Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Методи аналізу пропускної здатності бездротової сенсорної мережі

Виконав: студент 2 курсу, гр. КІТПВм-22-2
Карпов_М.С.
(прізвище, ініціали)

Спеціальність
151 Автоматизація та комп'ютерно-інтегровані технології

освітньої програми Комп'ютерно-інтегровані технологічні процеси і виробництва
(код і повна назва напряму)

Тип програми освітньо-професійна
(повна назва освітньої програми)

Керівник Стародубцев М.Г.
(посада, прізвище, ініціали)

Допускається до захисту
зав. кафедри _____ Невлюдов І.Ш.
(підпис) (прізвище, ініціали)

2024 р

Харківський національний університет радіоелектроніки

Факультет	Автоматики і комп'ютеризованих технологій
Кафедра	Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
Рівень вищої освіти	другий (магістерський)
Спеціальність	151 Автоматизація та комп'ютерно-інтегровані технології
Тип програми	освітньо-професійна
Освітня програма	Комп'ютерно-інтегровані технологічні процеси і виробництва

(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Карпову Максиму Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи аналізу пропускної здатності бездротової сенсорної мережі

затверджена наказом по університету від 03.11. 2023 р. № 1287 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 18.01.2024 р.

3. Вихідні дані до роботи

3.1 Платформа програмування NS2;

4. Зміст розрахункової записки(перелік питань, які потрібно розробити)

4.1 Вступ;

4.2 Аналіз та дослідження бездротових сенсорних мереж;

4.3 Дослідження методів пропускної здатності бездротових сенсорних мереж

4.4 Оцінка пропускної здатності у бездротових сенсорних мережах

4.5 Висновок

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Демонстраційний матеріал представлений у форматі презентації PowerPoint (*.ppt) – 13 с. формату А4

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Керівник (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз технічного завдання	15.11.2023	Виконано
2	Аналіз та дослідження бездротових сенсорних мереж	23.11.2023	Виконано
3	Дослідження методів пропускної здатності бездротових сенсорних мереж	03.12.2023	Виконано
4	Оцінка пропускної здатності у бездротових сенсорних мережах	12.12.2023	Виконано
5	Оформлення пояснювальної записки	27.12.2023	Виконано
6	Подання роботи до ЕК	24.12.2023	

Дата видачі завдання 25.11.2023

Студент _____ Карпов М. С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доц. Стародубцев М.Г.
(підпис) (посада, прізвище, ініціали)

Я як студент ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

06.01.2024 Карпов М. С.

РЕФЕРАТ

Пояснювальна записка: 103 с., 2 табл., 34 рис., 2 дод., 36 джерела.

БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ, ПРОПУСКНА ЗДАТНІСТЬ, IEEE 802.15.4 WPAN, ZIGBEE, 6LOWPAN, НАВАНТАЖЕННЯ В МЕРЕЖАХ, АГРЕГАЦІЯ ДАНИХ, АНАЛІЗ ТРАФІКУ, ДИСПЕРСІЯ, АВТОКОРЕЛЯЦІЙНА ФУНКЦІЯ, САМОПОДІБНІСТЬ, СИНХРОНІЗАЦІЯ.

Об'єкт дослідження — ефективність експлуатації бездротові сенсорні мережі.

Предмет дослідження — фактори, що впливають на пропускну здатність у бездротовій сенсорній мережі

Мета кваліфікаційної роботи — розробка методів аналізу бездротових сенсорних мереж для оптимізаціїї їх експлуатаційних характеристик в умовах промислового використання.

Методи дослідження включають літературний аналіз, математичне моделювання, статистичний аналіз та використання аналіз самоподібності для вивчення характеристик навантаження.

У результаті дослідження визначено класифікацію навантаження, розроблено моделі мереж для аналізу сценаріїв пропускної здатності, виявлено стадії обслуговування та перехідні процеси, обґрунтовано самоподібність навантаження та отримано значення Херстового показника. Результати також підтверджують можливість покращення точності синхронізації та енергоефективності в бездротових сенсорних мережах.

ABSTRACT

Explanatory note: 103 pp., 2 tables, 34 figures, 1 appendix , 36 sources.

WIRELESS SENSOR NETWORKS, BANDWIDTH, IEEE 802.15.4 WPAN, ZIGBEE, 6LOWPAN, LOADING IN NETWORKS, DATA AGGREGATION, TRAFFIC ANALYSIS, DISPERSION, AUTOCORRELATION FUNCTION, SELF SIMILARITY, SYNCHRONIZATION.

The object of research of this qualification work is wireless sensor networks.

The subject of the study includes the analysis of standards, protocols and methods of bandwidth analysis in wireless sensor networks.

The purpose of the qualification work is to study the methods of bandwidth analysis in wireless sensor networks, as well as the scientific study of the load in networks considered as the main element affecting the bandwidth.

Research methods include literature analysis, mathematical modeling, statistical analysis, and the use of wavelet analysis to study load characteristics.

As a result of the study, load classification was determined, network models were developed for the analysis of bandwidth scenarios, service stages and transitional processes were identified, load self-similarity was substantiated, and the value of the Hurst index was obtained. The results also support the possibility of improving synchronization accuracy and energy efficiency in wireless sensor networks.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АКФ – автокореляційна функція;

БСМ – бездротові сенсорні мережі;

МЕМС – мікроелектромеханічні системи;

AODV – алгоритм відстані та відкритості маршруту;

BLE – Bluetooth Low Energy;

GPS – глобальна система позиціонування;

ISM – індустріальні, наукові та медичні частоти;

LEACH – протокол обраних часових розділень;

MAC – метод доступу до середнього рівня;

PHY – метод доступу до фізичьного рівня;

SOSUS – система наведення із спостереженням підводних об'єктів;

SPIN – протокол сенсорних мереж;

WPAN – бездротова особиста місцева мережа.

ВСТУП

Останнім часом все швидше входять до оточення людини бездротові сенсорні мережі (БСМ). Вже в недалекому майбутньому сенсорні мережі як невід'ємний елемент Інтернету речей зможуть зайняти значне місце у мережах зв'язку. Переставши бути предметом тільки академічних досліджень, сенсорні мережі в наші дні поставляються великою кількістю виробників, що спричинило виникнення різноманітних індустріальних стандартів, які не забезпечують взаємний зв'язок між обладнанням різних виробників.

За результатами таких робіт з'явилося покоління стандартів IEEE 802.15.4, які регламентують канальний та фізичний рівні для формування БСМ, проте залишають невизначеними прикладний та мережевий рівні. Подальше вдосконалення IP мереж забезпечило створення робочої групи IETF 6LoWPAN з метою вирішити питання передачі пакетів IPv6 поверх каналів IEEE 802.15.4 методом, який відповідає відкритим стандартам та надає взаємний зв'язок з рештою IP каналів та пристроїв, як і в стандарті IEEE 802.15.

Важливою характерною ознакою бездротових сенсорних мереж можна вважати природу подібних мереж, що самоорганізується. Вузли, згруповані локально між собою створюють мережу й у вигляді однієї чи кількох шлюзів здійснюють передачу дані подальшої обробки, наприклад, у мережах зв'язку громадського користування. Для існування з'єднань між мережами зв'язку громадського користування та сенсорними мережами потрібне проведення розрахунку характеристик цих шлюзів, для чого слід провести дослідження природи навантаження, яке циркулює у БСМ.

Вивченню сенсорних мереж присвячувалися роботи вітчизняних та зарубіжних учених Міночкін А.І, Романюк В.А., Жук О.В., Тимченко О.В., Зеляновський М.Ю., A. Salim, W. Heinzelman, M. Younis, L. Borsani, IF Akyildiz. Проблем дослідження та методам аналізу пропускної здатності БСМ до сьогодні належної уваги не приділялося.

Процес передачі вважається головним елементом інфокомунікаційних систем, і методи аналізу пропускної здатності мають значення, коли оцінюється їх ефективність. За результатами досліджень телетрафіку мереж зв'язку, включаючи LAN, WAN мережі встановили, що моделі, що широко застосовуються на основі Пуассонівського, або процесів пов'язаних з ним не можуть дати опис самоподібного характеру навантаження. Такі моделі можуть призвести до надто оптимістичної оцінки пропускної спроможності інформаційно-комунікаційних мереж, недостатньої кількості ресурсів для обробки та передачі даних та складнощів у процесі гарантування якісного обслуговування мереж.

Мета роботи є дослідження методів аналізу пропускної здатності в бездротових сенсорних мережах, а також наукове дослідження навантаження в мережах, що розглядаються, як основний елемент, що впливає на пропускну здатність.

Для досягнення заданої мети необхідно виконати низку завдань:

– проаналізувати актуальне застосування бездротових сенсорних мереж у сучасних наукових дослідженнях та розглянути перспективи розвитку мереж для утвердження актуальності теми дослідження;

– провести дослідження найактуальніших протоколів бездротових сенсорних мереж з погляду пропускної здатності, таких як IEEE 802.15.4 WPAN, ZigBee та 6LoWPAN;

– провести аналіз вихідних даних для реалізації методів аналізу пропускної здатності у бездротових сенсорних мережах та розробити алгоритм запропонованого наукового дослідження;

– провести оцінку агрегації даних та аналіз трафіку зміни дисперсії як ключового моменту в організації пропускної здатності даних бездротових мереж;

– провести апроксимацію автокореляційної функції та моделювання сценарію пропускної здатності в БСМ;

– на основі проведених досліджень дослідити пропускну здатність даних сенсорних мереж за часом та скласти відповідні висновки щодо роботи.

Робота виконана згідно [1-2]. Результати роботи опубліковані в [3].

1 АНАЛІЗ ТА ДОСЛІДЖЕННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

1.1 Огляд стандартів бездротових сенсорних мереж

Детально розглянемо мережі бездротового широкосмугового доступу, сформовані на базі стандартів IEEE 802.16 і IEEE 802.11.

До 1985 року робота над стандартами бездротових мереж, які розроблялися комітетом IEEE 802.11, проходила надто повільно, тому що майже була відсутня зацікавленість ринку в таких технологіях, а частоти в спектрі гігагерца ліцензувалися державою. У 1985 році Федеральною Комісією зі Зв'язку (FCC) США реалізовано надання нових частот, які отримали назву «індустріальні, наукові та медичні» (ISM) частоти, та скасувала ліцензування обладнання, що функціонує на таких частотах. Це призвело до стрімкого розвитку мереж WLAN. Відпала потреба отримувати ліцензії потенційним операторам, отже, у разі невдалої комерційної експлуатації пристроїв, що функціонують на частотах ISM, вони не несуть витрат, пов'язаних із придбанням ліцензії. Найчастіше саме ці втрати вважаються найбільш значними у процесі діяльності операторів. Крім цього, зняття ліцензування створює умови для створення малих альтернативних операторів та здійснення ними комерційної діяльності без значних початкових вкладень, які можуть дозволити тільки великі оператори. Крім цього, відсутність ліцензування дала можливість корпоративним користувачам подумати про потенційне розгортання WiFi на підприємствах та в офісах [4].

Робоча група IEEE 802.11 у 1989 році розпочала роботу за канальним та фізичним рівнем для майбутнього стандарту. Створення стандарту IEEE 802.11 у розвитку бездротових локальних мереж зв'язку стало доленосною подією. 26 червня 1997 року було затверджено кінцевий варіант стандарту.

Стандартом IEEE 802.11 визначається базовий комплекс послуг, що називається BSS (Basic Service Set), який дозволяє мережам з двох і більше

мобільних або фіксованих станцій здійснювати обмін даними в будь-якій вузькій сфері простору. Стандартом визначаються 2 режими функціонування:

– Ad hoc (латинський вираз, який по–англійськи означає "for this purpose", тобто цільова мережа, цільовий режим). Такий режим надає можливість станціям, забезпеченим картами доступу IEEE 802.11, здійснювати обмін даними без операторської інфраструктури, яка передбачає існування точки доступу (базової станції) та ін. Процес обміну даними, що здійснюється між двома станціями, отримав назву незалежного базового набору послуг IBSS). Зазвичай, станціями передача широкомовних та інших службових пакетів здійснюються у межах будь–якої вузької сфери без прямого доступу до мережі, наприклад, Інтернет чи NGN. Режим Ad hoc може просто конфігуруватися для різних додатків, наприклад, обміну даними. Даний метод створення мереж на основі стандартів IEEE і став фундаментом теорії та практики побудови мереж, що самоорганізуються, зв'язку (self–organizing);

– інфраструктурний. Станції у такому режимі взаємодіють у вигляді точки доступу, що належить оператору. Як правило, підключається точка доступу до мережі Інтернет або NGN шляхом її підключення до фіксованої мережі. Будь–яка точка доступу сигналом покриває деяку вузьку територію, розмір якої залежить від виду стандарту сімейства IEEE 802.11. Діаметр такої території для відкритих просторів становить середньому від 50 до 100 метрів. Коли розгортання мережі WiFi здійснюється в будівлі, залежно від конфігурації будівлі зменшується розмір території та види матеріалів, з яких побудована будівля. З точкою доступу має асоціюватись будь–яка станція, до того ж тільки з однією. Розміщені точки доступу таким чином, щоб їх сигнали перекривалися, надаючи можливість мобільним станціям пересуватися в межах простору, який покритий сигналом від різних точок доступу. З метою переходу обслуговування, будь–якої станції з однієї точки доступу до іншої, реалізується процедура handover (хендовера), яка дозволяє виконати переасоціацію станції під час переходу від однієї базової станції до іншої.

На рисунку 1.1. наведено архітектури BSS та IBSS.

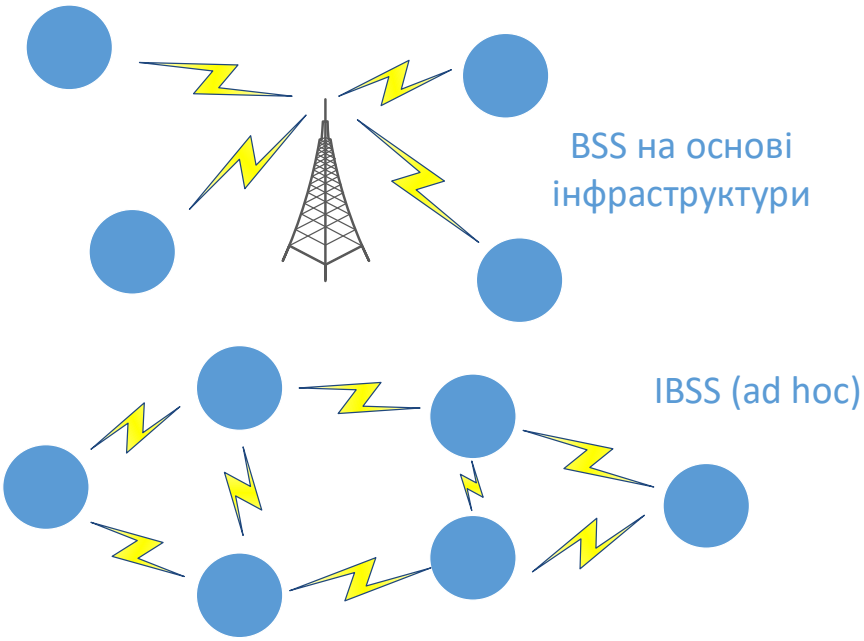

Рисунок 1.1 – Архітектури BSS та IBSS

Самоорганізація в аналогічних мережах організована на забезпеченні множинного одночасного доступу до каналу зв'язку та розподіленого доступу до сфери передачі. Для цього в стандартах IEEE 802.11 для рівня MAC канального рівня моделі взаємодії відкритих систем пропонувалося застосовувати функцію розподіленого доступу до сфери передачі DCF. Щоб реалізувати доступ до каналу, застосовують процедуру множинного доступу з детектуванням несучої та запобіганням колізій (CSMA/CA). Необхідно зауважити, що подібна побудова MAC застосовується і у всіх передових стандартах IEEE для мереж, що самоорганізуються, наприклад, у стандартах покоління IEEE 802.15 [5].

Щоб забезпечити функціонування MAC та зменшення потенційних колізій у стандарті IEEE 802.11, було введено кілька інтервалів між передачею кадрів. SIFS, короткий міжкадровий інтервал застосовується допоміжних (необхідних) кадрів, наприклад кадру докази ACK. DIFS, розподілений міжкадровий інтервал режиму DCF – підтримує можливість справедливого

розподілу ресурсів, тобто конкурентної боротьби за канал. EIFS, розширений міжкадровий інтервал застосовується у разі виникнення помилки.

Контроль (детектування) несучої вважається однією з найбільш значних функцій доступу до каналу зв'язку (MAC IEEE 802.11x) для запобігання можливим колізіям. Така функція реалізується фізично і вважається високоенергоємною при постійному використанні, тому реалізовується за запитом. Контролюється віртуальна несуча із застосуванням вектора резервування мережі (NAV).

Застосування NAV показано рисунку 1.2.

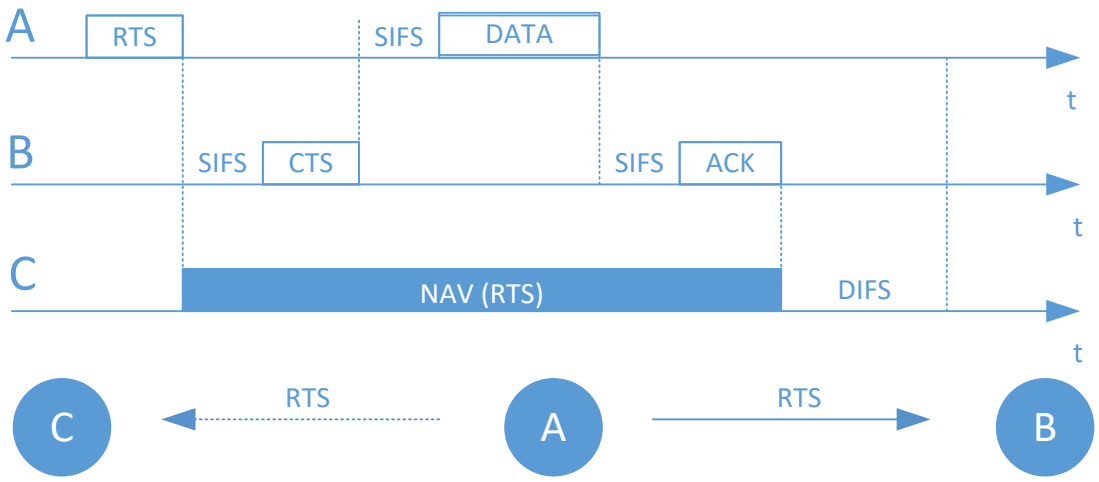

Рисунок 1.2 – Використання NAV

У IEEE 802.11 обмін інформацією здійснюється за допомогою механізму RTS/CTS. Функціонує механізм RTS–CTS за таким алгоритмом (рисунок 1.3): передавачем передається кадр RTS приймачеві, що містить адресу приймача та загальний час, який знадобиться передачі кадру. Внаслідок широкомовної процедури передачі інформації для IEEE 802.11x кадр RTS в межах досяжності приймається всіма станціями. Необхідний приймач визначається адресою і відповідає кадром CTS після SIFS, інші станції встановлюють «вектор резервування мережі» в межах досяжності. Також кадр CTS приймається у межах досяжності всіма станціями, але тепер можливо іншими. Поруч із цим

передавачем передається інформаційний кадр після SIFS, а «вектор резервування мережі» встановлюють нові станції. Коли перераховані пункти виконані, всі станції в межах досяжності та CTS та RTS інформуються про резервування каналу. Виконується передача інформаційного кадру DATA і, якщо вона здійснена успішно, приймачем передається доказ ACK після SIFS, закінчується «вектор резервування мережі», канал вважається вільним [6].

