
            loadFile .main.mid.text "$db($sample,dir)/README"

          } else {
            tk_messageBox -title {Error} -type ok -icon error -message "internal error: wrong type
'$db($sample,type)'"
            exit
          }
        }

        proc loadFile {t filename} {
          $t delete 1.0 end

          if [catch {
            # try with ".txt" suffix as well
            if [catch {set f [open $filename r]}] {set f [open "$filename.txt" r]}
            set contents [read $f]
            close $f
          } err] {
            #tk_messageBox -title {OMNeT++ Demo} -type ok -icon error -message "Cannot
display README: $err"
            return
          }

          $t insert end $contents
          $t mark set insert 1.0
        }

        proc runSample {sample} {
          global samples db tcl_platform
```

```
            if {$tcl_platform(platform) == "unix"} {
              set prog $db($sample,uprog)
            } else {
              set prog "cmd /c $db($sample,wprog)"
            }

            set pwd [pwd]
            if [catch {
               cd $db($sample,dir)
               #exec $prog &
               #exec [lindex $prog 0] [lindex $prog 1] [lrange $prog 2 end] &
               eval exec $prog &
             } err] {
               tk_messageBox -title {OMNeT++ Demo} -type ok -icon error -message "Error running
the simulation program: $err"
            }
            cd $pwd
         }

         proc openDocu {sample} {
            global samples db tcl_platform unixbrowser

            if [catch {
               if {$tcl_platform(platform) == "windows"} {
                  exec cmd.exe /c start $db($sample,docu)
               } else {
                  exec $unixbrowser $db($sample,docu) &
               }
             } err] {
               tk_messageBox -title {OMNeT++ Demo} -type ok -icon error -message "Error running
the simulation program: $err"
            }
         }

         #=================================================================
==
         #   GENERIC BINDINGS
         #=================================================================
==

         proc generic_bindings {} {
           bind Button <Return> {tkButtonInvoke %W}
         }

         #=================================================================
==
         #   FONT BINDINGS
         #=================================================================
==

         proc font_bindings {} {
           global fonts tcl_platform colors
```

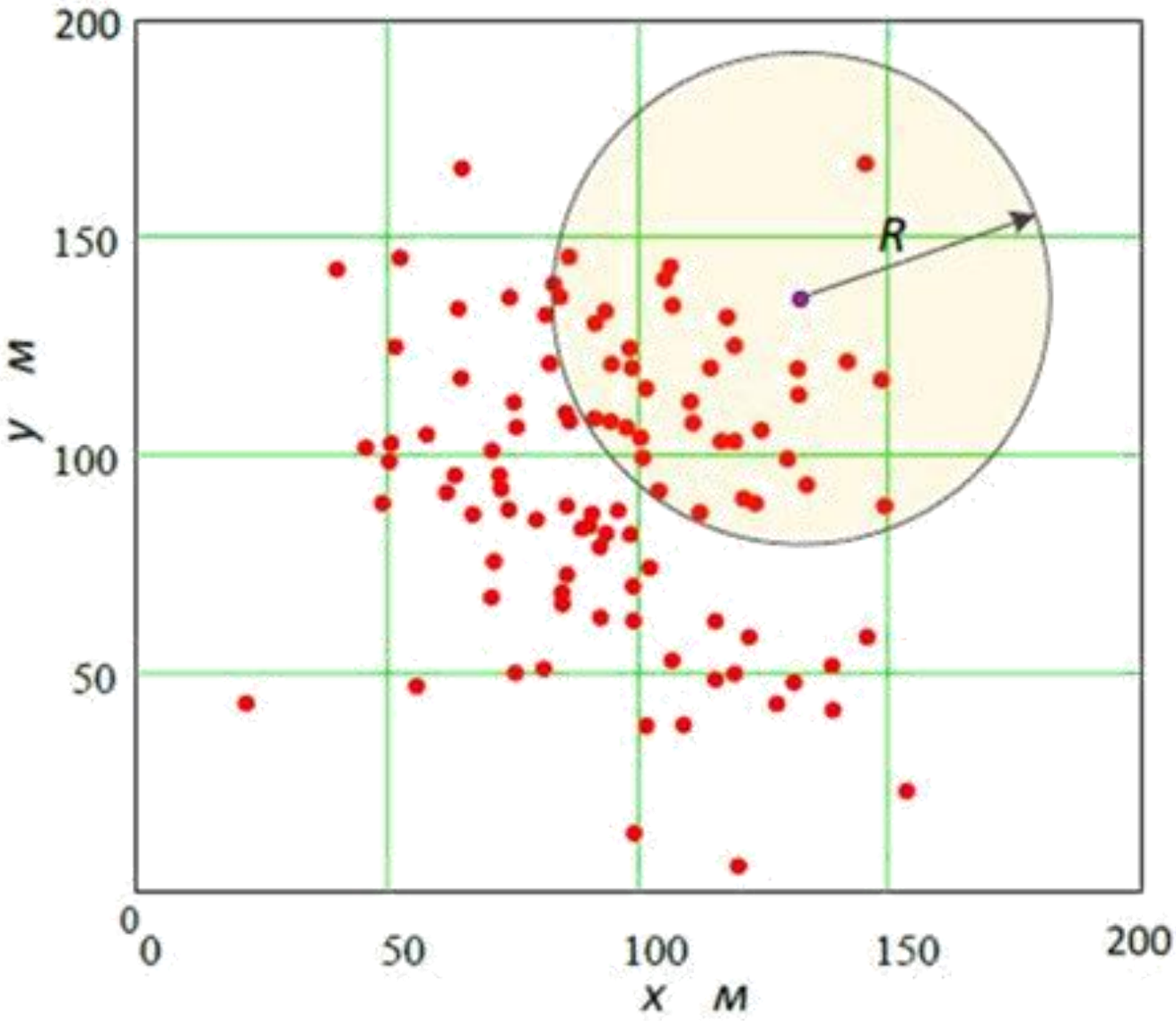
```
  set colors(banner)      #e0e0a0
  set colors(unselbutton) #c0c0c0
  set colors(selbutton)   #ffffff
  set colors(startbutton) #e0e0a0