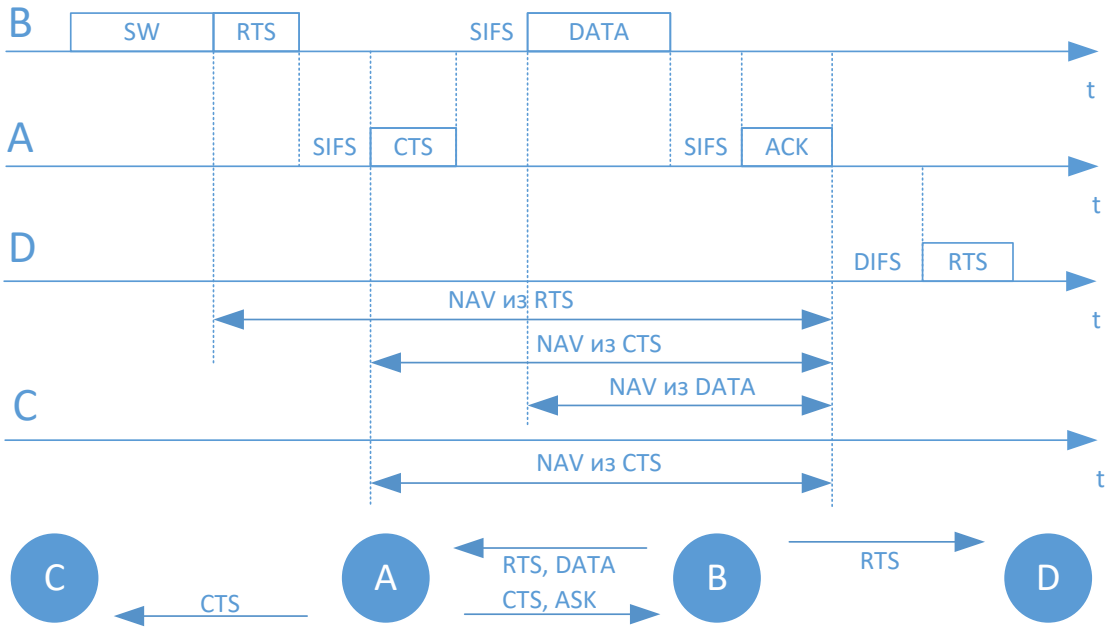

Рисунок 1.3 – Приклад алгоритму функціонування RTS–CTS

Вище зазначалося, що з запобігання колізій застосовується процедура CSMA/CA.

У наші дні за допомогою мережі бездротового широкосмугового доступу можна передавати як дані, а й передавати мова. Самоорганізується називається мережа, в якій кількість вузлів вважається випадковою величиною в часі і здатне змінюватися від 0 до деякого значення N_{max}. Взаємні зв'язки в подібній мережі між вузлами в часі також випадкові і формуються, щоб мережа досягла будь–якої мети для здійснення передачі даних в мережу зв'язку громадського користування або інші мережі [6].

На рисунку 1.4 зображена архітектура мережі, що самоорганізується.

Самоорганізовані мережі, аналогічно всім мережам зв'язку, складаються з транзитної мережі та мереж доступу. Транзитна мережа називається mesh (коміркова), а мережа доступу – Ad Hoc (цільова мережа). На рис. 1.8, показано, що вузли мережі Ad Hoc не мають функцію маршрутизації і здатні реалізовувати взаємозв'язок тільки з найближчими вузлами. Тому часто вузли Ad Hoc називають дочірніми. Однак це не означає, що дочірній вузол має сувору прив'язку до того чи іншого батьківського вузла. Дочірній вузол у процесі життєвого циклу мережі може бути прив'язаним до будь-якого батьківського вузла, розташованого найближче до нього. За конкретних обставин дочірній вузол має можливість назавжди чи тимчасово перетворитися на батьківський вузол, наприклад, в бездротових однорідних сенсорних мережах, механізми функціонування яких, розглядаються у наступному розділі.

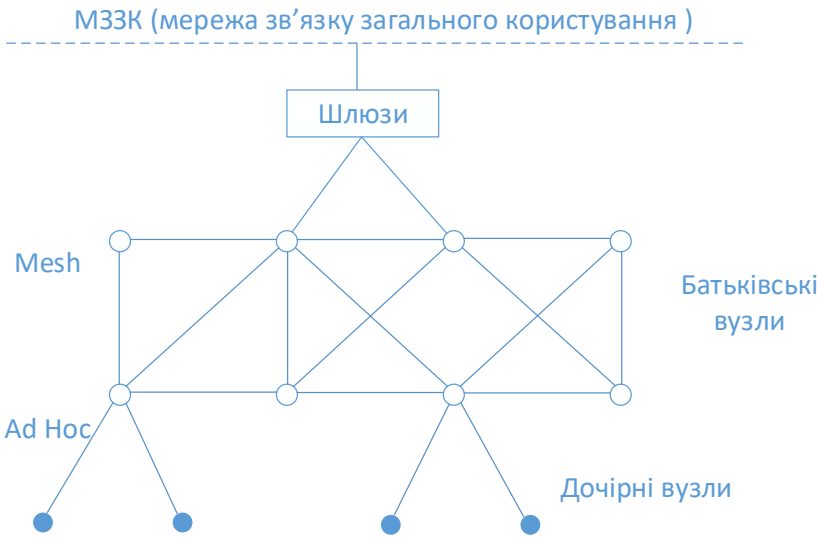

Рисунок 1.4 – Архітектура мережі, що самоорганізується

Вузли mesh мають вбудовані функції маршрутизації і здатні забезпечити підтримку встановлення з'єднання, як до найближчого вузла, так і до великої кількості інших. Цей мережевий режим отримав назву multi–hop (багатокрокове з'єднання). На відміну від з'єднань для дочірніх вузлів Ad Hoc

мережі, обмежені одним кроком у встановленні з'єднання (one–hop). Часто Mesh вузли називають батьківськими вузлами, що акцентує транзитну функцію mesh мережі. Вузли самоорганізується мають здатність поєднувати дочірні і батьківські функції, наприклад, за аналогією з давно відомими з історії розвитку зв'язку в нашій державі комбінованими місцевими/міжміськими автоматичними телефонними станціями [7].

З усіх додатків сенсорних мереж виділимо ті, що функціонують в даний час:

– USN – бездротові (всепроникні) сенсорні мережі;

– VANET – мережі для транспортних засобів;

– HANET – муніципальні мережі;

– MBAN – медичні мережі.

Найзначнішими за розрахунковим обсягом впровадження на сьогоднішній день прийнято вважати мережі USN, що входять і до складу концепції NGN як один із компонентів NGN мережних структур.

1.2 Дослідження програм для автоматизації діяльності за допомогою бездротових сенсорних мереж

Так як бездротові сенсорні мережі прийнято вважати всепроникними, то кількість їх додатків не обмежена. Але, з позиції розрахунку можливостей мереж зв'язку загального користування та сенсорних мереж, забезпечення необхідного ступеня якості обслуговування та ін. буде раціональним класифікувати додатки сенсорних мереж.

Останнім часом набуло популярності рішення «розумний» будинок, яке дозволяє автоматизувати та зробити комфортніше проживання у сучасних будинках. Рішення містить у собі контроль, забезпечення безпеки та зручності користувачів [8]:

– сенсорна програма для надання гнучкого управління з будь–якого

місця в будинку системою кондиціювання, опаленням освітленням;

– сенсорна програма для здійснення автоматичного контролю великої кількості домашніх систем, які призначені для вдосконалення безпеки, зручності та економії;

– сенсорний додаток, що дозволяє знімати коректні дані про використану кількість газу, води та електрики;

– інтелектуальний сенсорний додаток для скорочення використання природних ресурсів;

– сенсорна програма, яка забезпечує бездротове з'єднання, а також встановлення та оновлення програмного забезпечення для систем, що здійснюють керування будинком;

– сенсорна програма, яка дозволяє використовувати та налаштовувати кілька систем керованих одним пультом дистанційного керування;

– сенсорна програма, яка підтримує встановлення та роботу бездротових датчиків контролю різноманітних фізичних умов;

– сенсорна програма, яка полегшує отримання повідомлень в автоматичному режимі за ступенем виявлення незвичайних подій.

Елементи рішення «розумний» будинок зображено рисунку 1.5.

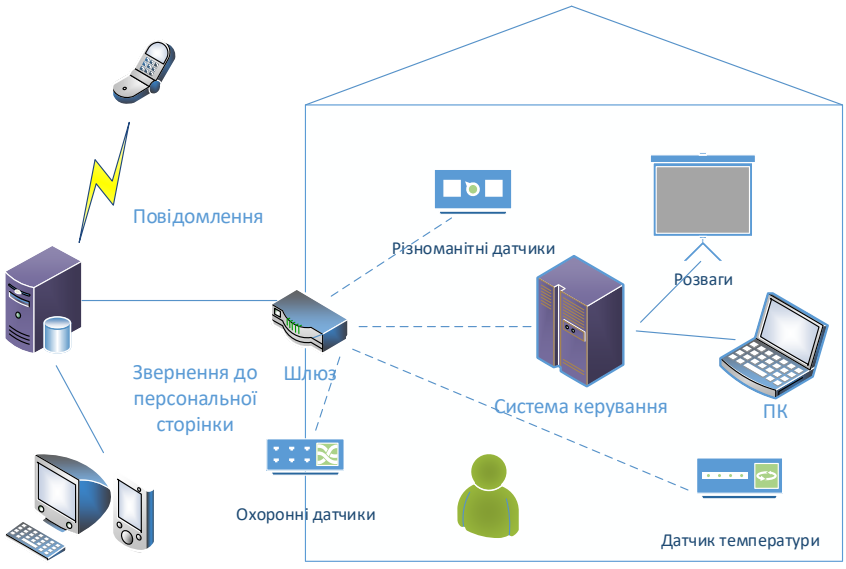

Рисунок 1.5 – Компоненти системи "Розумний" будинок

Під час спрацювання датчиків здійснюється передача у відповідну службу тривожних повідомлень.

Окремі медичні центри та лікарні розглянули можливість використання технології WSN для здійснення медичних додатків, включаючи ліквідацію результатів стихійних лих та спостереження за реабілітаційним періодом пацієнтів після виписки з клініки, надання екстреної медичної допомоги. Мережі WSN мають у своєму розпорядженні можливість забезпечення швидкого реагування на події та своєчасне забезпечення медичними послугами, які дозволяють у реальному періоді часу здійснювати збір важливих показників життєдіяльності, а також організувати сортування та кореляцію з лікарняними картами пацієнтів при довгострокових спостереженнях [9].

Також WSN надають можливість організації тривалого збору медичної інформації, яка заповнює бази лікарняних даних, що сприяє проведенню довготривалих обстежень населення та надає медичному персоналу інформацію для вивчення результатів від запровадження всебічних медичних програм.

Гарвардським університетом разом з іншими навчальними закладами створено датчик електрокардіограми (ЕКГ) та невеликий за розмірами бездротовий вимірник пульсу. Цими пристроями збираються дані про насичення киснем, серцевому ритмі та ЕКГ, і ретранслюються на невеликі відстані (до 100 м) за допомогою бездротової мережі на будь–яке число пристроїв, у тому числі ноутбуки, КПК або термінали швидкої медичної допомоги. Відображаються ці дані в режимі реального часу та вносяться до попередньо створеної особистої карти пацієнта. Існує можливість запрограмувати сенсорні пристрої для самостійної обробки параметрів життєдіяльності, наприклад, передавати тривожні повідомлення, коли результати виміряних властивостей перевищують стандартні рамки, про будь–

які несприятливі зміни в стані хворого. Цю інформацію можна передати фельдшеру або термінал найближчої станції медичної допомоги.

У спільній роботі з Motion Analysis Laboratory у реабілітаційному госпіталі Spaulding Гарвардським університетом розроблено мініатюрний прилад для контролю м'язової діяльності та рухів кінцівок у період реабілітації хворих після інсульту. Прилади містять три осьових акселерометри, гіроскоп і електроміограмні датчики, що дозволяють обстежувачам накопичувати велику чисельність даних про м'язову активність з метою вивчення впливу різноманітних відновлювальних вправ і виробляти найоптимальніші процедури.

Апаратну платформу Гарвардський університет поповнив програмним забезпеченням, яке підтримує працездатність масштабованої інфраструктури бездротових сенсорних медичних приладів CodeBlue [10].

Також за допомогою WSN мереж реалізується і бездротовий контроль освітлення (наприклад, керовані перемикачі світла, схеми освітлення, що настроюються, економія електроенергії в світлі дні). Оптимальне застосування електроенергії вважається одним із завдань, яке елементарно вирішується за допомогою WSN. Енергетика вважається однією з найважливіших статей операційних витрат у сфері готельного бізнесу. Централізоване HVAC управління надає можливість готельним операторам значно заощадити електроенергію, наприклад, відключивши систему кондиціювання в номерах, де немає мешканців. Управління активами також вважається завданням, яке вирішують сенсорні мережі. Наприклад, у кожному контейнері датчиками формується WSN мережу; на кораблі кілька контейнерів формують розширену сенсорну мережу, яка призначена для збору даних. Мережа WSN гарантує додаткову безпеку завдяки установці на будь–якому судні та вантажівці датчиків розтину. Швидко обробляти контейнери можна завдяки попередньому збору даних від сенсорів до того часу, коли судно зайшло порт. Програми автоматизації приміщень забезпечують гнучкість, збереження,

контроль та безпеку в наступних випадках [11]:

– сенсорні програми для централізованого управління та інтеграції освітлення, безпеки, опалення, охолодження;

– сенсорні програми для автоматизації управління різноманітних систем з метою забезпечення безпеки та гнучкості, удосконалення охорони;

– сенсорні програми для зменшення енергетичних втрат за допомогою оптимізації управління HVAC;

– сенсорні програми, які дозволяють достовірно встановити комунальні витрати на основі фактичного використання;

– сенсорні програми, які дозволяють швидко переконфігурувати освітлювальні системи для створення адаптованих робочих місць;

– сенсорні програми для модернізації та розширення інфраструктури приміщень з мінімальними витратними зусиллями;

– сенсорні програми, які дозволяють об'єднати в мережу та здійснювати інтегрування даних від різних точок контролю доступу;

– сенсорні програми, які дозволяють здійснювати розгортання бездротових мереж моніторингу, щоб покращити охорону по периметру.

Вище було зазначено, що основним інтересом є контроль стану довкілля у приміщеннях і, як наслідок, – економія електроенергії. Перевага надається використанню мікросенсорних технологій, в основі яких лежать радіосистеми, що мають наднизьке споживання електроенергії в малогабаритних корпусах; такий контроль здійснюється завдяки використанню мультимодальних технологій комунікацій та бездротового зондування. Приділяється увага двом напрямкам: застосування сенсорних мереж з метою контролю температури всередині будівель та методики моніторингу повітряних потоків. Велика кількість сенсорних вузлів (що забезпечують синхронну роботу різноманітних датчиків, таких як присутності, температурний та ін.) застосовуються разом з одним блоком управління (прийняття рішень), що надає можливість на основі інформації з WSN здійснювати контроль кількох приміщень у будівлі,

внаслідок чого можна знизити споживання енергії та одночасно покращити комфорт. Досягається такий ефект методом заміни одиночних провідних датчиків, характерних більшості споруд, сенсорної мережею, яка має, як мінімум, одним вузлом у кожному приміщенні. Підвищення продуктивності здійснюється без необхідності змінювати систему управління, внаслідок чого стратегію можна вважати ідеальною з метою оновлення інфраструктури в існуючих будинках.

Доцільно застосовувати сенсорні мережі для управління систем, які призначені для здійснення градієнтної установки температури в приміщеннях; такі системи нині застосовуються у більшості комерційних будинках. Вони мають назву: системи розподіленого внутрішнього підігріву повітря (UFAB). Системи UFAB, як правило, здійснюють контроль за допомогою одного датчика температури; такі функції зазвичай локалізуються лише у точці. За результатами досліджень встановлено, що суттєве покращення енергетичної продуктивності досягається застосуванням для контролю такою системою сенсорної мережі, яка має два або більше датчиків у кожній зоні.

Мережі WSN полегшують процедуру розподілу функцій управління по всьому фізичному простору всередині приміщення. З позиції розробки кабельних систем вартість прокладання кабелів для датчиків, як правило, знаходиться в межах від 50 до 90% від загальної вартості системи, тому розгортаючи бездротові сенсорні мережі можна значно знизити загальну вартість системи. Бездротові вузли, що містять у своїй основі технологію MEMS, за прогнозами, забезпечать ще більше зниження вартості системи. У перспективі бездротові датчики можуть інтегруватися прямо у вироби, такі як меблі та стельові плитки, що призведе до покращення контролю навколишнього середовища всередині приміщень.

Мережі WSN, які використовуються для забезпечення енергетичного моніторингу та управління, покращують умови проживання для мешканців будівлі завдяки покращенню продуктивності та безпеки, якості повітря,

теплового комфорту та здоров'я. Одночасні вони здатні зменшити споживання електроенергії, яке необхідне для підтримки комфортних умов у приміщенні. Витрата енергії, яка використовується з метою освітлення, становить близько 50 % від усієї споживаної електроенергії комерційних приміщень. У більшості будинках основною частиною таких витрат вважається зайве освітлення. Це факт обумовлюється тим, що звичайні вимикачі світла є витратними для установки, їх нелегко адаптувати до запитів, що змінюються; оскільки одним вимикачем контролюються багато світильників, і у споживача відсутня можливість контролю освітлення на кожному робочому місці. До складу WSN системи включаються бездротові вузли, що мають датчик присутності, а також реле, які здатні вимикати та включати освітлення залежно від присутності співробітників на робочому місці [12].

Використовуються бездротові системи контролю освітлення для модернізації систем управління будівлі, а також реалізації нових. Дані WSN застосовують бездротові вузли, які встановлюються у персональних освітлювальних приладах спільно з віддаленими бездротовими вимикачами, які здійснюють контроль світильників. Щоб сформувати комплексну систему необхідний бездротовий сенсор із такими характеристиками:

– підтримка бездротових мережних інтерфейсів;

– підтримка деякої кількості датчиків, таких як звук, світло, температура, потоку і локалізації;

– підтримка програмного забезпечення керування будинками;

– існування інтегрованого джерела енергії, що дозволяє вузлу самостійно функціонувати тривалий час.

У промисловій автоматизації поєднуються такі програми:

– сенсорна програма для вдосконалення управління активами методом безперервного моніторингу критичного обладнання;

– сенсорний додаток для мереж моніторингу, спрямованих на підвищення персональної та громадської безпеки;

– сенсорна програма для виявлення обладнання з низькою продуктивністю або малоефективних операцій;

– сенсорна програма для автоматизації збору даних від віддалених датчиків, щоб зменшити втручання користувача;

– сенсорний додаток зменшення витрат на електроенергію за допомогою найбільш раціональних виробничих процесів;

– сенсорний додаток для розширення надійності системи управління процесами наявного виробництва;

– сенсорна програма для впорядкованого збору даних, щоб покращити процес звітності;

– сенсорний додаток для надання детальних даних щодо вдосконалення програм профілактичного обслуговування.

На рисунку 1.6 представлені елементи автоматизації промислового підприємства.