  #
  # fonts() array elements:
  #  normal:  menus, labels etc
  #  bold:    buttons
  #  icon:    toolbar 'icons'
  #  big:     STOP button
  #  msgname: message name during animation
  #  fixed:   text windows and listboxes
  #

  if {$tcl_platform(platform) == "unix"} {
    set fonts(normal) -Adobe-Helvetica-Medium-R-Normal-*-12-*-*-*-*-*-*-*
    set fonts(bold)   -Adobe-Helvetica-Bold-R-Normal-*-12-*-*-*-*-*-*-*
    set fonts(icon)   -Adobe-Times-Bold-I-Normal-*-12-*-*-*-*-*-*-*
    set fonts(big)    -Adobe-Helvetica-Medium-R-Normal-*-18-*-*-*-*-*-*-*
    set fonts(msgname) -Adobe-Helvetica-Medium-R-Normal-*-12-*-*-*-*-*-*-*
    set fonts(fixed)  fixed
    set fonts(balloon) -Adobe-Helvetica-Medium-R-Normal-*-12-*-*-*-*-*-*-*
  } else {
    # Windows, Mac
    set fonts(normal) -Adobe-Helvetica-Medium-R-Normal-*-*-140-*-*-*-*-*-*
    set fonts(bold)   -Adobe-Helvetica-Bold-R-Normal-*-*-140-*-*-*-*-*-*
    set fonts(icon)   -Adobe-Helvetica-Bold-R-Normal-*-*-140-*-*-*-*-*-*
    set fonts(big)    -Adobe-Helvetica-Medium-R-Normal-*-*-180-*-*-*-*-*-*
    set fonts(msgname) -Adobe-Helvetica-Medium-R-Normal-*-*-140-*-*-*-*-*-*
    set fonts(fixed)  FixedSys
    set fonts(balloon) -Adobe-Helvetica-Medium-R-Normal-*-*-140-*-*-*-*-*-*
  }

  if {$tcl_platform(platform) == "unix"} {
     option add *Scrollbar.width  12
     option add *Menubutton.font  $fonts(normal)
     option add *Menu.font        $fonts(normal)
     option add *Label.font       $fonts(normal)
     option add *Entry.font       $fonts(normal)
     option add *Listbox.font     $fonts(fixed)
     option add *Text.font        $fonts(fixed)
     option add *Button.font      $fonts(bold)
  }
}