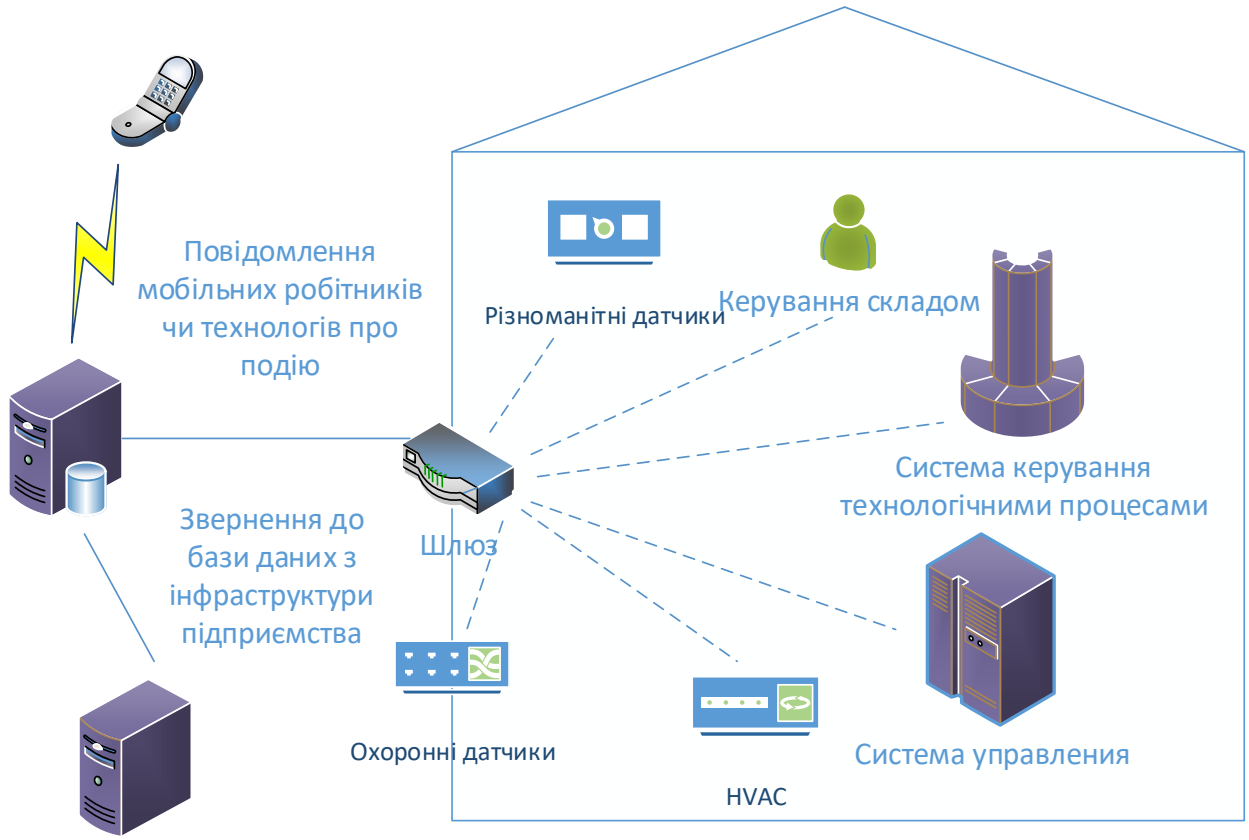

Рисунок 1.6 – Компоненти мережі автоматизації промислового підприємства

У ці системи включені деякі специфічні завдання, які також реалізуються на основі мереж WSN:

– система віддаленої діагностики;

– система обробки матеріалу;

– обслуговування технологічного процесу, лінії збирання;

– послуги з управління та профілактичного обслуговування обладнанням;

– управління автопарком, склади.

У районах, що мають високу сейсмічну активність, важливе значення має контроль руйнування промислових об'єктів. Щоб здійснити моніторинг подібних об'єктів, також використовують систему, засновану на сенсорних мережах. Здійснюючи контроль приміщень за зовнішнім периметром, встановлюються датчики, які постійно контролюють стан будівель. Шлюзом виступає існуюча WSN мережа, і здійснює передачу даних виділений сервер [13].

Якщо є необхідність виконати контроль стану моста, то по всій його довжині формується мережа сенсорів, залежно від розмірів моста можуть встановлюватися кілька шлюзів. Здійснюючи передачу даних для подальшої обробки, слід застосовувати одну з бездротових методик доступу, нею може бути передача пакетів у мережах стільникового зв'язку 2G/3G або безпроводового мережі доступу на базі технології WiMax/LTE.

Галузь транспортних перевезень отримала великі переваги підвищення рівня моніторингу. Наведемо приклад. Транспортні компанії щорічно зазнають великих матеріальних втрат через затори на автошляхах. Рішення Traffic Pulse Technology, розроблене корпорацією Traffic.com, є прикладом мережі WSN, яка призначена для контролю ситуації на автошляхах. Мета даної системи, яка використовує стаціонарні бездротові вузли, полягає у збиранні даних за допомогою сенсорної мережі, обробці та збереженні в

єдиному сховищі даних, та розповсюдженні таких даних за допомогою різноманітних додатків. Орієнтовано рішення Traffic Pulse на відкритому повітрі. Рішення гарантує збирання даних реальному часі (наприклад, контроль рівня забруднення чи перевірка температури). Система встановлюється вздовж головних автомагістралей, цифрова сенсорна мережа здійснює збір даних про зайнятість смуг, швидкість руху по кожній смузі, а також враховує кількість автотранспортних засобів. Такі базові дані дають можливість розрахувати час проїзду та середню швидкість. Далі отримані вимірювання прямує до центру обробки даних з метою переформатування. Мережа здійснює контроль автомобільних доріг безперервно за принципом 24/7 та надає в масштабі реального часу оновлення центр обробки даних. Системою здійснюється збір основної інформації про рух, включаючи швидкість руху автотранспортних засобів, його кількість та щільність зайнятості автошляхів. За допомогою бездротової мережі дані передаються кожні 60 секунд.

Убудь–якому великому населеному пункті Traffic.com підтримується оперативним центром Traffic Pulse, якому надходять у реальному часі звіти про інциденти на дорогах та ремонтних роботах. Така інформація доповнює дані, отримані від датчиків. Інформація кожному центру відправляється за допомогою різноманітних способів: мобільних підрозділів, літальних апаратів, відео, моніторингу екстремальних ситуацій на службових частотах. Для поширення цієї інформації застосовуються всілякі програми. Перерахуємо основні:

– індивідуальні інформаційні провайдери в Америці: компанія в режимі реального часу надає придбані дані різноманітним урядовим та комерційним програмам;

– телематика: придбані дані запитуються навігаційними транспортними пристроями, які здатні не лише вказувати маршрути, а й здійснювати вибір альтернативних шляхів при пробках на автомобільних дорогах.

Використовуються WSN мережі також для охорони зоопарків, заповідників, парків та інших місць відпочинку. На великій території розміщено комплексні датчики температури, вологості диму, які створюють бездротову мережу самостійно. У ряді місць організуються шлюзи передачі сигналів тривоги.

У разі пожежі дані про неї передаються автоматично до пожежної служби. Щоб ця система коректно функціонувала, слід знати місце розташування сенсора. Щоб швидко визначити зону займання, необхідно сформувати локальну систему позиціонування сенсорів. З цією метою виділяється деяка кількість сенсорних вузлів, розташування яких відомі і є незмінними. Доцільніше розміщувати прикордонні вузли в точках із відомими координатами. Потім за допомогою тріангуляції вузли, що залишилися, зможуть визначати свої координати, зорієнтувавшись на встановлені вузли [13].

Крім цього цю мережу можна застосовувати для моніторингу переміщення персоналу або контролю поведінки тварин, а також у будь-якому іншому додатку, який вимагає визначення розташування об'єкта та спостереження за ним.

Бездротові сенсорні мережі доцільно застосовувати при боротьбі з лісовими пожежами, щоб контролювати лінію поширення пожежі.

1.3 Перспективи розвитку бездротових сенсорних мереж

Всепроникні бездротові сенсорні мережі (USN) вважаються однією з найперспективніших технологій у 21 столітті. «Розумні» та недорогі сенсори у значних кількостях об'єдналися в бездротову мережу, яка підключена до глобальної телекомунікаційної мережі, у перспективі нададуть неймовірні за переліком послуг для управління та контролю будинків, підприємств, автотранспорту, організмів та ін. Крім цього, USN знайдуть широке

використання таких стратегічно важливих галузях як боротьба з тероризмом, управління надзвичайними та кризовими ситуаціями, військова стратегія та ін. Наприклад, і на тілі людини. Щоб підтримати задані характеристики, будь–який сенсор повинен створюватися відповідно до певної архітектури, в яку як головні компоненти входять: джерело живлення, антена, пам'ять і сенсорний пристрій.

Передбачається і безпосереднє використання сенсорів у життєдіяльності самої людини, зокрема: контроль місця знаходження тварин, контроль медичних характеристик, у тому числі при вільному пересуванні людини, контроль особистісних характеристик та розташування за допомогою сполучених з людиною сенсорів. Щоб реалізувати ці цілі, існують проекти, які пропонують вбудовувати сенсори в нашийник та/або повідець собаки, взуття людей, та ін.

Не беручи до уваги малоприємні моральні аспекти подібного розвитку мережі, все ж таки, необхідно відзначити, що цей технологічний розвиток, безсумнівно, спричинить дещо інші характеристики в суспільстві, яке вже залишить стадію електронного. Зважаючи на всепроникний характер сенсорних мереж, можна абсолютно доречно охарактеризувати подібне суспільство як ubiquitous.

На етапі активного розвитку методики NGN мережеві структури USN перебували в NGN як складовий компонент. Тоді було прийнято вважати, що база користувача USN становитиме не одну сотню мільйонів сенсорних вузлів. Але, блискавичний розвиток цієї інноваційної технології, виникнення концепцій Інтернету речей (IoT) та Інтернету речей (WoT), стимулювали переглянути перспективи розвитку сенсорних мереж. За сучасними прогнозами до 2020 року кількість бездротових пристроїв становитиме 7 трильйонів на 7 мільярдів осіб [14].

Зараз USN мережі використовуються в автоматизації будівель, датчиках військових мереж, агрокультурі, АСУТП, логістиці, транспортних мережах,

для отримання даних довкілля, у контролі зростання тварин і рослин тощо.

Передбачуване принципова зміна бази користувача підштовхнуло світове телекомунікаційне співтовариство переглянути концептуальні основи створення мереж зв'язку, враховуючи істотне переважання в базі користувачів майбутнього конструкцій, біомас, пристроїв та ін.

У наші дні сектором стандартизації Міжнародного Союзу Електрозв'язку розглядається можливість заміни концепції NGN на концепцію Розумних Всепроникних Мереж (SUN), яка включає концепцію NGN як один із складових компонентів.

У складі концептуальної моделі SUN складаються Інтернет речей (IoT), мережа NGN, яка модернізована до ступеня підтримки міжмашинних комунікацій (MOC), транспортні мережі VANET, наносіти та мережі пристрій, тобто. пристрій (M2M).

Інтернет речей містить у собі мережеві структури USN, створені з урахуванням протоколу 6LoWPAN (Low energy IPv6 based Wireless Personal Area Networks protocol). Протоколом 6LoWPAN допускається присвоєння IP адреси сенсорним вузлам, і навіть RFID чи його групам. Ця можливість перетворює USN з використанням IP адресації в основу Інтернету речей.

Веб речей вважається складовим елементом Інтернету речей та дає можливість здійснювати моніторинг та керування речами за допомогою сторінок WWW. Ключова роль структурі організації Інтернету речей відводиться брокеру Інтернету вещей. Брокер дозволяє використовувати інтернет речей як для речей спочатку пристосованих для цього, так і для речей, яким знадобляться відповідні шлюзи, наприклад, для речей, що діють за протоколами Bluetooth або ZigBee. Програми (Веба речей поділяються на управління, моніторинг, послуги, включаючи змішані.

Головна відмінність M2M від IoT полягає в тому, що M2M забезпечує підтримку всіляким взаємозв'язкам між пристроями, для яких IP адреса не вважається необхідною умовою організації з'єднань.

Як пристрої, які не підтримують адресацію IP, розглядалися сенсорні вузли та RFID, що діють за протоколом Bluetooth, IEEE 802.15.4 та UWB пристрою. Звичайно, що існування відповідних шлюзів подібні пристрої (речі) мають можливість приєднуватися і до мереж IoT.

Мережі автотранспортних засобів VANET вважаються одним із найбільш перспективних напрямків у розвитку систем бездротового доступу. Мережі VANET належать до категорії мобільних Ad hoc мереж MANET, незважаючи на те, що вони мають деякі особливості, як з позиції використання, так і з позиції протоколів. Важливо, що, незважаючи на назву VANET, у цих мережах передбачається не тільки режим функціонування Ad hoc, а й комбінований, при якому елементи мережі VANET мають можливість зв'язуватися з інфраструктурними вузлами мережі [16].

1.4 Висновки до першого розділу

Проаналізувавши передові концепції розвитку мереж зв'язку загального користування, визначено найперспективніші: всепроникні (бездротові) сенсорні мережі та Інтернет речей, що спричинило обґрунтований вибір актуального напряму досліджень. Для подальшого дослідження необхідно провести аналіз протоколів бездротових мереж для дослідження методів аналізу пропускної здатності у них.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ПРОПУСКНОЇ ЗДАТНОСТІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

2.1 Дослідження протоколів бездротових сенсорних мереж з погляду пропускної здатності

2.1.1 IEEE 802.15.4 WPAN

Мережі IEEE 802.15.4 є основою для побудови WSN [17]. Такі мережі часто називають LR-WPAN – низькошвидкісні бездротові персональні мережі.

У процесі розробки протоколу IEEE 802.15.4 пред'являлися такі вимоги, як надійність, простота в розгортанні, з простим протоколом та зниженим енергоспоживанням, що дозволяє тривалий час працювати пристроям від акумуляторних джерел живлення. При цьому запити щодо швидкості передачі та дальності дії вважаються досить простими. Окремі характеристики мереж стандарту 802.15.4:

– швидкості передачі 250 кБ/с, 40 кБ/с та 20 кБ/с;

– робота в топології зірка або кожен з кожним;

– застосування короткої 16–ти чи розширеної 64 бітної адресації;

– призначення забезпечених тимчасових інтервалів (GTS);

– застосування множинного доступу з контролем несучої та попередженням колізій (CSMA–CA);

– протокол із підтвердженнями для гарантованої передачі;

– невелике споживання електроенергії;

– знаходження сигналу (ED);

– індикатор якості каналу зв'язку (LQI);

– 16 каналів у смузі частот 2450 МГц, 10 каналів у смузі частот 915 МГц та 1 канал у смузі частот 868 МГц.

Існують два види пристроїв, що застосовуються в мережах 802.15.4: повнофункціональний пристрій (FFD) та пристрій, що має обмежені функції

(RFD). FFD може функціонувати в трьох режимах: координатор, координатор PAN або просто кінцевий пристрій. А FFD підтримує з'єднання з RFD або з іншими FFD на противагу RFD, який здатний здійснювати зв'язок тільки з FFD. Використання RFD обмежується елементарними програмами, такими як пасивний інфрачервоний сенсор або детектор світла; вони повинні здійснювати передачу великої кількості даних. Цими програмами одночасно підтримує лише одне з'єднання. Таким чином, RFD можуть реалізуватися при застосуванні мінімального числа ресурсів та розміру пам'яті [18].

Щоб створити WPAN мережу знадобиться зв'язок щонайменше двох пристроїв, один з яких FFD пристрій, який працює як PAN координатор. Отже, неможливо побудувати мережу IEEE 802.15.4 із одних RFD пристроїв.

Для бездротового зв'язку немає чіткої конкретної зони покриття, так як характеристики поширення є непостійними. Незначні зміни в напрямку або положенні руху можуть спричинити істотні відмінності в якості зв'язку і потужності сигналу. Це відбувається незалежно від того, стаціонарний або мобільний пристрій застосовується, оскільки об'єкт, що рухається, здатний вплинути на поширення хвиль від станції до станції.

Мережами IEEE 802.15.4 підтримуються два види архітектур побудови: кожен-з-кожним (однорангова) та зірка. На рисунку 2.1 зображено доступні типи архітектур. Зв'язок в архітектурі зірка встановлюється між пристроями та єдиним центральним контролером, який називається PAN координатором. Як правило, пристрої мають деякі супутні застосування і вважаються або вузлом початку передачі, або вузлом призначення для сеансів зв'язку в мережі. PAN координатор найчастіше застосовується виключно з метою маршрутизації повідомлень у мережі. Всі пристрої, які приєднані до мережі, незалежно від топології мають унікальну 64 бітну розширену адресу. Таку адресу можна застосовувати для безпосереднього встановлення з'єднання в межах мережі або його можна замінити короткою 16-бітною адресою, яка призначається PAN координатором в момент з'єднання пристрою з мережею. Отримує живлення

PAN координатор найчастіше від мережі на противагу іншим пристроям, які найчастіше живляться від батарей. Використання архітектури зірка вважається оптимальним рішенням для автоматизації будинку, індивідуального контролю за здоров'ям [25].

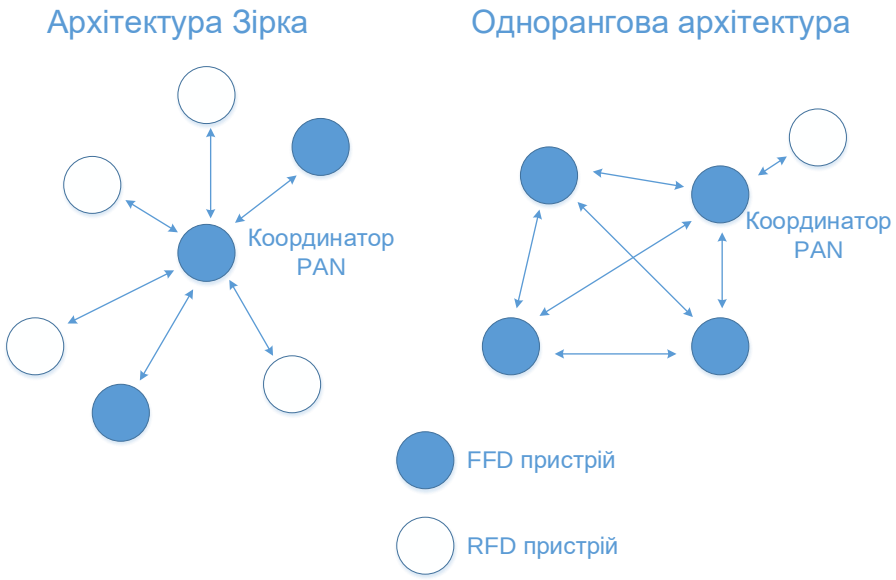

Рисунок 2.1 – Архітектура мереж 802.15.4

Крім цього одноранговa архітектура має PAN координатор, втім, така архітектура відрізняється від архітектури зірка тим, що кожен пристрій здатний спілкуватися з кожним іншим пристроєм, коли вони знаходяться в радіусі дії один одного. Одноранговa мережа надає можливість організації більш складної мережі, такий як мережу, що має пористу архітектуру (архітектура мережі, коли до кожного вузлу є два чи більше маршрутів). Однорангові мережі можуть бути самокерованими, самоорганізуються, спеціальними. Також вони дозволяють здійснити маршрутизацію повідомлення від одного вузла до іншого, проте дані функції виконуються за допомогою протоколів мережевого рівня.

Будь–яка незалежна мережа набуває унікального ідентифікатора. Такий ідентифікатор створює умови для зв'язку пристроїв усередині мережі,

застосовуючи коротку адресу, та передає дані між пристроями незалежних мереж.

Відповідно до семирівневої моделі OSI стек протоколів IEEE 802.15.4 містить у собі протоколи канального та фізичного рівнів.

Протоколом PHY надаються два сервіси: сервіс даних та сервіс обслуговування, який пов'язаний з елементом керування фізичним рівнем (PLME). Сервіс даних PHY надає можливість передачі та отримання протокольних одиниць обміну PHY (PPDU) за допомогою радіоканалу.

У PHY включені можливості активації та деактивації радіо приймача, виявлення сигналу (ED), перевірки якості зв'язку (LQI), вибору каналу, звільнення каналу, передачі та прийому пакетів за допомогою фізичного середовища.

Протоколом MAC також надається два сервіси: сервіс даних MAC та сервіс обслуговування, який пов'язаний з елементом керування рівнем доступу (MLME–SAP). Сервіс даних MAC надає можливість передачі та отримання протокольних одиниць обміну MAC (MPDU) за допомогою сервісу даних PHY.

Підрівень MAC має у своєму розпорядженні можливості управління синхронізацією, доступу до каналу передачі даних, обслуговування забезпечених тимчасових слотів, перевірки кадрів, доставки кадрів підтверджень, встановлення та руйнування з'єднань. Додатковою функцією підрівня MAC є можливість здійснення механізмів безпеки, які необхідні для застосування.

Стандартом IEEE 802.15.4 надається можливість опціонального застосування надциклової структури. Координатор визначає формат надциклу. Надцикл може обмежуватися маяком, сигнальним кадром, який передає координатор (рисунок 2.2) та ділиться на 16 однакових слотів. Передача сигнального кадру виконується на початку будь–якого надциклу. Коли координатором не використовується надциклова структура, передачу сигнального кадру може вимкнути. Призначаються сигнальні кадри, щоб

синхронізувати підключені пристрої, ідентифікувати мережу та дати опис структури надциклу. Кожен пристрій, який має намір здійснити передачу даних у період змагального доступу (CAP) між двома сигнальними кадрами, має отримати доступ до каналу, за допомогою слотованого механізму C8MA–CA. Необхідно всі транзакції завершити, перш ніж розпочнеться наступний сигнальний кадр [19].

У надциклу є активний та пасивний режим. У пасивному режимі координатор не здійснює зв'язок із мережею та здатний переходити в енергозберігаючий режим.

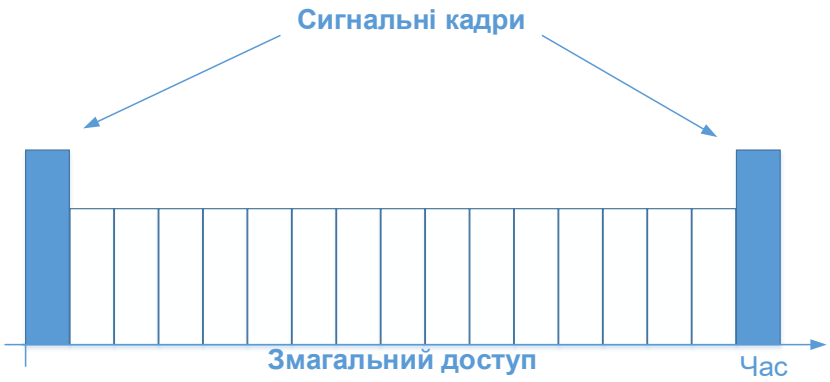

Рисунок 2.2 – Надциклова структура без використання GTS

Для таких програм, де необхідна гарантована смуга пропускання, координатором PAN може надаватися частина активного періоду. Виділений час отримав назву гарантованого тимчасового слота (GTS), з них формуватиметься період вільний від конкуренції (CFP), який розташований наприкінці надциклу (рисунок 2.3). Координатор PAN має можливість призначати до 7 періодів GTS і GTS здатний захоплювати більше одного тимчасового слота. Тим не менш, повинна залишитися конкретна частина часу, щоб здійснити асоціативний доступ інших мережевих вузлів або нових пристроїв, які мають намір приєднатися до мережі. Необхідно закінчити всі асоціативні транзакції, перш ніж настане CFP період. Також будь-який пристрій, який передається протягом GTS, повинен переконатися, що

транзакція перерветься до наступного наступного GTS або коли закінчиться період CFP.

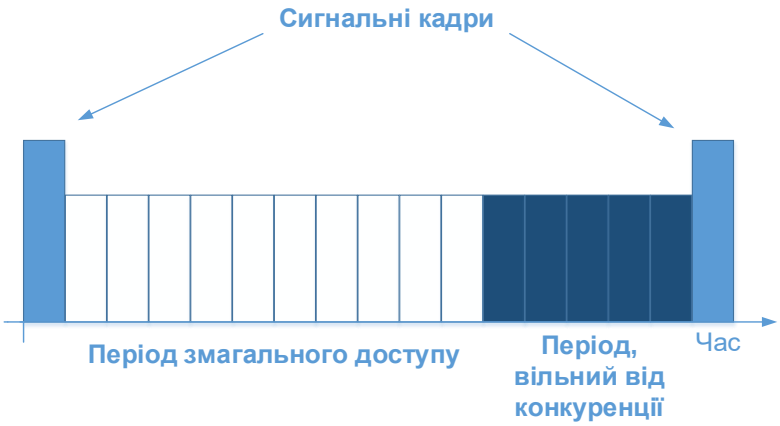

Рисунок 2.3 – Надциклова структура із застосуванням GTS

Є три види даних: передача даних від координатора, координатору і між двома пристроями. Усього два види передач можна застосовувати в топології зірка, оскільки обмін даними здійснюється виключно між координатором та пристроєм. В одноранговій топології є можливість здійснювати обмін даними між двома довільними пристроями, внаслідок цього в цій топології можуть застосовуватися всі три види транзакцій.

Якщо пристрій має намір виконати передачу даних у мережі із надциклами, спочатку ним прослуховується канал з метою очікування сигнального кадру. Якщо сигнал виявлено, пристрій здійснює синхронізацію із структурою надциклу. У відповідній точці за допомогою слотованого методу CSMA–CA пристроєм передається кадр даних координатору. Координатор за допомогою спеціального кадру підтвердження підтверджується успішний прийом. Цим транзакція закінчується. Послідовність зображено рисунку (рисунок 2.4).

Якщо пристрій має намір виконати передачу даних в асинхронній мережі, він просто здійснює передачу кадру даних координатору за допомогою неслотованого методу CSMA-CA. За допомогою спеціального кадру

підтвердження координатором підтверджується вдалий прийом кадру. Транзакцію на цьому закінчено. Послідовність зображено на рисунку 2.5.

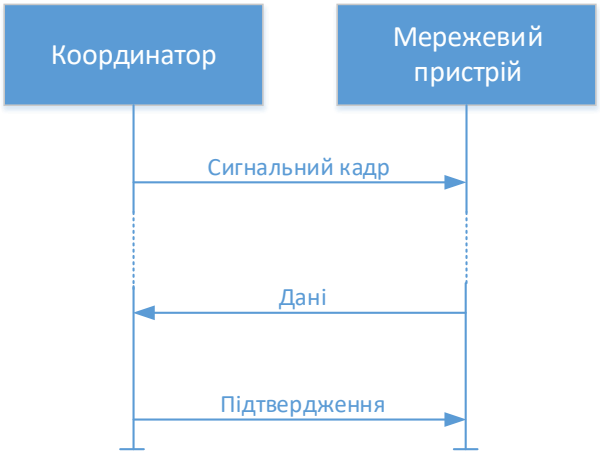

Рисунок 2.4 – Передача даних координатору у синхронізованій мережі

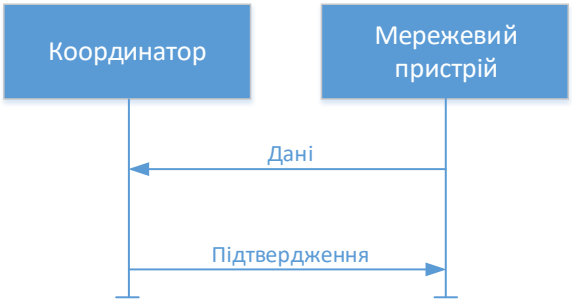

Рисунок 2.5 – Передача даних координатору асинхронної мережі

Коли координатор має намір здійснити передачу даних в мережі, що синхронізується, в сигнальному кадрі він вказує, що пристроєм очікується повідомлення. Сигнальний кадр проглядається пристроєм і, якщо очікуване повідомлення виявлено, передається MAC повідомлення запиту даних за допомогою неслотованого методу CSMA-CA. Координатором підтверджується запит і передаються дані. За допомогою спеціального кадру підтвердження пристроєм підтверджується успішний прийом даних.

На цьому транзакцію закінчено. Коли отримано підтвердження, повідомлення зі списку повідомлень, що очікують, у сигнальному кадрі видаляється. Послідовність зображено рисунку 2.6.

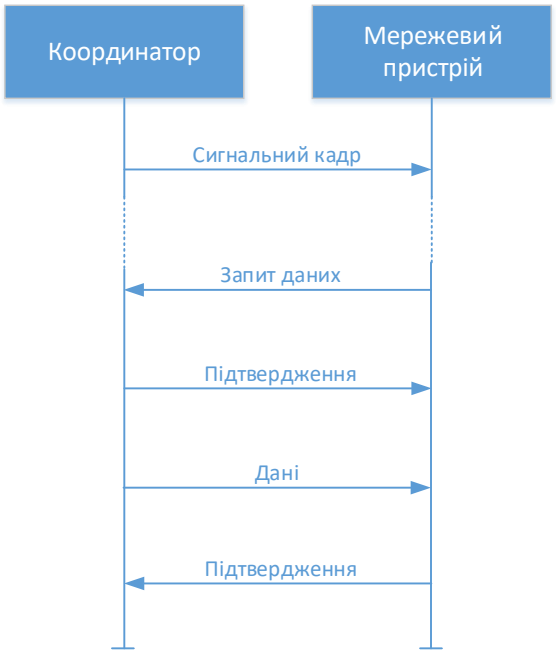

Рисунок 2.6 – Передача даних від координатора у синхронізованій мережі

Якщо координатор має намір здійснити передачу повідомлення в асинхронній мережі, він зберігає дані до тих пір, поки не запитає дані відповідний пристрій. Пристрій може здійснювати контакт, виконуючи за допомогою неслотованого методу CSMA-CA передачу MAC команди запиту даних координатору, із встановленою частотою додатком. За допомогою кадру підтвердження координатором підтверджується отримання запиту. Коли для пристрою, який надіслав запит, дані збережені, то за допомогою неслотованого методу CSMA-CA ці дані передаються. Коли дані для передачі відсутні, координатор здійснює передачу кадру даних з нульовим полем даних, щоб показати, що ніякі дані не збережені. За допомогою спеціального кадру підтвердження пристроєм підтверджується успішний прийом даних. На цьому транзакцію закінчено. Послідовність зображено рисунку 2.7.

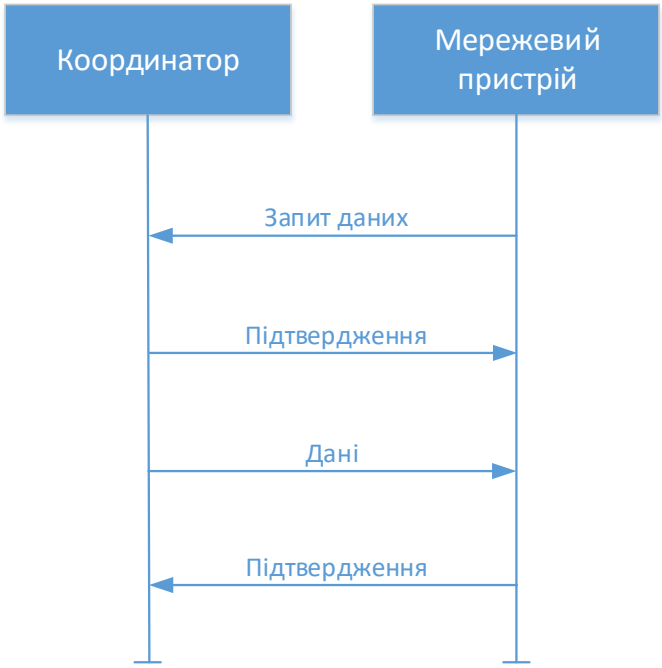

Рисунок 2.7 – Передача даних координатора в асинхронної мережі

В одноранговій мережі будь-який пристрій може зв'язуватися з будь–яким іншим пристроєм в області радіопокриття. Для ефективного встановлення зв'язку, пристрої, яким потрібно виконати з'єднання, повинні з'єднатися в певний період часу або здійснити взаємну синхронізацію. У наведеному вище прикладі пристроєм здійснювалася передача даних, за допомогою неслотованого методу CSMA-CA, проте для ефективної роботи слід виконати попередні заходи, щоб забезпечити синхронізацію. Такі дії реалізуються протоколами верхніх рівнів, які до стандарту IEEE 802.15.4 не належать.

Було розроблено структуру кадрів, щоб складність звести до мінімуму. У той же час кадри повинні бути досить завадовими для передачі в каналі, який має сильні шуми. Стандартом IEEE 802.15.4 виділяються чотири види структур кадрів [20]:

– кадр MAC команд призначається управління передачами;

– кадр підтверджень призначається на підтвердження успішного прийому;

– кадр даних призначається передачі корисних даних;

– сигнальний кадр використовує координатор передачі маяків.

Стандарт IEEE 802.15.4 передбачає низку механізмів, щоб підвищити надійність передачі даних. Це такі механізми як: механізм CSMA–CA, перевірки та підтвердження даних.

У LR-WPAN використовується два види доступу до каналу в залежності від конфігурації мережі. Неслотований механізм CSMA-CA застосовується в асинхронній мережі. Завжди, коли пристрій має намір виконати передачу MAC команди чи кадр даних, він повинен чекати випадкового періоду часу. Якщо після очікування канал вільний, то пристрій виконує передачу кадру, в іншому випадку пристрій чекатиме ще одного випадкового періоду часу, до того як здійснить спробу доступу до каналу. Кадри підтвердження передаються без застосування CSMA-CA механізмів.

Злоттований механізм CSMA-CA застосовується у синхронізованій мережі. У разі з передачі сигнального кадру починається період очікування. Завжди, коли пристрій має намір здійснити передачу кадру протягом CAP періоду, йому слід знайти межу (сигнальний кадр), а далі чекати на випадкове число тимчасових слотів. Коли канал пристрою зайнятий, слід знову чекати випадкового числа тимчасових слотів, перш ніж спробувати повторно отримати доступ. Коли канал вільний, пристрій починає передачу кадру. Потрібно передавати кадри підтвердження без застосування механізмів CSMA-CA.

Перевірка кадрів із даними чи кадрів управління, і навіть успішний прийом опціонально підтверджуються з допомогою спеціальних кадрів. Коли пристрій, що приймає, не здатний виконати обробку отриманих кадрів даних з тієї чи іншої причини, то повідомлення не підтверджується. Коли доказ не отримує джерело, він вважає, що передача не здійснилася і повторно передає кадр. Коли не отримано підтвердження і після низки спроб, джерело має вибір: або здійснити транзакцію знову або її припинити. Коли не потрібні кадри

підтверджень, джерело має на увазі, що передачу здійснено.

Щоб виявити бітові помилки в структурі кадрів, передбачається 16 бітне поле з метою перевірити надмірність циклічної суми (CRC).

При розробці протокол передбачалося застосування з живленням від акумуляторних пристроїв. Тим не менш, в окремих програмах частини пристроїв необхідне живлення від мережі. Пристроям, які живляться від батарей, слід застосовувати робочий цикл, щоб зменшити споживання енергії. Такими пристроями переважна більшість своєї життєдіяльності проводиться у сплячому режимі. Будь–який пристрій має періодично прослуховувати радіоканал, щоб виявити очікуване повідомлення. Подібним механізмом визначається баланс між часом очікування доставки повідомлень та споживанням електроенергії. Пристрої, які отримують живлення від мережі, мають у своєму розпорядженні можливість постійного контролю радіоканалу.

Контроль доступу вважається сервісом безпеки, який дозволяє пристрою здійснити вибір можливого встановлення зв'язку. У разі надання в мережі сервісу контролю доступу пристрій повинен скласти перелік контролю доступу (ACL), до якого заносяться пристрої, від яких існує можливість отримання кадрів.

У межах стандарту IEEE 802.15.4 шифрування даних є сервісом безпеки, який використовує симетричний шифр, щоб захистити дані від прочитання пристроями, які не мають криптографічного ключа. Дані можуть шифруватися з використанням ключа, який спільно застосовується у групі пристроїв (зазвичай зберігається як ключ за замовчуванням) або з використанням ключа відомого лише двом сторонам (зберігається в ACL). Здійснюється шифрування над корисним навантаженням кадру даних чи командного, сигнального кадрів [21].

Перевірка цілісності кадру є сервісом безпеки, який використовує код цілісності повідомлення (MIC), щоб захистити дані від модифікації сторонами, які не мають криптографічного ключа. Також сервіс забезпечує впевненість у

тому, що дані надійшли від пристрою, що має криптографічний ключ. Цей стандарт може забезпечувати цілісність кадрів даних, командних та сигнальних. Ключ, який використовується з метою забезпечення цілісності кадрів, може зберігатися у ряду пристроїв або двох сторін (зберігається у спеціальному записі ACL).

Оригінальність послідовності є сервісом безпеки, який використовує впорядковану черговість кадрів, що входять для того, щоб фільтрувати повторні пакети. У разі отримання кадру значення поточного номера порівнюється з відомим останнім номером. Коли отриманий номер буде новіше ніж збережений, то перевірка вважається пройденою і здійснюється оновлення номера, інакше кадр відхиляється. Даним сервісом гарантується, що дані нові дані, які були прийняті пристроєм до цього.

2.1.2 ZigBee

На базі стандарту IEEE 802.15.4 [22] було створено ряд стеків протоколів, призначених длясенсорних мереж. Максимального поширення на сьогоднішній день набув індустріальний стандарт ZigBee, розроблений підприємством ZigBee Alliance [24], у складі якого складаються провідні творці програмного забезпечення та обладнання для бездротових сенсорних мереж. У 2007 році було випущено останній варіант специфікації ZigBee. У процесі розробки стека протоколів ZigBee враховувалося багато досвіду провідних колективів творців, які працюють у галузі економічних, низькошвидкісних локальних, бездротових мереж. Специфікацією ZigBee забезпечується стандартизація організації бездротового зв'язку між пристроями від різних виробників у різноманітних галузях застосування. Специфікацією пропонуються методи, які сприяють швидкому розгортанню та впровадженню розподілених бездротових систем управління та спостереження. Такі методи нагадують добре відомі методи у провідних індустріальних мережах і створюються на концепції профілів пристроїв.

Специфікацією інтегровані найкращі практики та моделі, які прийняті при створенні локальних розподілених систем управління, їх обслуговуванні та використанні:

– відкритість для впровадження інтеграторами своїх технологій та протоколів на основі сервісів, які надає ZigBee;

– високий рівень захищеності інформації – криптографічний захист на трьох ступенях стека, ідентифікація вузлів мережі;

– вирішення питань якості зв'язку – при незадовільній якості зв'язку існує можливість встановлення додаткових роутерів;

– вирішення питань живучості мережі – у разі якщо втрачено зв'язок із вузлами мережі, мережа перебудовується, змінюючи маршрутизацію і структуру. Легко передбачається дублювання координатора у разі втрати зв'язку з головним координатором;

– простота спостереження за мережею і оптимізація її структури з допомогою спеціальних методів адміністрування;

– простота установки та налагодження – кінцеві пристрої мережі оголошують про можливості та сервіси, які вони надають, та за допомогою координатора розшукують пристрої, з якими їм необхідно взаємодіяти, щоб виконати цільові завдання управління;

– функціональна масштабованість – одну мережу можна використовувати у великій кількості систем управління одночасно, та їх різноманітність та кількість можна елементарно нарощувати, не змінюючи програмне забезпечення та переналаштування координатора мережі та роутерів;

– просторова масштабованість – можливість збільшення кількості вузлів мережі до 64 тисяч.

Архітектура стека ZigBee [25], зображена на рисунку 2.8, містить у своїй основі семирівневу модель OSI, проте регламентує лише ряд шарів. Стандартом IEEE 802.15.4-2003 визначаються два нижні рівні: рівень

контролю доступу до середовища (MAC) та фізичний (PHY) рівень. Взявши за основу цей стандарт, альянс ZigBee створив специфікацію, яка регламентує мережевий рівень (NWK), та структуру прикладного рівня. До складу прикладного рівня входить рівень підтримки об'єктів ZigBee пристроїв (ZDO), додатків (APS) та об'єктів встановлених виробником.