proc checkVersion {} {

  global tk_version tk_patchLevel

  catch {package require Tk}
  if {$tk_version<8.0} {
```

```
    wm deiconify .
    wm title . "Bad news..."
    frame .f
    pack .f -expand 1 -fill both -padx 2 -pady 2
    label .f.l1 -text "Your version of Tcl/Tk is too old!"
    label .f.l2 -text "Tcl/Tk 8.0 or later required."
    button .f.b -text "OK" -command {exit}
    pack .f.l1 .f.l2 -side top -padx 5
    pack .f.b -side top -pady 5
    focus .f.b
    wm protocol . WM_DELETE_WINDOW {exit}
    tkwait variable ok
  }
  if {[string compare $tk_patchLevel "8.0p1"]<0} {
    tk_messageBox -title {Warning} -type ok -icon warning \
      -message {Old Tcl/Tk version. At least 8.0p1 is strongly recommended!}
  }
}

set tk_strictMotif 1
cd [file dirname [info script]]
checkVersion
generic_bindings
font_bindings
createWindow
```

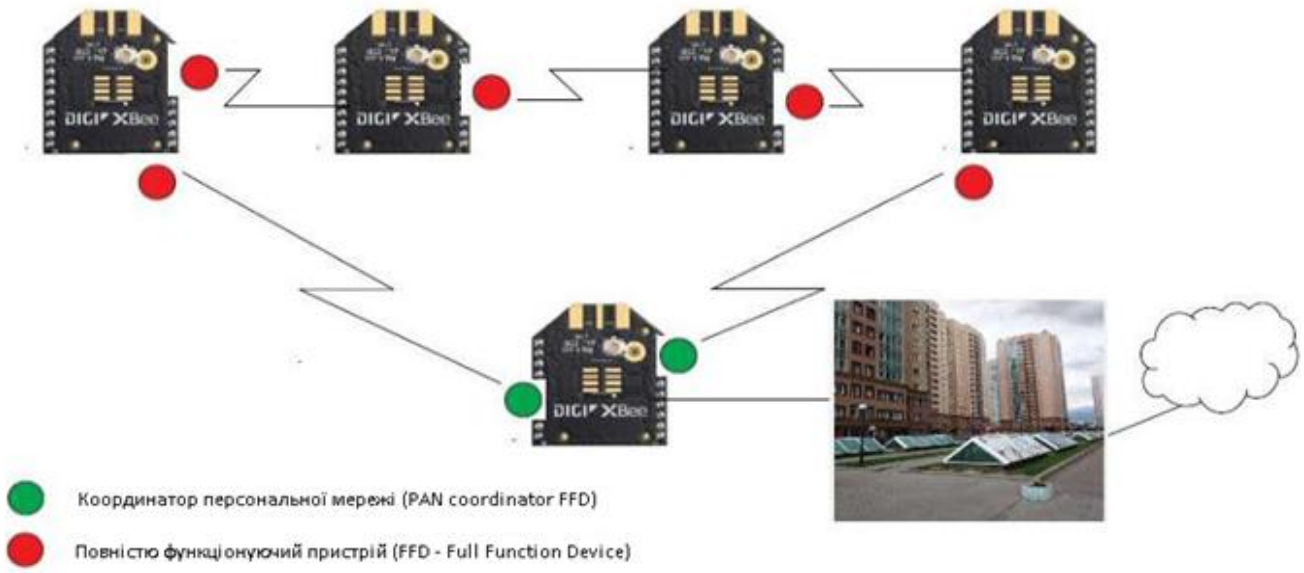
```
<@setoutput path=targetFileName?default("")/>
${bannerComment}

<#if nedPackageName!="">package ${nedPackageName};</#if>

// numOfHosts: ${numOfHosts}
// parametric: ${parametric?string}
// static:     ${static?string}

import inet.networklayer.autorouting.ipv4.IPv4NetworkConfigurator;
import inet.nodes.inet.AdhocHost;
import inet.world.radio.ChannelControl;


network ${targetTypeName}
{
   parameters:
<#if parametric>
       int numHosts;
</#if>
   submodules:
<#if parametric>
       host[numHosts]: AdhocHost
       {
           parameters:
               @display("r=,,#707070");
       }
<#else>
   <#list 0..numOfHosts?number-1 as i>
       host${i}: AdhocHost
       {
           parameters:
               @display("r=,,#707070");
       }
   </#list>
</#if>

       channelControl: ChannelControl
       {
           parameters:
               @display("p=60,50");
       }

       configurator: IPv4NetworkConfigurator
       {
           @display("p=140,50");
       }
}