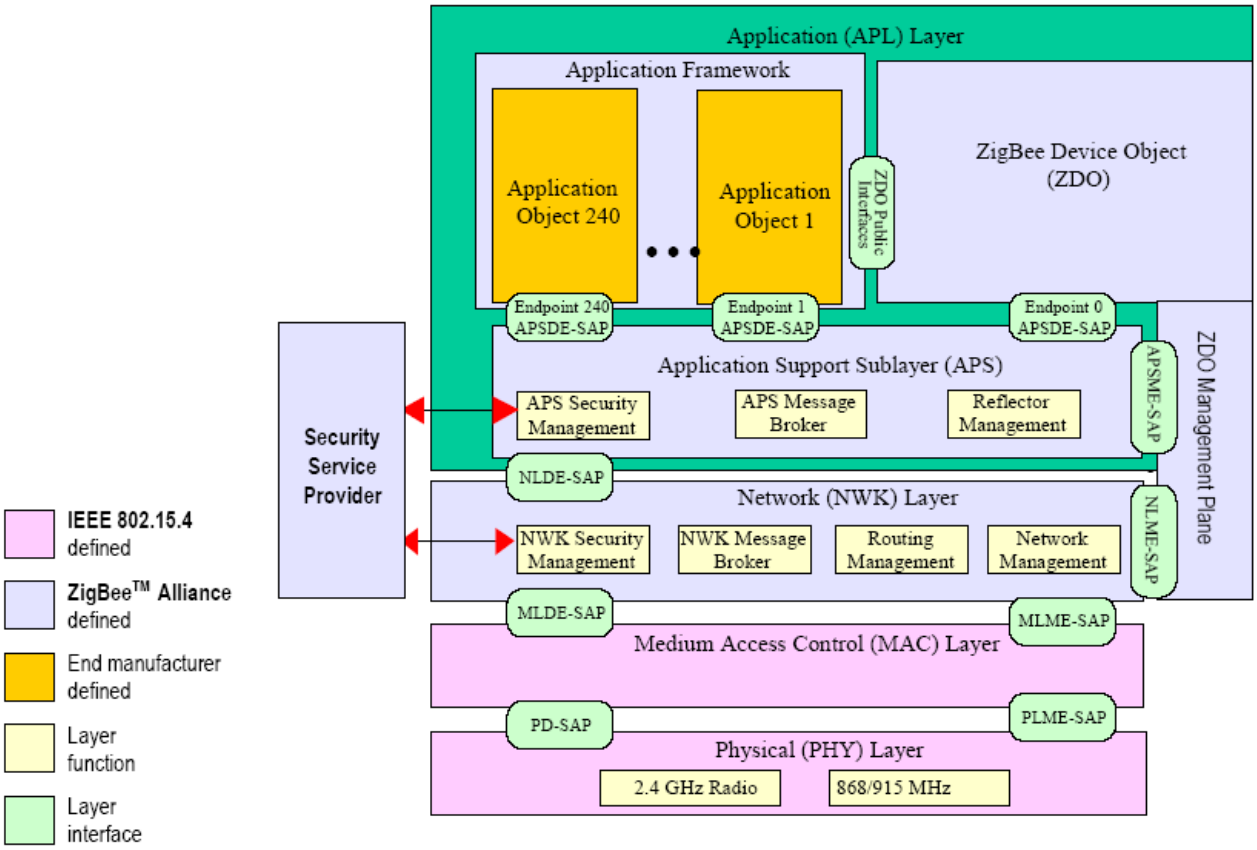

Рисунок 2.8 – Архітектура стека ZigBee

Пояснення до рисунка: Security Service Provider – сервіс безпеки, APL – прикладний рівень, ZDO – об'єкт ZidBee пристрій, Application Object – об'єкт програми, Endpoint – контрольна точка, ZDO Management Plane – управління ZDO, APS – підрівень підтримки додатків, Security Management – управління безпекою, Message Broker – управління повідомленнями, Reflektor Management – сортування повідомлень, NWK – мережевий рівень, Routing Management – управління маршрутизацією, Network Management – управління мережею,

MAC – рівень контролю доступу до несучої, PHY – фізичний рівень.

До обов'язків мережевого шару NWK включені механізми, що застосовуються для:

– збереження необхідних даних про сусідів;

– виявлення найближчих сусідів;

– виявлення та сервісу маршрутів між пристроями;

– здійснення маршрутизації кадрів до адреси призначення;

– використання засобів безпеки для кадрів;

– підключення до мережі та від'єднання від неї.

Крім цього NWK рівень ZigBee координатора відповідає за ініціалізацію нової мережі, і призначає адреси новим пристроям, що підключаються.

Основним призначенням рівня підтримки додатків APS вважається забезпечення зв'язку мережевого рівня NWK з об'єктами додатків. До його обов'язків входять:

– фрагментація, складання та надання надійної передачі даних;

– порівняння 16 бітної NWK адреси та 64 бітної IEEE адреси;

– встановлення групової адреси, фільтрацію та доставку групових повідомлень;

– передача повідомлень між прикордонними пристроями;

– обслуговування таблиць зв'язку (біндингу), обумовлених як можливість порівняти два пристрої.

Підрівнем ZigBee пристроїв надається найпростіший комплекс функціональних можливостей, щоб забезпечити інтерфейс між профілями пристроїв, об'єктами програми та підрівнем APS. До обов'язків підрівня ZDO включаються:

– виявлення пристроїв у мережі та встановлення, які послуги вони надають;

– керування сервісами безпеки;

– ініціалізація та/або відповідь на запит зв'язку (біндинг);

– встановлення ролі пристрою у мережі (кінцевий пристрій чи координатор).

Мережа ZigBee має три типи логічних пристроїв: координатором ZigBee, маршрутизатором ZigBee і кінцевим пристроєм ZigBee. З'єднанням як мінімум двох пристроїв, одним з яких є координатор ZigBee, утворюється мережа ZigBee.

Координатором ZigBee вважається повнофункціональний пристрій, який є координатором PAN. Від топології мережі залежить його функції.

Маршрутизатором ZigBee вважається повнофункціональний пристрій, що не є координатором ZigBee, втім, може виступати як координатор стандарту IEEE 802.15.4 всередині своєї сфери радіодоступу та маршрутизатора повідомлень між пристроями в мережі ZigBee.

Кінцевим пристроєм ZigBee прийнято вважати будь–який пристрій стандарту IEEE 802.15.4 (RFD та FFD), який не є маршрутизатором ZigBee ні координатором [26].

Мережевим рівнем ZigBeї підтримуються архітектури дерево, зірка та пориста (рисунок 2.9).

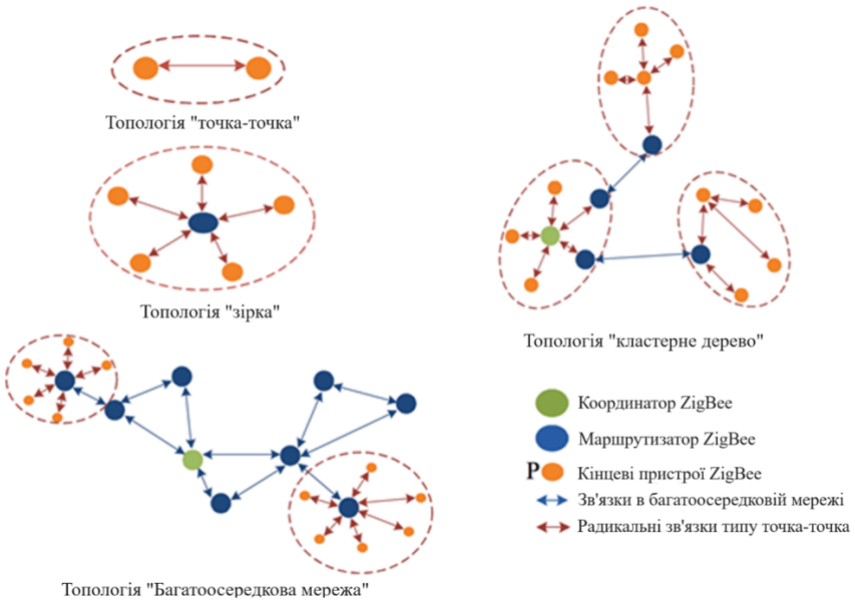

Рисунок 2.9 – Архітектура ZigBee мереж

Контроль мережі в архітектурі зірка здійснюється одним пристроєм, який називається координатором ZigBee. Координатор ZigBee відповідає за ініціалізацію та сервіс пристроїв у мережі. Всі інші пристрої, відомі як кінцеві пристрої, спілкуються безпосередньо з координатором ZigBee. В архітектурі дерева та ніздрюватій архітектурі ZigBee координатор відповідає за ініціалізацію мережі та здійснення вибору ряду основних характеристик мережі, таких як використовуваний радіоканал та ідентифікатор мережі, проте дана мережа здатна розширюватися за рахунок застосування ZigBee маршрутизаторів. У мережі, яка має архітектуру дерева, повідомлення управління та дані передаються через мережу із застосуванням ієрархічної стратегії для вибору маршруту, і може здійснюватися під централізованим управлінням. Для цієї мети фізично необхідно застосовувати сигнали маяків, що періодично видаються координаторами IEEE 802.15.4. У пористих мережах використовуються однорангові зв'язки. Маршрутизація у цих мережах вважається децентралізованим та розподіленим через мережу процесом. У пористих мережах ZigBee маршрутизатори маяків IEEE 802.15.4-2003 не передають.

ZigBee мережі вважаються такими, що самоорганізуються. Коли вибір первинних установок та координатор мережі увімкнені, всі інші пристрої самостійно здійснюють підключення. Спочатку координатором визначається рівень енергії на всіх частотних каналах, які доступні. Вибирається канал, який має мінімальний рівень енергії. Після вибору каналу координатором визначаються в ньому наявність інших функціонуючих мереж ZigBee та їх ідентифікатори за допомогою спілкування з вузлами таких мереж. Далі координатором випадково вибирається ідентифікатор для власної мережі з діапазону 0x0000-0x3FFE таким чином, щоб не було його збігу з ідентифікаторами інших мереж у цьому ж частотному діапазоні. Мережева 16–бітна адреса координатора постійно дорівнює 0x0000. Потім координатор дає

дозвіл на приєднання до своєї мережі іншим пристроям. Координатор, виконавши приєднання деякої кількості перших маршрутизаторів та кінцевих пристроїв, не приєднує інших безпосередньо до себе. Не приєднаним необхідно знаходити вже приєднані до координатора маршрутизатори (у кінцевих пристроїв відсутня можливість будь–кого приєднувати) та здійснити приєднання до них. За допомогою цього алгоритму процес розгортання мережі полегшується, час введення мережі в експлуатацію скорочується. Специфікацією передбачається і спосіб заздалегідь запрограмованого приєднання пристроїв до координатора і маршрутизатора.

У момент під'єднання до мережі пристрій набуває унікального в рамках подібної мережі 16–і розрядна мережна адреса. Враховуючи цей факт, мережа може мати близько 64 тисяч вузлів. При необхідності формування мережі з великою кількістю вузлів організовується ряд мереж, які зв'язуються між собою за допомогою шлюзу.

Залежно від вибраного типу топології мережі існує кілька методів маршрутизації в ZigBee мережі. Першим методом маршрутизації в мережах ZigBee вважається ієрархічна маршрутизація по гілках деревоподібної структури. Ієрархічна маршрутизація за умовчанням застосовується усіма маршрутизаторами і координаторами, якщо вони відсутні чи закінчилися ресурси підтримки інших типів маршрутизації.

Ще одним видом маршрутизації можна вважати пористу (mesh) маршрутизацію. Комірчасту маршрутизацію підтримують лише координатор та роутери, кінцеві пристрої в ній участі не беруть. Кінцеві пристрої виконують передачу пакетів даних лише своїм батьківським вузлам, так як вони не мають таблиці маршрутизації. Коли роутери отримують пакет даних, який не призначений для його вузла–батька або вузла–нащадка і в таблиці маршрутизації відсутня відповідний запис, вони ініціюють процес виявлення маршруту. Починається виявлення маршруту з того, що надсилаються відповідні широкомовні команди всім маршрутизаторам, які знаходяться в

межах радіовидимості. Всі маршрутизатори мережі, які прийняли команду, створюють тимчасові записи про прийнятий запит і відрізняються неналагодженістю (навмисно забезпечується таймерами, що мають випадково обрану затримку) широкомовно здійснюють ретрансляцію команди далі. З метою не перетворити широкомовну ретрансляцію на «радіошторм», пакети мають лічильник максимальної кількості ретрансляцій, який знижується на 1 при проходженні пакета через будь-який маршрутизатор.

Існує безліч маршрутів проходження пакетів до вузла призначення, однак кожним маршрутизатором на шляху прямування відкидаються і не ретранслюються пакети з командами виявлення маршруту, які мають більшу вартість шляху, ніж вже зафіксована цим маршрутизатором у попередніх пакетів. Коли пакет має однакову вартість шляху, що маршрутизатор уже був зафіксований, то їм оновлюються дані в таблиці виявлення маршруту. Перевага надається останньому. Знаходиться вартість шляху в самому пакеті і оновлюється в ньому завжди, коли маршрутизатор виконує його ретрансляцію.

Специфікацією пропонуються різноманітні варіанти розрахунку вартості колії. Найбільш елементарним вважається простий підрахунок числа ретрансляцій за маршрутом. Більш складним вважається варіант обчислення вартості колії за сумою критеріїв якості зв'язку між вузлами за маршрутом LQI. Найважче реалізованим і найбільш правильним буде вважатися варіант підсумовування функцій від можливості проходження пакетів між вузлами, яка обчислюватиметься зі статистичних даних.

Маршрутизатор, який є батьківським вузлом пункту призначення типу RFD або пунктом призначення пакетів команди виявлення шляху, при отриманні пакета направляє пакет із командою підтвердження. Такий пакет направляється ініціатору маршруту згідно з відомою адресою та проходить зворотним шляхом, раніше прокладеним. На цей момент усіма проміжними маршрутизаторами шляхом проходження пакета формується новий запис маршруту. Пакетом підтвердження, що проходить, встановлюється статус

такого запису маршруту в активний стан. Досягши ініціатора виявлення маршруту, пакет підтвердження закінчує процедуру організації маршруту, після якої у всіх проміжних вузлах ліквідовуються всі тимчасові записи в таблицях виявлення маршруту, а записи таблиць маршрутизації у вузлах зберігаються у пам'яті [27].

З допомогою розглянутого вище алгоритму сіткової маршрутизації створюється односпрямований шлях. Якщо в стеку ZigBee постійна nwkSymLink має значення TRUE, то і для зворотної передачі буде застосовуватися цей шлях, в іншому випадку для виявлення зворотного шляху необхідно повторно запустити алгоритм маршрутизації. Вочевидь, що зворотний шлях може збігтися з прямим, у разі розрахунку вартості шляхом елементарного лічильника переходів, оскільки вибираються розгалуження по маршруту з урахуванням генератора випадкових затримок.

Специфікацією 2006 року запроваджено ще два методи маршрутизації. Це маршрутизація виду багато до одного та групова маршрутизація. Необхідністю в них послужила нестабільність великих мереж, що виявляється при ряді умов, що мають сіточну маршрутизацію.

Здійснюючи контроль параметрів мереж, намагаючись досягти прогнозованого часу доставки повідомлень, творець мережі мінімізує кількість вузлів, через які пакет має можливість проходження від джерела до одержувача. Однак специфікацією не вносяться жодні обмеження, і теоретично є можливість побудови мережі з необмеженою кількістю проміжних вузлів.

Будь–який пристрій на рівні NWK має лічильник помилок для всіх вихідних з'єднань, які здійснюють передачу даних. Коли значення лічильника перевищуватиме конкретний параметр, то з'єднання відзначається як збійне та пристрою необхідно ініціювати процес відновлення маршруту. Автор реалізації стека має можливість вибору або застосування найпростішої схеми, що має лічильник, або найбільш точну схему, яка заснована на тимчасових

вікнах.

Отже, здійснюється важлива властивість сенсорних мереж – самоусунення несправностей (self–healing). Динамічна переконфігурація маршрутів при виході з ладу або відключення електроживлення окремих вузлів дає можливість сенсорної мережі самостійно забезпечити безвідмовну доставку даних до центру обробки інформації протягом тривалого періоду.

Дані, отримані з сенсорів, слід обробляти і виводити у затребуваному користувачем вигляді. Обробляти дані безпосередньо на місці збору нераціонально, оскільки обмежена потужність мікрокомп'ютера (сенсора). Щоб встановити зв'язок із мережею зв'язку загального користування, створюються шлюзи, які передають потік даних із сенсорних мереж на віддалений центр обробки та збереження інформації. При спостереженні за довкіллям це може виконувати GSM модем чи Ethernet інтерфейс підключення до локальної інфраструктури. Після обробки дані зберігаються на конкретному сервері і можуть бути потрібні клієнтською програмою або користувачем за допомогою Інтернету.

Крім цього, нерідко потрібно забезпечити узгоджену роботу двох і більше розподілених у просторі сенсорних мереж. У такому випадку за допомогою шлюзу інтерфейс організується в транзитну мережу будь–якої з сенсорних мереж. Транзитною мережею може бути глобальна мережа Інтернет чи мережу NGN, захищені корпоративні мережі чи спеціально організований радіоканал передачі на значні відстані. На рисунку 2.10 зображено стандартний приклад взаємодії з МЗЗК [28].

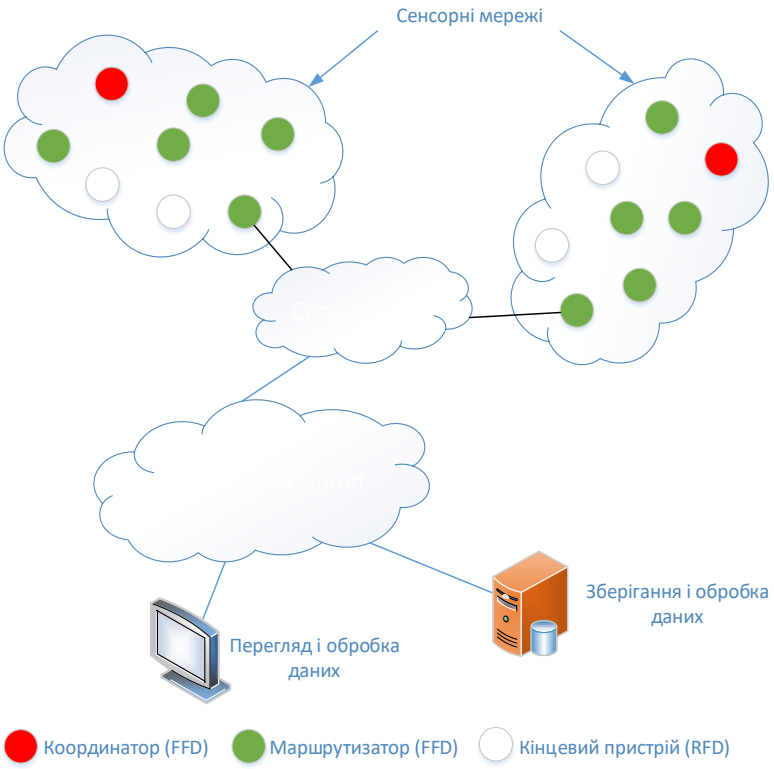

Рисунок 2.10 – Взаємодія із мережею зв'язку загального користування

На сьогоднішній день розроблено та випущено шлюзи, які дозволяють здійснювати передачу даних із ZigBee мережі в GSM мережі мобільних операторів, провідні TCP/IP мережі, мережі стандарту IEEE 802.11a/b/g. У випадку, якщо жодна з готових версій шлюзів не підійде, можна підключити модуль ZigBee до комп'ютера за допомогою інтерфейсу USB або RS232 і передавати інформацію за допомогою будь–якого мережного інтерфейсу, який доступний на комп'ютері (рис. 2.11).

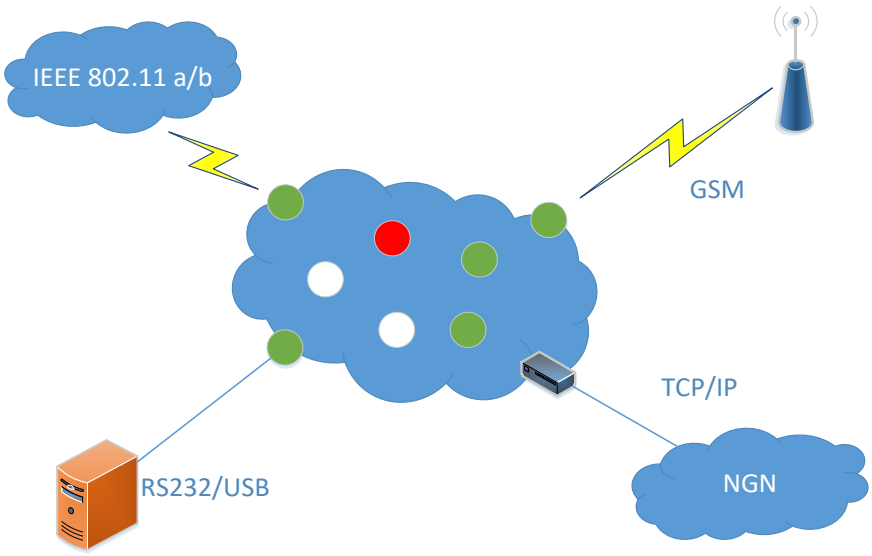

Рисунок 2.11 – Взаємодія з різними мережами

2.1.3 6LoWPAN

До останнього часу в бездротових сенсорних мережах використовувати IP підхід було неможливо, так як IP протокол не масштабувався для роботи на мікроконтролерах з каналами, що мають обмежену енергію, таких як радіоканал IEEE 802.15.4 [20]. Пакети, що використовуються у IEEE 802.15.4, досить невеликі. Весь стек протоколів повинен використовувати незначний обсяг пам'яті.

Значні зміни зробив проект стандарту IETF 6LoWPAN [29], який рекомендує передачу повідомлень IPv6 поверх IEEE 802.15.4 і випущений у березні 2007 року. Можливості 6LoWPAN для роботи з пристроями з невеликим електроспоживанням робить його кращим для застосування не тільки в портативній техніці, а й у широкому спектрі промислових засобів. Інтегрована підтримка шифрування AES–128 створює основу для надійної ідентифікації та безпеки. З метою конкурентоспроможності по відношенню до інших протоколів, у 6LoWPAN використовується схема стиснення заголовків типу «плати тільки за те, що використовуєш» [30]. Здійснюючи пряму інтеграцію з IP маршрутизаторами, можна отримати перевагу у застосуванні найбільш прогресивних мережевих систем безпеки, на відміну від шлюзів, що

пропонуються в ad hoc мережі.

Група творців IETF 6LoWPAN була створена для вирішення питань передачі IP пакетів поверх каналів IEEE 802.15.4 методом, який відповідає відкритим стандартам і надає взаємодію з іншими IP каналами та пристроями так само, як і з пристроями IEEE 802.15.4 [30, 35].

Це рішення має велику кількість переваг. Будь-який сенсор в 6I0WPAN мережі має персональну IPv6 адресу. Це дозволяє більшості компаній виготовляти LR–WPAN пристрої, здатні спільно працювати в одній мережі. Також надає можливість взаємодії даним пристроям, роботи з мережевими комп'ютерами та існуючим обладнанням. Будь–який вузол сенсорної мережі може бути доступним із зовнішніх мереж за адресою IP. Це усуває необхідність наявності комплексних шлюзів для будь–якого локального протоколу IEEE 802.15.4, великої кількості адаптерів, які використовуються наявними додатками для зв'язку за допомогою цих шлюзів, робить простіше різноманітні та специфічні для шлюзів процедури автентифікації та безпеки. Комплект усталених сформованих на IP протоколі програмних інструментів, таких як traceroute, ping, SNMP може негайно використовуватися з метою об'єднання в мережу та сервісу LR–WPAN пристроїв. Крім цього, на основі IP легко реалізується NAT (підміна адрес), кешування, розподіл навантаження. Наявні сервіси на основі HTTP/XML/SOAP та моделі передачіданих на програмномурівні спрощують процес створення програм для LR-WPAN мереж, і уніфікують інтеграцію пристроїв у наявну корпоративну мережу.

Втім, застосування IP інфраструктури призводить також до складнощів. Заголовки та адреси, що використовуються в IPv6 великі і тому дані, які слід передати, можуть бути більшими за розмір пакету IEEE 802.15.4. Така проблема в 6I0WPAN вирішується шляхом розбивки пакета більш дрібні пакети. Застосувавши стиснення заголовків, можна істотно збільшити розмір корисних даних, що передаються. На рисунку 2.12 зображено 6loWPAN пакет, у якому стандартний 40-байтний IPv6 та 8-байтний UDP заголовки стиснуті до

7 байт, що менше простого ZigBee заголовка.

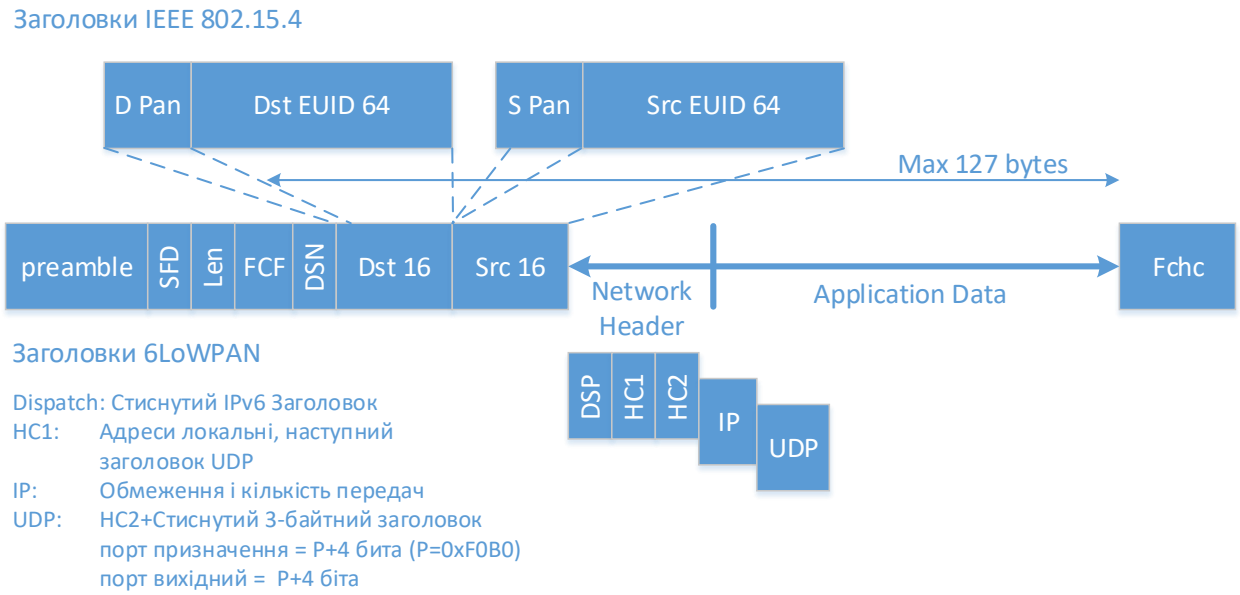

Рисунок 2.12 – Структура пакета зі стислим IPv6 заголовком

Якщо пристрій IEEE 802.15.4 здійснює зв'язок з рядом пристроєм IP адресу, здатний стискатися до одного байта, який вказує на те, що адреса призначення взятий з канальної адреси IEEE 802.15.4 пакета. А якщо зв'язок здійснюється з пристроєм поза сенсорною мережею, повна IP адреса буде включена в заголовок. Стандарт IPv6 має вимогу, щоб усіма каналами зв'язку підтримувалися пакети розміром до 1280 байт. Якщо розмір даних, що передаються, такий, що міститься в звичайному пакеті IEEE 802.15.4, вони можуть додаватися без зайвої інформації, в іншому випадку додається заголовок фрагментації, щоб спостерігати, як повідомлення розбивається на частини. Якщо пристрій самостійно не може здійснити доставку повідомлення до адресата, то додається заголовок меш (mesh) маршрутизації. Використовуючи mesh маршрутизацію, адреси призначення та джерела можуть записуватися як короткі 16-бітові або повні 64-бітові адреси. Також у mesh заголовок включений лічильник передач (Hops Left), який дозволяє обмежити тривалість життя пакета максимально чотирнадцятьма передачами.

Здійснюється вибір mesh протоколу при кожній передачі на пристрої. Рисунок 2.13 показує 6LoWPAN пакет, який використовує mesh стиснення заголовків і маршрутизацію [31].

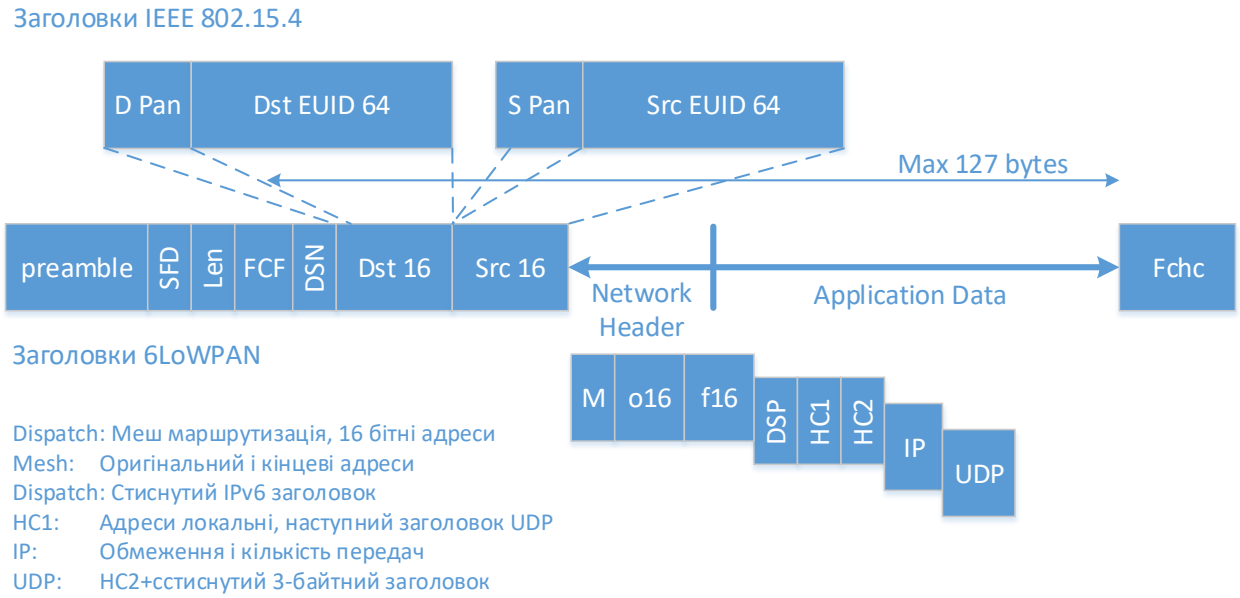

Рисунок 2.13 – 6LoWPAN пакет з підтримкою міш маршрутизації

За результатами практики встановлено, що схеми стиснення заголовків LOWPAN_HC2 і LOWPAN_HC1 не ефективні для основної частини практичних використань IPv6 в LR-WPAN. Максимальний ефект від застосування LOWPANHC1 можна досягти використовуючи локальні одноадресні комунікації, властивих для протоколів маршрутизації, виявлення або DHCPv6 і не часто використовуються в процесі передачі прикладних даних.

Використовувати адресу, що маршрутизується, необхідно при передачі даних на пристрій, який розташований за межами мережі 6LoWPAN, або у разі застосування схеми маршрутизації «route-over». Маршрутизована адреса LOWPAN HC1 потрібна передача префікса IPv6 для обох адрес: призначення та джерела. Якщо використовується мультикаст мовлення, то потрібна передача повної 128-бітної адреси.

У 2008 році розпочалася робота над проектом специфікації Compresion Format for IPv6 Datagrams in Low Power and Lossy Networks (draft-ietf-61owpan-hc), яка визначила новий формат кодування заголовків LOWPAN_IPHC, з метою ефективного стиснення глобальних, локальних, унікальних та мультикаст IPv6, Взявши за основу поширення стану за допомогою контексту. Крім цього, у цій специфікації було запропоновано деякі поліпшення формату стиснення заголовків, що регламентується в RFC4944.

Важливою відмінністю цієї специфікації вважалося існування механізму LOWPAN_NHC, формату застосовуваного з метою стиснення заголовка наступного за IPv6 заголовком. Схема стиснення LOWPAN_HC1 надавала можливість організації стиснення наступних заголовків, застосовуючи LOWPAN HC2, але виключно протоколів ICMPv6, TCP і UDP. Втім, біти заголовків HC2 розташовуються між стиснутими полями заголовків IPv6 та октетами стислих заголовків HC1. В останній специфікації дані наступного заголовка поміщаються після всіх бітів, що належать до IPv6, що надає можливість організувати правильну структуру шарів і гарантувати безпосередню підтримку заголовків розширень IPv6.

Прямо у специфікації описуються формати для стиснення UDP заголовків, а також інкапсуляціїIPv6 Extension Headers таIPv6–в–IPv6. Однак список може бути розширений для набору протоколів.

Формат LOWPANIPHC може бути представлений у такому вигляді (рис. 2.14) та (табл. 2.1).

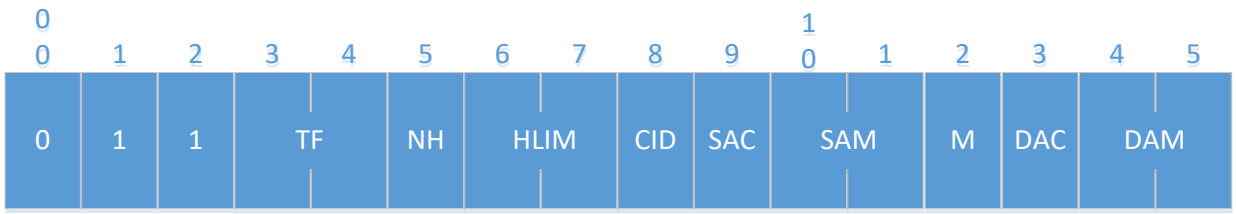

Рисунок 2.14 – Формат LOWPAN IPHC

Таблиця 2.1 – Формат кодування заголовків LOWPAN_IPHC

TF	2 біти	Клас навантаження та мітка потоку
NH	1 біт	Прапор наступного заголовка
HLIM	2 біти	Прапор обмеження кількості передач
CID	1 біт	Ідентифікатор контексту
SAC	1 біт	Стиснення адреси джерела
SAM	2 біти	Режим стиснення адреси джерела
M	1 біт	Стиснення мультикаст адреси
DAC	1 біт	Стиснення адреси призначення
DAM	2 біти	Режим стиснення адреси призначення

Протокол 6LoWPAN містить у собі два види маршрутизації: передачу пакетів із застосуванням IP адресації – "route-over" і механізм міш маршрутизації канального рівня, що має назву "mesh-under". Відмінності між цими механізмами аналогічні відмінностям між IP маршрутизації поверх Ethernet і мостовими мережами. У разі «mesh–under» маршрутизації всі вузли розміщені на одному каналі, який обслуговується одним або більшою кількістю роутерів, які називаються прикордонними маршрутизаторами 6LoWPAN (6LoWPAN Border Router – 6LBR). Одночасно в мережах route-over можуть існувати кілька каналів. Учасники даних каналів, на противагу фіксованим IP каналам, можуть здійснювати обмін відповідно до властивостей бездротової мережі, таких як умови довкілля та низьке енергоспоживання. Дані мережі містять гнучкий набір зв'язків між внутрішніми роутерами, які називаються 6LoWPAN маршрутизаторами (6LoWPAN Routers – 6LR) [32].

У мережах "route–over" існує два види маршрутизаторів: 6LR та 6LBR. Прикордонні маршрутизатори знаходяться на межі мереж 6LoWPAN та інших мереж, тоді як маршрутизатори 6LoWPAN розміщуються всередині мережі та реалізовують протокол маршрутизації.

Як IPv6 маршрутизаторів у конфігурації «mesh-under» виступають 6LBR, тоді як всі хости LR-WPAN розташовані на одному каналі, на відстані одного IP переходу. Така топологія немає 6LoWPAN маршрутизаторів, оскільки пересилання забезпечується з допомогою протоколу маршрутизації

канального рівня.

У цих конфігураціях хости не беруть участь у маршрутизації та передачі пакетів, оскільки вони працюють як прості IPv6 вузли.

Головні способи, такі як визначення дублікатів адрес, вибір адреси, пошук шляху, які дозволяють працювати IPv6 мережі, регламентовані RFC4861 – IPv6 Neighbor Discovery. Після подачі живлення та ініціалізації провідної IPv6 мережі, вузол приєднується до мультикаст адресою режиму запиту і далі виконується процедура визначення дублюючої адреси (Duplicate Adress Detection – DAD) для призначеної локальної канальної адреси (link-local adress) за допомогою передачі багатоадресного (муптикаст) повідомлення в канал. Далі здійснюється надсилання багатоадресного повідомлення на загальну адресу маршрутизаторів для запиту оголошень маршрутизатора. Коли хост отримує пакет Router Advertisement (RA) з прапором "A", він автоматично налаштовує адресу IPv6 з урахуванням префікса, отриманого в повідомленні RA. Крім цього, маршрутизатори здійснюють періодичну передачу в мережу оголошень на адресу муптикастаст, який включає всі вузли мережі.

Вузлами 6LoWPANконфігуруються свої IPv6 адреси за допомогою механізмів, що розглядаються у специфікаціях RFC4862 та RFC4861, обґрунтовуючись на інформації, що отримується у повідомленні Router Advertisement. Втім, застосування прапора M запропонованої оптимізації є обмеженим порівняно з рекомендацією RFC4861. Якщо прапор M встановлений, вузлу необхідно застосувати DHCPv6, щоб отримати будь-яку, не засновану на EUI-64 адресу. Якщо прапор M не встановлений, мережа зобов'язана підтримувати механізми виявлення дублюючих адрес, щоб хост міг безпечно застосовувати механізм реєстрації адрес для перевірки унікальність адреси, який заснований на EUI-64.

Маршрутизатори 6LR можуть використовувати ті самі механізми, щоб конфігурувати свої IPv6 адреси.

Маршрутизатори 6LBR відповідають за обслуговування префіксів, призначених мережі LR-WPAN, застосовуючи ручну конфігурацію, DHCPv6 Prefix Delegation (RFC3633) або інші механізми. У ізольованих мережах LR-WPAN префікс ULA (RFC4193) повинен генеруватися 6LBR.

Вузол здійснює передачу повідомлення Router Solicitation при включенні до мережі, а також при втраті зв'язку з одним з головних маршрутизаторів (після перевірки Neighbor Unreachability Detection у напрямку недоступного маршрутизатора).

Вузол отримує повідомлення RA, як правило, має опцію надійного маршрутизатора ABRO і додатково переносить одну або ряд опцій контексту (6LoWPAN Context Option – 6CO) на додаток до наявної префіксної інформації (Prefix Information Option – PIO) згідно з RFC4861.