[General]
network = ${targetTypeName}
```

```
#record-eventlog = true
#eventlog-message-detail-pattern = *:(not declaredOn(cMessage) and not declaredOn(cNamedObject) and not declaredOn(cObject))

<#if parametric>
*.numHosts = ${numOfHosts}
   <#assign host_0 = "host[0]">
   <#assign host_all = "host[*]">
<#else>
   <#assign host_0 = "host0">
   <#assign host_all = "host*">
</#if>

num-rngs = 3
**.mobility.rng-0 = 1
**.wlan[*].mac.rng-0 = 2
#debug-on-errors = true

tkenv-plugin-path = ../../../etc/plugins

**.channelNumber = 0

# channel physical parameters
*.channelControl.carrierFrequency = 2.4GHz
*.channelControl.pMax = 2.0mW
*.channelControl.sat = -110dBm
*.channelControl.alpha = 2
*.channelControl.numChannels = 1

# mobility
**.${host_all}.mobilityType = "MassMobility"
**.mobility.constraintAreaMinZ = 0m
**.mobility.constraintAreaMaxZ = 0m
**.mobility.constraintAreaMinX = 0m
**.mobility.constraintAreaMinY = 0m
**.mobility.constraintAreaMaxX = 600m
**.mobility.constraintAreaMaxY = 400m
**.mobility.changeInterval = truncnormal(2s, 0.5s)
**.mobility.changeAngleBy = normal(0deg, 30deg)
**.mobility.speed = truncnormal(20mps, 8mps)
**.mobility.updateInterval = 100ms

# ping app (${host_0} pinged by others)
*.${host_0}.pingApp[0].destAddr = ""
*.${host_all}.numPingApps = 1
*.${host_all}.pingApp[0].destAddr = "${host_0}"
*.${host_all}.pingApp[0].startTime = uniform(1s,5s)
*.${host_all}.pingApp[0].printPing = true

# nic settings
**.wlan[*].bitrate = 2Mbps

**.wlan[*].mgmt.frameCapacity = 10
```

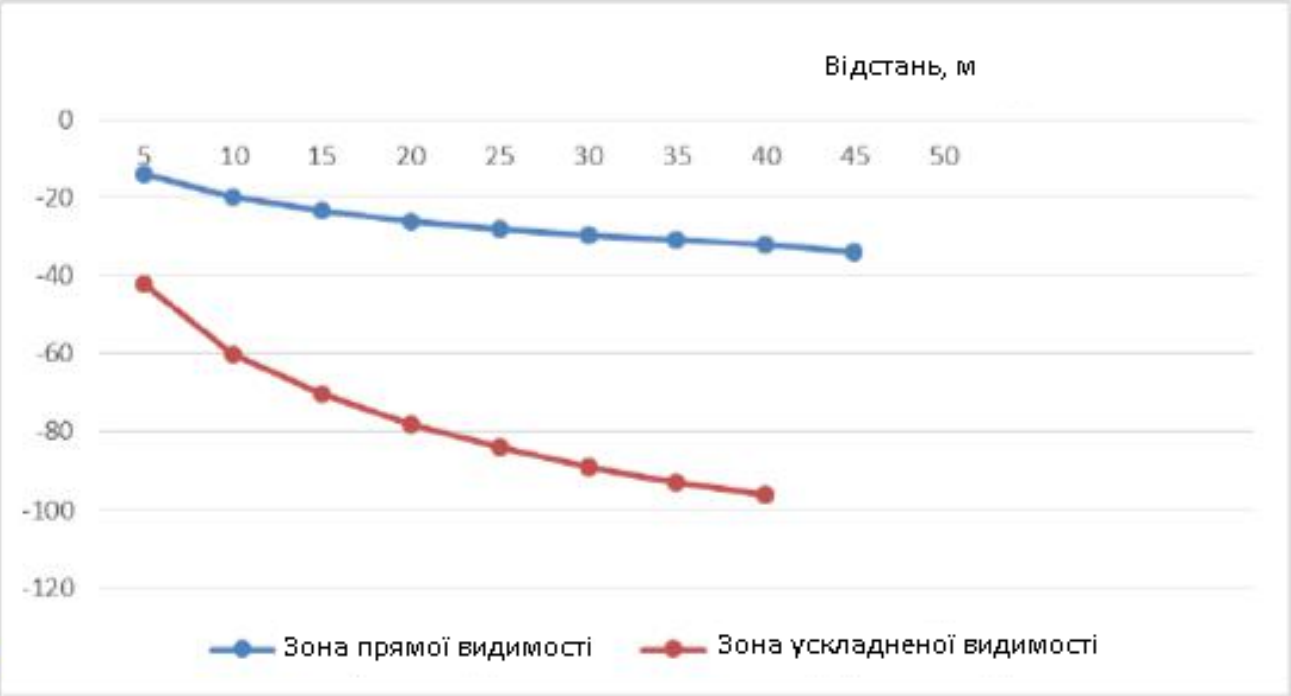
```
**.wlan[*].mac.address = "auto"
**.wlan[*].mac.maxQueueSize = 14
**.wlan[*].mac.rtsThresholdBytes = 3000B
**.wlan[*].mac.retryLimit = 7
**.wlan[*].mac.cwMinData = 7
**.wlan[*].mac.cwMinMulticast = 31

**.wlan[*].radio.transmitterPower = 2mW
**.wlan[*].radio.thermalNoise = -110dBm
**.wlan[*].radio.sensitivity = -85dBm
**.wlan[*].radio.pathLossAlpha = 2
**.wlan[*].radio.snirThreshold = 4dB
```



					Бакалаврська кваліфікаційна робота		
					Графічне представлення моделі аналізу бездротової сенсорної мережі при мультимодальному розподілі вузлів	Літера	Мас	Масштаб
Зм.	Лист	Прізвище	Підпис	Дата		Н		
Дипломник		Слота Н.				Аркуш 1	Аркушів 6	
Керівник		Белей О.І.						
Консул.						Національний університет “Львівська політехніка” ІКНІ, КН-411		
Консул.								
Реценз.								
Зав.каф.		Лобур М.В.						

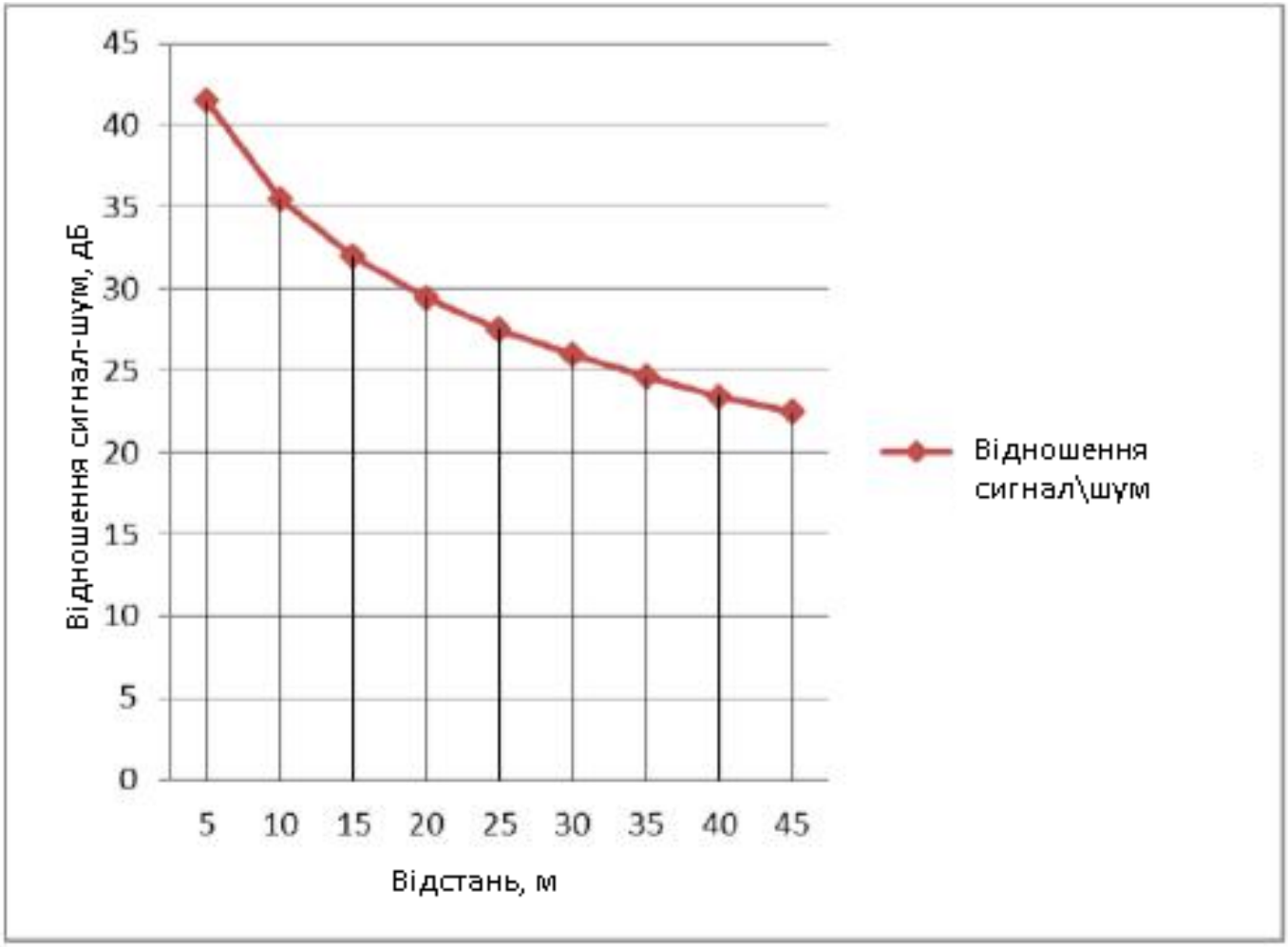


					Бакалаврська кваліфікаційна робота		
						Літера	Мас	Масштаб
Зм.	Лист	Прізвище	Підпис	Дата	Схема структури бездротової сенсорної мережів в житловому кварталі Манхеттен	Н		
Дипломник		Слота Н.				Аркуш 2	Аркушів 6	
Керівник		Белей О.І.						