Коли хостом конфігурується не канальний (link-local) IPv6 адресу, він здійснює його реєстрацію однією чи кількох зі своїх основних маршрутизаторів, застосовуючи опцію реєстрації адреси (Adress Registration Option – ARO) у повідомленні NS. Взлом вибирається час підтримки реєстрації (lifetime) та періодично повторюється повідомлення ARO (до закінчення часу підтримки) з метою обслуговування реєстрації. Час підтримки вибирається з огляду на період знаходження вузла в стані сну. З іншого боку, мобільні вузли, які найчастіше змінюють точку взаємодії з мережею, мають здійснювати вибір найкоротшого періоду підтримки реєстрації [33].

Процедура реєстрації може збиватися(опція ARO повернеться на вузол із не нульовим статусом), якщо маршрутизатором визначиться, що обрана IPv6 адреса вже застосовується іншим вузлом. Це можна використовувати з метою підтримки адресації, заснованої не на EUI–64, наприклад, тимчасової IPv6 адресації, яка описана в рекомендації RFC4941, або адресації, заснованої на ідентифікаторі інтерфейсу – короткому 16-бітному адресі 802.15.4. Крім цього, помилка може відбуватися при переповненні кеша Neighbor Cache на маршрутизаторі.

Повторну реєстрацію можна поєднати з процедурою встановлення недоступності сусідів (Neighbor Unreachability Detection – NUD) щодо маршрутизатора, оскільки обидві процедури застосовують одноадресне повідомлення NS. Це стає можливим, коли вузол прокидається з метою відправити повідомлення і йому необхідно впевнитись, що маршрутизатор ще доступний, а також виконати оновлення своєї реєстрації.

На реєстрацію адреси відповідь може бути отримана не відразу, оскільки при конфігурації "route-over" маршрутизатор 6LR може ініціалізувати перевірку DAD на 6LBR. Взлом виконується повторне надсилання повідомлення ARO, щоб отримати підтвердження отримання.

Нові необов'язкові механізми взаємного зв'язку маршрутизатор – маршрутизатор застосовуються лише у конфігурації "route–over", де є тип пристроїв 6LR. Подібні розширення опціональні, оскільки функції, які вони надаються, можуть реалізуватися іншими протоколами, наприклад, DHCPv6, протоколами маршрутизації, протоколами канального рівня чи іншими механізмами. Мають на увазі, що всі 6LR налаштовані на однорідне здійснення таких функцій. Наприклад, передача префіксної та/або контекстної інформації здійснюється засобами цього протоколу, а DAD – за допомогою іншого протоколу.

6LR здатні поводитися як прості вузли при конфігурації та ініціалізації префіксів, виконуючи передачу повідомлень RS, та на відміну від поведінки маршрутизаторів у рекомендації RFC4861 здійснювати автоматичне налаштування своїх адрес.

У разі застосування багатоадресного префікса або поширення контексту, маршрутизаторами 6LR зберігаються отримані (безпосередньо чи ні) 6CO, ABRO і префіксна інформація, і виконується повторне її поширення в повідомленнях RA для інших маршрутизаторів або вузлів у відповідь на запит RS. ABRO передбачає прапор версії, яка обмежує неконтрольоване поширення даних між 6LR.

Маршрутизатори 6LR можуть додатково здійснювати визначення дублюючих адрес на одному або кількох 6LBR, застосовуючи повідомлення запиту дублюючої адреси (DAR) та відповіді (DAC), який містить інформацію з повідомлення Adress Registration. Повідомлення DAC та DAR зможуть передаватися між маршрутизаторами. В даному випадку правило на граничне число переходів, що дорівнює 255, на дані повідомлення не поширюється.

Алгоритм взаємодії вузлів показаний рисунку 2.15.

При об'єднанні різних пристроїв та мереж слід вирішити проблему безпечної передачі даних. Дані, що передаються радіо каналом, можуть підслухуватися. Безпека фізично вважається важливою основою захисту інформації. IEEE 802.15.4 регламентується дуже потужна система шифрування AES–128 та всіма мікроконтролерами інтегруються можливості шифрування в апаратне забезпечення. Пристрій має ключ захисту, який отримує при введенні пристрою в експлуатацію, за допомогою якого дешифруються пакети, що приймаються, і шифруються всі передані. Також за допомогою таких ключів пристрою проходять процедуру ідентифікації.

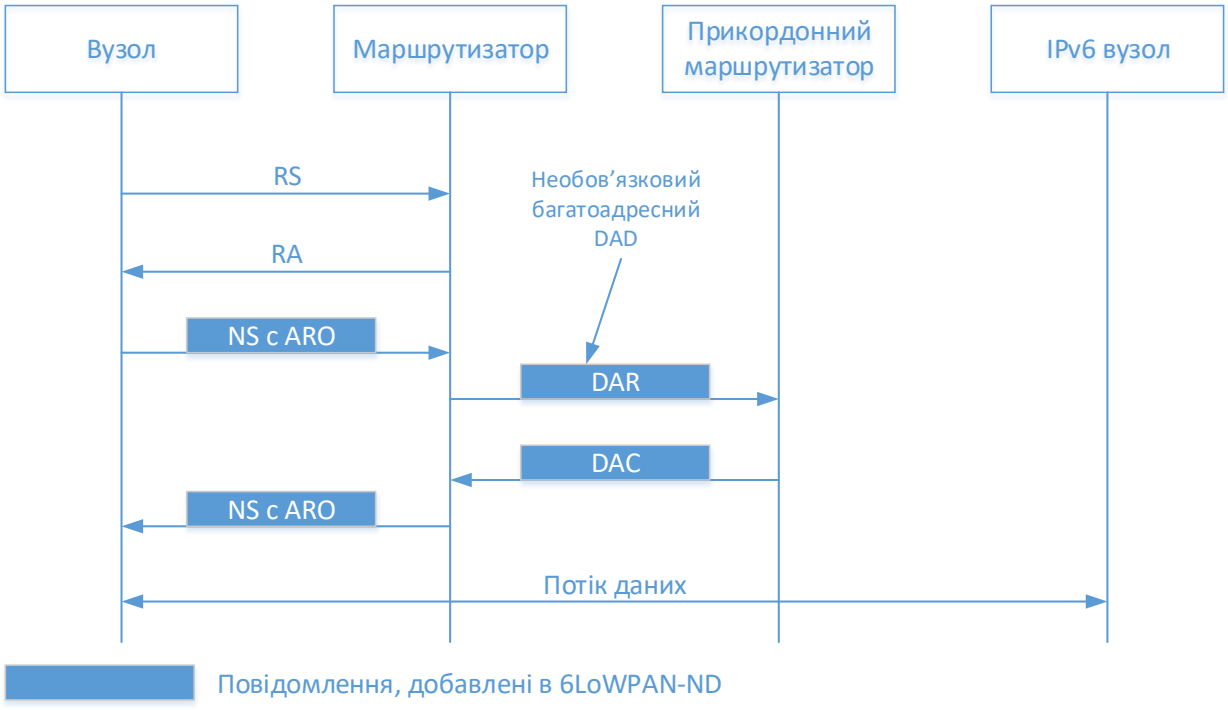

Рисунок 2.15 – Алгоритм взаємодії вузлів

Нерідко сенсорні мережі підключають до інших мереж у тому, щоб виконати передачу даних подальшої обробки. Для протоколів, що не маршрутизуються, таких як RS-485, SCADA, HART і ZigBee, підключення може виконуватися за допомогою шлюзів; як правило, це комп'ютери з IP підключенням та інтерфейсом у сенсорну мережу. Вразливим місцем у забезпеченні безпеки, як правило, вважається шлюз. Коли шлюз зламаний, то опиняється під загрозою вся LoWPAN мережа. Подібні шлюзи переважно управляються простою операційною системою з поширеними помилками безпеки, які можуть застосовуватися для злому. Щоб зменшити ймовірність злому, шлюзи встановлюють за фаєрволом, який обмежує доступ [34].

Коли побудова сенсорної мережі виконується на основі IP протоколу, то як шлюз можна використовувати простий маршрутизатор між сенсорною мережею і звичайною. Маршрутизатором є спеціалізований пристрій, на якому відсутня необхідність встановлення стандартної операційної системи та додаткових додатків. Його можна налаштовувати та обслуговувати так само, як і інші мережеві маршрутизатори. Їм додатково надаються послуги обмеження доступу та фільтрації пакетів. Маршрутизатор має в своєму розпорядженні можливість надання найпростіших сервісів трансляції адрес, які конфігурують правила для фаєрволу, що нерідко застосовуються в комерційних та домашніх мережах, а також селективно забезпечувати доступ допристроїв IEEE 802.15.4 із корпоративної мережі, аналогічно DMZ хостам у звичайній мережі.

Застосування протоколів 6LoWPAN надає можливість шифрувати канали точка–точка.

На сьогоднішній день найвідомішим протоколом маршрутизації вважається ZigBee, однак у нього є деякі недоліки в порівнянні з 6LoWPAN. У ZigBee дається опис лише взаємодії з іншими вузлами IEEE 802.15.4. Щоб передати дані сенсорів для подальшої обробки, слід встановити шлюзи, які не

зможуть надати доступ до конкретного сенсорного вузла. Щоб написати програмне забезпечення, потрібна реалізація верхніх рівнів стека замість застосування наявних стандартів. Специфікація поки що на стадії розробки, поточний стандарт ZigBee Pro не сумісний з ZigBee 1.0. Немає у наявності транспортного рівня. Нещодавно альянс ZigBee оголосив про роботу над здійсненням підтримки IP у ZigBee стеку.

Стек протоколів SP100.11f на даний момент знаходиться на початковому етапі розвитку, але йому необхідно описати та визначити дуже багато з того, що вже здійснено в протоколі IP. Після реалізації стандарту заявлена підтримка різних типів каналів, таких як IEEE 802.16, IEEE 802.11, IEEE 802.15.4. Його характерною особливістю вважається застосування технології TDMA.

Стандартом 6LoWPAN регламентується застосування мережевих рівнів IP для передачі каналами IEEE 802.15.4. Стандарт дозволяє встановити передачу між пристроями IEEE 802.15.4 і зв'язати пристрій IEEE 802.15.4 з іншим IP–обладнанням. Впровадження IPv6 можна застосовувати широкий спектр протоколів верхнього рівня, прикладного програмного забезпечення та інструментів [27]. Метою його розробки є можливість застосування нового класу пристроїв у загальноприйнятих додатках.

Енергетичну ефективність протоколу 6LoWPAN можна порівняти з корпоративними аналогами. Інші протоколи передають аналогічну адресну інформацію. 6LoWPAN оптимізується з метою обміну даними у підмережі IEEE 802.15.4. Значна витрата енергії потрібна тільки при передачі даних в інші сегменти IPv6 мережі через збільшення розміру заголовків, але в подібній ситуації іншим протоколам потрібно передати цю інформацію, тільки на рівні додатків, щоб вказати шлюзу вузол призначення даних.

2.2 Аналіз методів пропускної здатності бездротових сенсорних мереж

Аналіз методів пропускної здатності бездротових сенсорних мереж виявляє ряд ключових аспектів, які варто враховувати при розгляді та розробці таких мереж. Фізичні обмеження, такі як робочі частоти та втрати сигналу, впливають на загальну пропускну здатність.

Енергоефективність грає важливу роль у довгостроковому функціонуванні сенсорних вузлів, і важливо розробляти методи оптимізації для енергозбереження. Системи множинного доступу вимагають уваги до балансу між пропускною здатністю та затримкою, а також врахуванням обмеженого спектра. Аналіз обробки та аналізу даних вказує на необхідність оптимального стиснення та передачі інформації, а також ефективного агрегування та фільтрації.

В таблиці 2.2 наведено приклад структуризованого опису методів аналізу пропускної здатності бездротових сенсорних мереж.

Цей комплексний підхід до аналізу дозволяє розуміти взаємозв'язок різних аспектів пропускної здатності BSN та визначити стратегії для покращення ефективності та надійності бездротових сенсорних мереж.

Таблиця 2.2 – Методи аналізу пропускної здатності БСМ

Аспект	Метод Аналізу	Параметри та критерії оцінки
Фізичні обмеження	Спектральний аналіз	– Робочі частоти
		– Втрати сигналу та ефекти перешкод
Протоколи та алгоритми комунікації	Вивчення протоколів передачі даних	– Ефективність передачі та отримання даних
		– Методи роутингу та оптимізації маршрутів
		– Обробка колізій та управління ресурсами
Енергоефективність	Вимірювання витрат енергії на передачу та приймання	– Вплив на тривалість роботи сенсорних вузлів
		– Розробка методів оптимізації для енергозбереження

Продовження табл. 2.2

Аспект	Метод Аналізу	Параметри та критерії оцінки
Методи доступу до каналу	Аналіз різних методів (TDMA, CDMA, CSMA/CA)	– Ефективність методів доступу та керування колізіями
		– Забезпечення балансу між пропускною здатністю та затримкою
Системи множинного доступу	Порівняння технологій (LTE–M, NB–IoT, LoRa, Zigbee)	– Пропускна здатність та дальність передачі
		– Ефективність в умовах обмеженого спектра
Обробка та аналіз даних	Оцінка методів стиснення та передачі даних	– Рівень стиснення та втрата якості даних
		– Алгоритми агрегації та фільтрації даних
Безпека	Аналіз методів шифрування та захисту від атак	– Рівень захисту від несанкціонованого доступу
		– Ідентифікація та автентифікація сенсорних вузлів
Розширені технології	Вивчення впливу розширених технологій (5G)	– Підвищення пропускної здатності та надійності мережі
		– Використання нових можливостей для сенсорних мереж

Для подальшої роботи в рамках роботи було обрано вивчення навантаження для додатків збору даних телеметрії з нерухомих та змішаних (рухливих та нерухомих) об'єктів як найпоширеніших на цій стадії введення WSN.

Додатки збору даних вважаються основними елементами основних застосувань бездротових сенсорних систем, таких як контроль промислових споруд, автоматизація виробничих процесів та будівель, «розумні» будинки та ін. Щоб створити складні системи управління, слід мати уявлення про навантаження, яке циркулює в системі збору даних.

Вивчення в обраному напрямку вимагають, перш за все, проектування

моделей бездротової сенсорної мережі для описаних вище сценаріїв. Взявши за основу результати аналізу, фізичним середовищем для моделей, що проектуються, обраний протокол IEEE 802.15.4, а мережевим протоколом – ZigBee. Моделі повинні будуватися в такий спосіб, щоб результати досліджень можна застосовувати і використання протоколу 6LoWPAN.

Через практично необмежений перелік додатків у бездротових сенсорних мережах, а також стрімко змінних умов обслуговування навантаження в WSN, малоефективним є використання аналітичного моделювання для вивчення навантаження. Інструментарієм для вивчення навантаження в бездротових сенсорних мережах буде імітаційне моделювання [35].

Найбільш відомим і широко застосовуваним пакетом імітаційного моделювання для мереж зв'язку на сьогоднішній день вважається пакет NS-2 (Network Simulator 2), тому в роботі пропонується використовувати NS-2.

Основою для моделювання обрано сенсорне поле 30 на 30 метрів, на якому у випадковому порядку розміщено вузли сенсорної мережі. Вузол збору даних, шлюз, розміщений у центрі цього поля, під час впровадження на індустріальних об'єктах гарантує дальність поширення сигналу не більше 15-20 метрів. Відповідно, запропонована модель дає адекватний опис мережі навколо одного вузла збору даних. Насправді подібних вузлів може бути кілька. Працюють вони паралельно та обслуговують значні мережі датчиків.

На цій території у випадковому порядку розміщено 50 датчиків та у ненавмисний період часу вони передають повідомлення із встановленою частотою. Коли вибирається час початку передачі, то обирається і частота повторних передач: 60, 45, 30, 15 секунд. Подібні інтервали вибиралися на основі оприлюднених рекомендацій IETF та досліджень Міжнародного товариства автоматизації (International Society of Automation – ISA).

У результаті отримуємо карту розташування датчиків, її приклад зображено на рисунку 2.16.

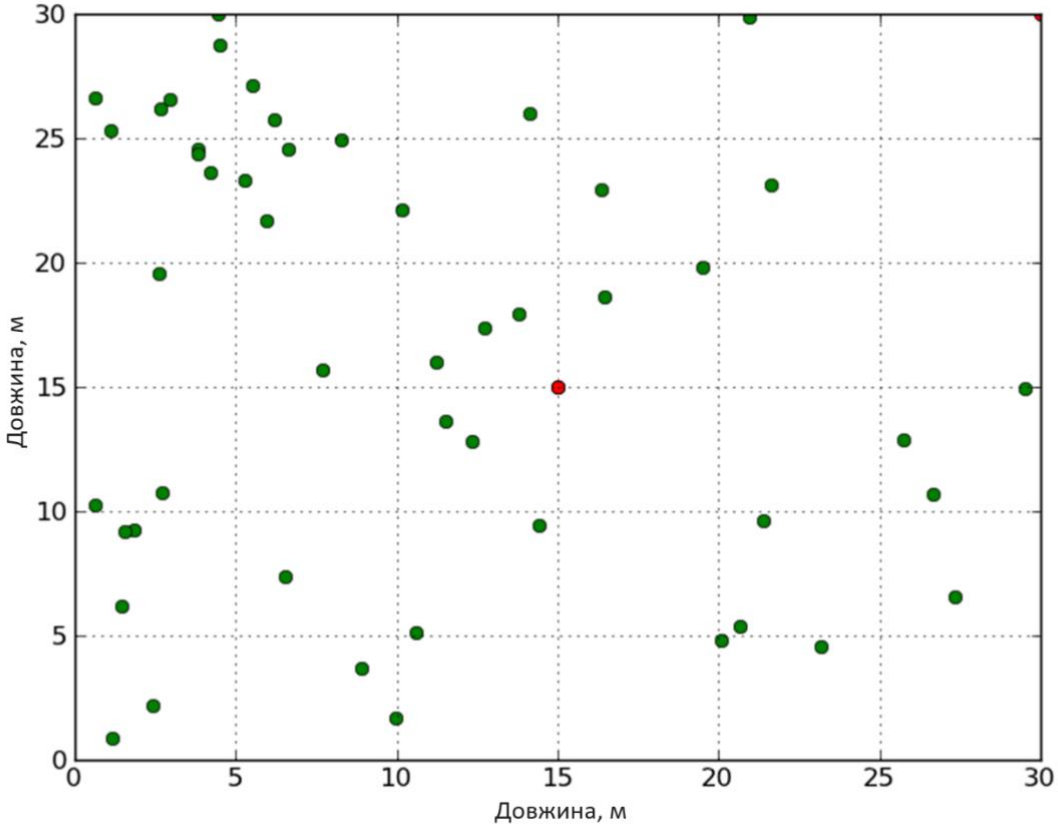

Рисунок 2.16 – Розміщення датчиків на плані

Дані, які необхідно передавати будь–якому вузлу надаються набором виміряних показників, яким дається опис або коротким рядком, або дробом або числом. Отже, при моделюванні подібного сценарію для передачі можна вибрати пакет найменшого розміру 4 байти.

У разі змішаних вузлів спочатку алгоритм функціонує аналогічним чином, проте для 50 % вузлів задаються випадкові координати, куди вони переміщуються з часом.

Щоб вибрати місце переміщення, застосовується генератор випадкових чисел. Для будь–якого з рухомих вузлів задаються дві координати для нового розташування. У ненавмисний момент часу, який для будь–якого вузла генерується персонально, вузлами починається прямолінійний рух із постійною швидкістю 2 метри на секунду. Така швидкість вважається

рекомендованою середньою швидкістю пересування рухомих об'єктів бездротових сенсорних мереж.

У процесі руху мобільними вузлами продовжується передача повідомлення з даними. Крім цього, вони ретранслюють повідомлення від інших джерел, що тягне за собою перебудову сенсорної мережі та появу особливостей, опис яких буде дано в наступному розділі [36].