Консул.						Національний університет “Львівська політехніка” ІКНІ, КН-411		
Консул.								
Реценз.								
Зав.каф.		Лобур М.В.						

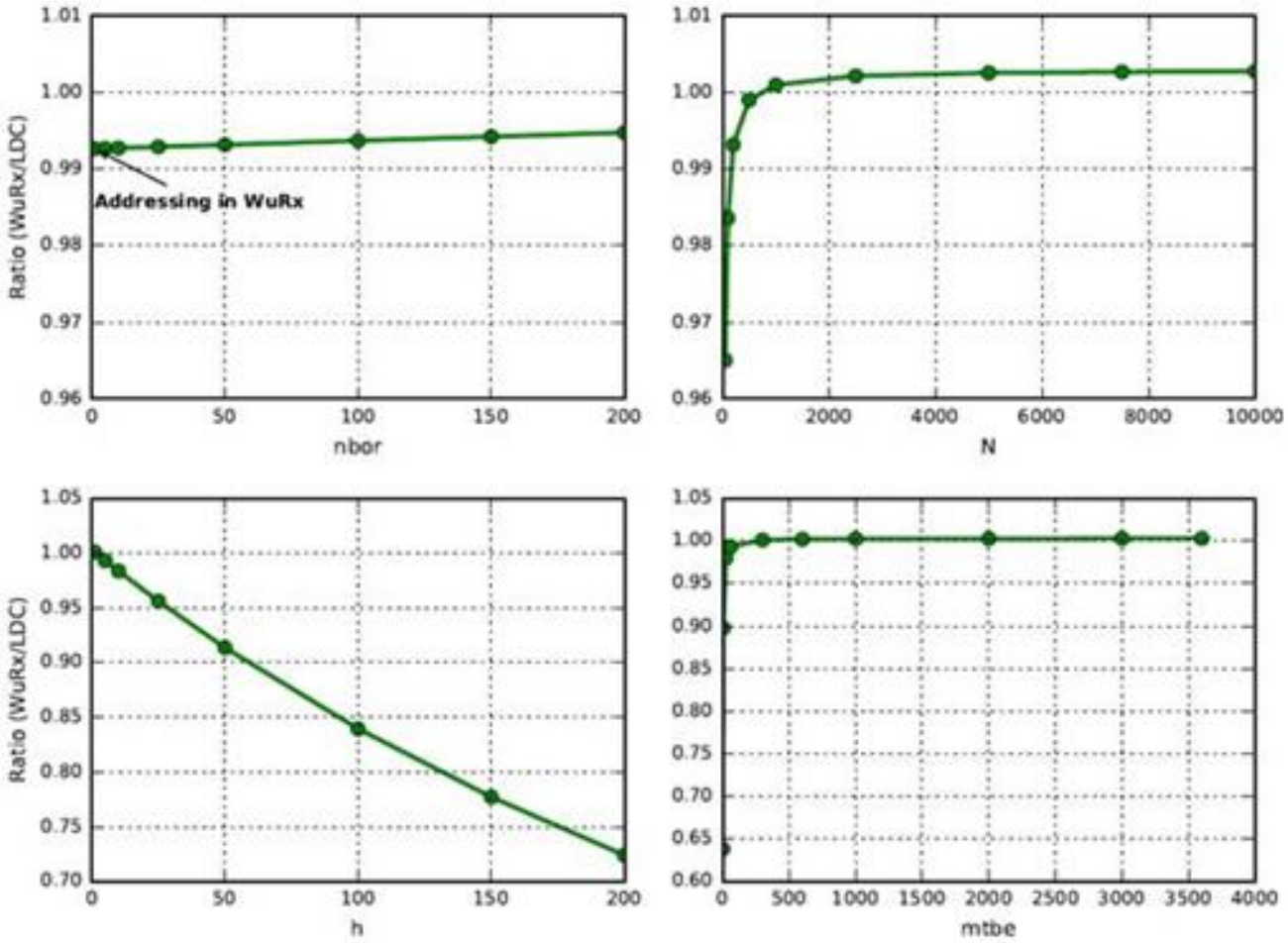


					Бакалаврська кваліфікаційна робота		
Зм.	Лист	Прізвище	Підпис	Дата	Залежність прийнятої потужності від потужності на контрольній відстані в бездротовій сенсорній мережі	Літера	Мас	Масштаб
Дипломник		Слота Н.				Н		
Керівник		Белей О.І.				Аркуш 3	Аркушів 6	
Консул.						Національний університет “Львівська політехніка” ІКНІ, КН-411		
Консул.								
Реценз.								
Зав.каф.		Лобур М.В.						

					Бакалаврська кваліфікаційна робота		
Зм.	Лист	Прізвище	Підпис	Дата	Затухання на маршруті після врахування затухання, спричиненого перешкодами в бездротовій сенсорній мережі	Літера	Мас	Масштаб
Дипломник		Слота Н.				Н		
Керівник		Белей О.І.				Аркуш 4	Аркушів 6	
Консул.						Національний університет “Львівська політехніка” ІКНІ, КН-411		
Консул.								
Реценз.								
Зав.каф.		Лобур М.В.						



					Бакалаврська кваліфікаційна робота		
					Зв'язок між співвідношенням сигнал/шум та відстанню в бездротовій сенсорній мережі	Літера	Мас / Масштаб
Зм.	Лист	Прізвище	Підпис	Дата		Н	
Дипломник						Аркуш 5	Аркушів 6
Керівник		Белей О.І.				Національний університет "Львівська політехніка" ІКНІ, КН-411	
Консул.							
Консул.							
Реценз.							
Зав.каф.		Лобур М.В.					



					Бакалаврська кваліфікаційна робота	
Зм.	Лист	Прізвище	Підпис	Дата	Загальний коефіцієнт споживання енергії при двох рішеннях бездротових сенсорних мереж та використанні різних ресурсів	Літера: Н; Мас; Масштаб
Дипломник		Слота Н.				Аркуш 6; Аркушів 6
Керівник		Белей О.І.				Національний університет "Львівська політехніка" ІКНІ, КН-411
Консул.						
Консул.						
Реценз.						
Зав.каф.		Лобур М.В.				