Запропоноване дослідження охоплює аналіз пропускної здатності бездротових сенсорних мереж з урахуванням вивчення навантаження для додатків збору даних телеметрії. Вибір моделювання на основі пакету NS-2 вказує на прагматичний підхід до дослідження через його широку застосовуваність та добре встановлену репутацію в області імітаційного моделювання мереж зв'язку.

Зазначена область застосування BSN – додатки збору даних телеметрії для нерухомих та змішаних об'єктів – визначається як одна з ключових у бездротових сенсорних системах, що відображає їхню широку практичну важливість у різних областях, таких як промисловість та будівництво.

Використання протоколу IEEE 802.15.4 та мережевого протоколу ZigBee, а також можливість застосування протоколу 6LoWPAN, свідчать про спробу вибору стандартів, що відомі своєю ефективністю та здатністю пристосування до обмежень сенсорних мереж.

Моделювання на основі сенсорного поля 30 на 30 метрів і випадкового розташування датчиків реалістично відображає умови бездротових сенсорних мереж, особливо на промислових об'єктах. Рухомі вузли, які використовуються для змішаних об'єктів, додають до моделі аспекти мобільності, що може відображати реальні умови застосування.

Загальною метою є вивчення та розуміння навантаження для подальшого покращення ефективності та надійності бездротових сенсорних мереж, а використання імітаційного моделювання через NS-2 дозволяє більш глибоке вивчення умов та динаміки мережі в різних сценаріях.

На основі наданого контексту і завдань дослідження, слід врахувати кілька методів аналізу пропускної здатності, які можуть бути особливо важливими:

а) імітаційне моделювання (NS-2):

1) переваги: NS-2 – широко використовуваний пакет для імітаційного моделювання мереж, і він може забезпечити реалістичні умови для вивчення пропускної здатності у складних сценаріях, враховуючи мобільні та нерухомі вузли;

2) обмеження: хоча імітаційне моделювання дозволяє проводити дослідження в контрольованих умовах, важливо пам'ятати, що результати можуть мати обмежену адаптабельність до реальних умов роботи;

б) аналіз фізичного середовища:

1) переваги: розгляд фізичних характеристик середовища, таких як розташування сенсорів, їхні фізичні обмеження та дальність поширення сигналу, може допомогти у визначенні реальних умов експлуатації;

2) обмеження: цей метод може бути важким для систем з великою кількістю вузлів або у разі складної топології мережі;

в) аналіз протоколів та стеку протоколів:

1) переваги: врахування особливостей протоколів (наприклад, IEEE 802.15.4, ZigBee, 6LoWPAN) дозволяє точніше визначити можливості та обмеження мережі;

2) обмеження: важливо також враховувати взаємодію різних рівнів стеку протоколів, а також їх вплив на пропускну здатність;

г) аналіз навантаження:

1) переваги: вивчення типів даних, що передаються, та інтервалів передачі може надати інформацію про реальні потреби мережі та допомогти визначити оптимальні стратегії передачі даних;

2) обмеження: потребує детального вивчення конкретних додатків та їх характеристик.

Комбінація цих методів дозволяє створити повніший образ пропускної здатності бездротових сенсорних мереж у конкретних умовах дослідження.

2.3 Розробка алгоритму моделювання пропускної здатності у бездротових сенсорних мережах

Пакет імітаційного моделювання NS-2 вважається плодом багаторічної роботи вчених та розробників, які координувалися університетом Берклі. Це дискретний симулятор подій, спрямований на моделювання роботи бездротових та дротових мереж. Пакет надає можливість моделювання TCP/UDP з'єднань, різних протоколів маршрутизації, мультикаст та юнікаст передачі даних. Він моделює процеси, в яких просування за шкалою часу залежить від часу подій, які управляється планувальником. Подія є об'єктом, що має унікальний ідентифікатор, запланований час виконання та покажчик на об'єкт, що обробляє таку подію. Планувальником зберігаються впорядковані структури даних подій для їх виконання один за одним. Він запускає оброблювач для будь–якої події.

Написаний NS-2 мовою програмування C++ та скриптовою мовою OTcl як інтерфейс. Пакет використовує дві мови програмування, оскільки у процесі роботи необхідно вирішувати два види завдань. З одного боку, для докладного моделювання протоколів потрібне використання мови, яка дозволяє ефективно оперувати заголовками пакетів, байтами та імплементувати алгоритми, що працюють зі значним набором даних. Для таких завдань має значення швидкість виконання, а час обробки (повторний запуск, перекомпіляція, пошук та виправлення помилки, запуск моделювання) вважається менш важливим. Втім, для більшості досліджень мереж потрібні різні параметри, конфігурації

або різноманітні сценарії. У такому випадку час обробки (повторний запуск та зміна моделі) стає важливим. Оскільки конфігурація запускається лише один раз на початку моделювання, час її здійснення не має значного впливу на загальну швидкість.

Пакетом NS-2 задовольняються обидві ці вимоги за допомогою двох мов програмування OTcl та C++. Мова C++ має швидку швидкість виконання, однак у зміні він повільніший. Цей факт дозволяє йому стати оптимальним для детальної реалізації протоколів. OTcl виконується значно повільніше, але може змінюватися легше (і інтерактивно), що дозволяє стати оптимальним для опису сценаріїв моделювання.

Моделювання бездротових мереж має деякі особливості. Здійснити з'єднання двох вузлів у бездротових мережах можна двома підходами. Першим вважатимуться централізовану (інфраструктурну) мережу, у якій будь–який мобільний вузол з'єднується з однією чи деякою кількістю базових станцій, у процесі передачі між двома вузлами додатково бере участь базова станція. Другим підходом є децентралізована мережа, яка базується на ad–hoc мережі між користувачами, які мають намір виконати передачу даних між собою. За такого підходу мобільним вузлам необхідно бути як приймачем чи джерелом даних, а й виконувати передачу даних з інших вузлів.

В інфраструктурній мережі бездротова частина обмежується лише доступом до мережі, де застосовуються класичні протоколи маршрутизації. Мережа Ad-hoc базується на спеціальних протоколах маршрутизації, які адаптуються до нерідких змін мережевої топології. Щоб коректно моделювати інфраструктурні мережі, часто необхідні складні інструменти для симуляції фізичного радіо каналу, і моделювання механізмів управління живленням. Розширений модуль фізичного рівня NS-2 не має. В рамках роботи, що надається, були реалізовані деякі прості моделі радіоканалу. Основна увага у децентралізованих мережах приділяється протоколам маршрутизації. NS-2 застосовується для моделювання основних протоколів маршрутизації ad–hoc

мереж, і навіть транспорту та додатків, що їх використовують. Крім цього, він дає можливість налаштування параметрів MAC рівня, мобільності та основних параметрів фізичного рівня.

Пакетом NS-2 реалізуються основні протоколи маршрутизації: AODV (Ad hoc On-Demand Distance Vector Routing), TORE/IMPE (Temporally Ordered Routing Algorithm/Internet MANET Encapsulation Protocol), DSR (Dynamic Source Routing),DSDV (Destination-Sequenced Distance Vector).

Для моделювання поставлених завдань було розроблено наступний алгоритм (рис. 2.17).

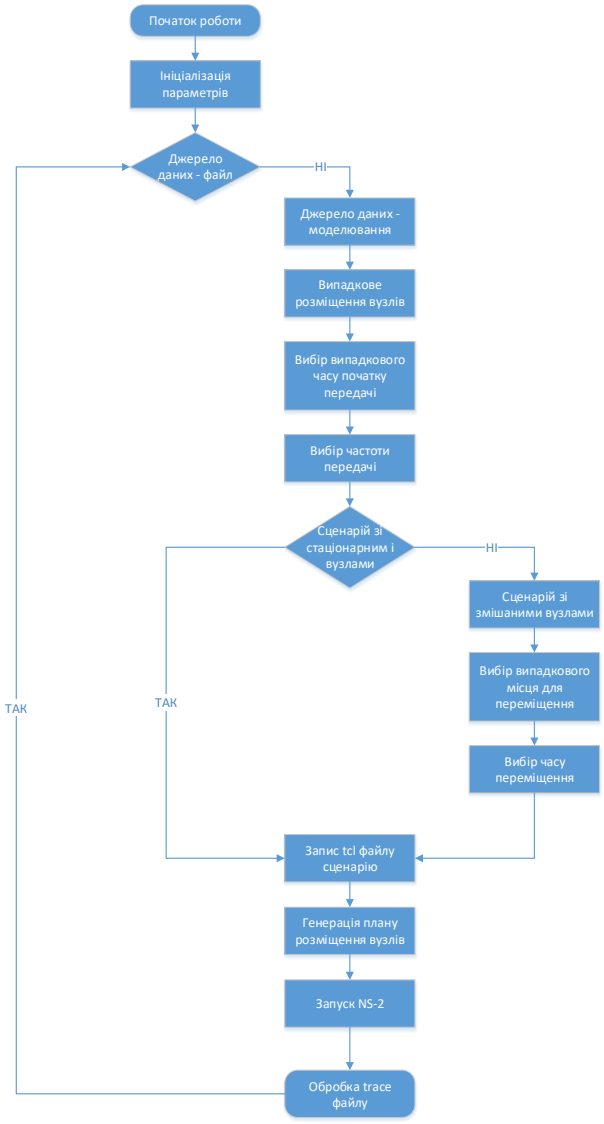

Рисунок 2.17 – Алгоритм моделювання

Як видно з рисунку, після ініціалізації параметрів вибираємо джерело даних, тобто, файл, в якому містяться дані дослідження. В нашому випадку – це відкриті числові дані по дослідженням пропускної здатності бездротових сенсорних мережах. Після цього проводиться моделювання цих даних, що і буде проведено в рамках наступного розділу. В рамках моделювання буде проведено випадкове розміщення вузлів, вибір початкового часу початку передачі, вибір частоти передачі, а вже після цього проводяться сценарії. Якщо не проходить сценарій зі стаціонарними вузлами, проводиться сценарій зів змішаними вузлами, вибір випадкового місця для переміщення, вибір часу переміщення. Після реалізації сценарію записується його файл, генерується план розміщення вузлів, запускається система моделювання і проводиться обробка файлу. Результатом всього вищеперерахованого будуть графіки моделювання, представлені в наступному розділі.

2.4 Висновки до другого розділу

За результатами аналізу протоколу IEEE 802.15.4, який забезпечує підтримку канального та фізичного рівнів для бездротових сенсорних мереж, розкрито характерні риси його функціонування для реалізації у наступному розділі моделей сенсорних мереж.

За результатами аналізу протоколу ZigBee, який забезпечує підтримку прикладного та мережного рівнів для бездротових сенсорних мереж, розкрито характерні риси його функціонування для реалізації у наступному розділі моделей сенсорних мереж.

За результатами аналізу протоколу 6LoWPAN, який забезпечує підтримку прикладного та мережевого рівнів для бездротових сенсорних мереж, розкрито характерні риси його функціонування для реалізації у наступному розділі моделей сенсорних мереж. Було проведено порівняння недоліків та переваг протоколів 6LoWPAN та ZigBee у процесі застосування з

метою створення бездротових сенсорних мереж.

У результаті, створено моделі для докладання збору даних зі змішаних та нерухомих об'єктів у бездротових сенсорних мережах.

3 ОЦІНКА ПРОПУСКНОЇ ЗДАТНОСТІ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

3.1. Оцінка агрегації даних у БСМ та аналіз трафіку зміни дисперсії

Підсумок роботи NS-2 показаний як трейс файл, що має інформацію про всі пакети, які передані в мережі, що моделюється. У кожному записі міститься тимчасова мітка, вид пакета, приймач та джерело повідомлення та додаткові службові дані. Проаналізувавши кожен рядок даного файлу, надається можливість отримання всієї необхідної інформації.

Спочатку слід оцінити зміну числа пакетів, які з часом передано на шлюз. Тривалість моделювання ділиться на періоди довжиною у встановлену кількість секунд (цей параметр може змінюватися під час запуску процесу). Аналізуючи трейс файл, обираються пакети, що мають адресу шлюзу. При розгляді часу надходження пакета час відносять до одного з періодів надходження. Придбані дані зберігаються для подальшого застосування, а також можуть бути візуалізації для наочного подання. На рисунку 3.1 зображено приклад агрегації з інтервалом 1 секунду.

Об'єднуючи дані зрізним тимчасовим інтервалам, є можливість бачити навантаження як у різних масштабах, у тому, що загальна форма навантаження продовжує залишатися однаковою. Це вважається однією з якостей самоподібних процесів, зміна часового масштабу рівноцінна зміні просторового масштабу стану. Характерні реалізації сомоподібного процесу зорово подібні незалежно від масштабу часу, на якому їх розглядають [18].

Розглядаючи графік навантаження неважко помітити, що потік має дві фази, стаціонарний процес і перехідний процес, який триває не більше 200 секунд. Перехідний процес відповідає процедурі встановлення початкових маршрутів. Характерне поділ на дві фази можна переглянути на всіх даних, які отримані в результаті моделювання.

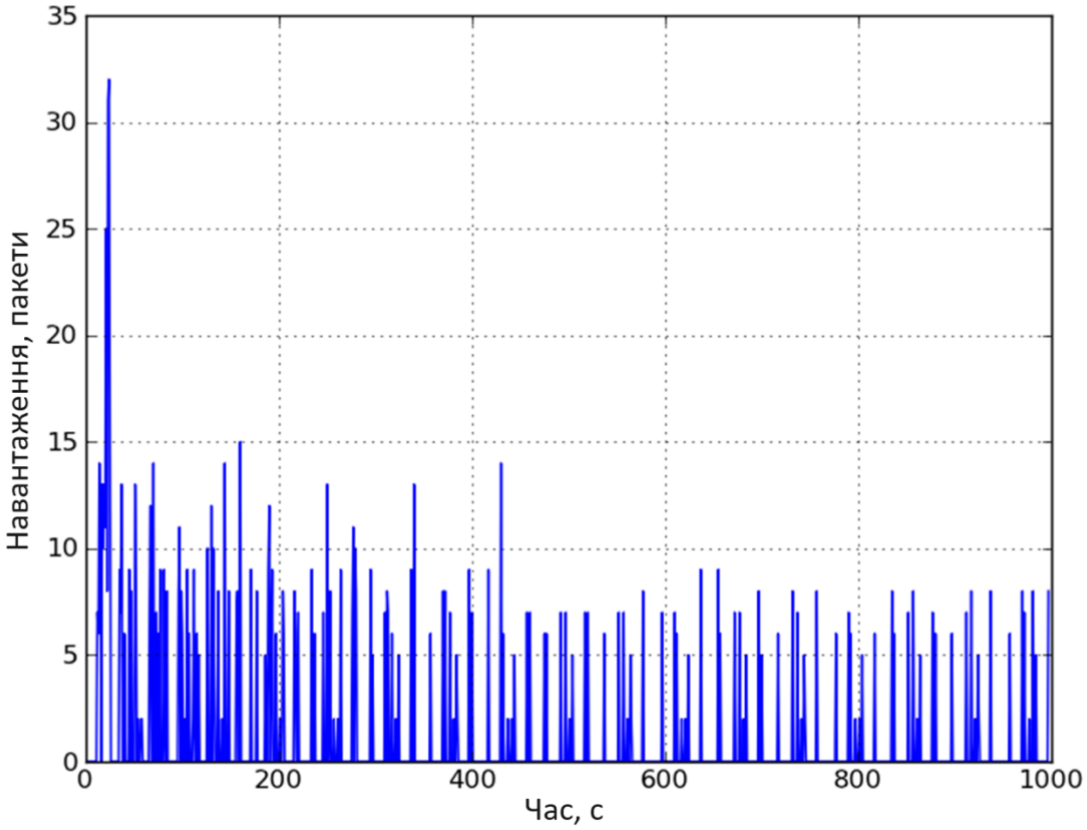

Рисунок 3.1 – Приклад агрегації даних

У разі додавання мобільності ряду вузлів перехідні процеси нижчого порядку з'являються протягом усього часу моделювання. Це зумовлено процедурами перебудови маршруту внаслідок зміни топології мережі.

На рисунку 3.2 зображено розглянутий метод аналізу.

Інформація про кількість пакетів, отримана раніше, застосовується визначення коефіцієнта Херста, який характеризує рівень самоподібності навантаження у мережі. Є ряд метод визначення коефіцієнта Херста. У даному проекті обрано найпопулярніший спосіб, метод аналізу графіка зміни дисперсії. Суть такого методу полягає у вивченні повільним темпом згасаючої дисперсії самоподібного агрегованого процесу. Для самоподібного процесу взаємний зв'язок між дисперсією об'єднаного процесу $X^{(m)}$ та розміром блоку m можна уявити в такий спосіб:

$$\sigma^2(X_t^{(m)}) \sim \alpha m^{-\beta} \text{ при } m \to \infty, \quad (3.1)$$

де α є кінцевою позитивною константою.

Беремо логарифми обох частин, отримуємо залежність:

$$log(\sigma^2(X_t^{(m)})) \sim -\beta \cdot log(m) + log(\alpha) \text{ при } m \to \infty. \quad (3.2)$$

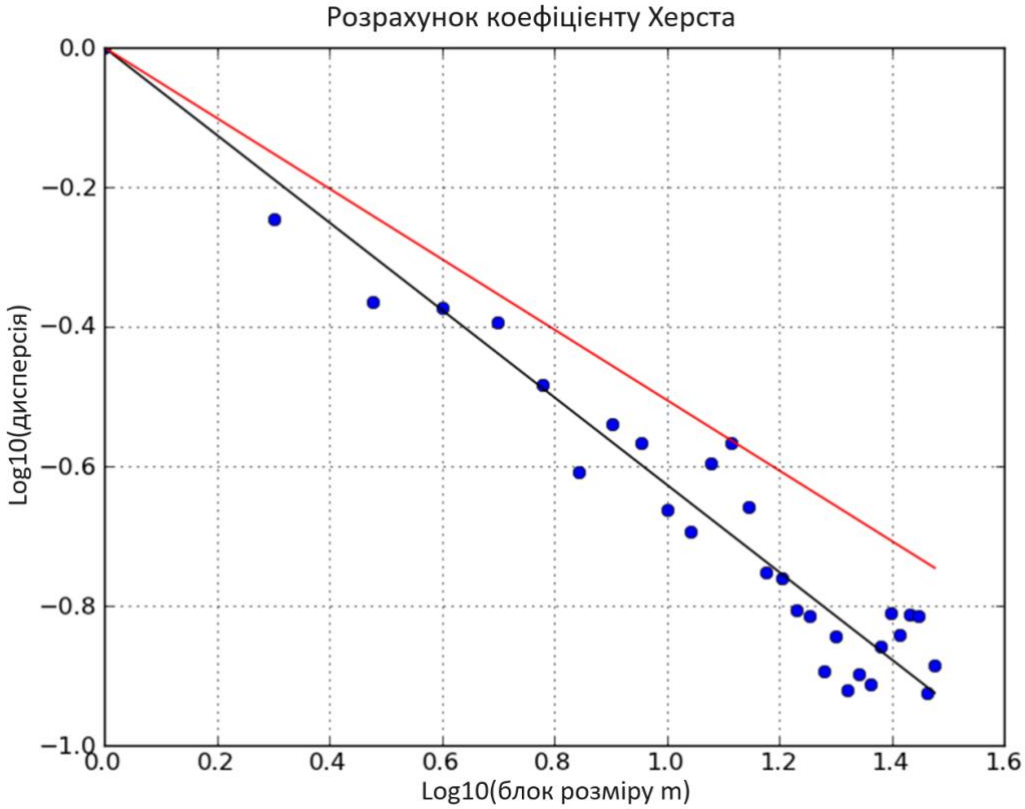

Рисунок 3.2 – Метод аналізу графіка зміни дисперсії

Визначивши $log(\sigma^2(X_t^{(m)}))$ для різних значень m та графічно відобразивши залежність від $log(m)$, отримуємо значення β. β можна визначити як негативний нахил прямої, яка підібрана методом найменших квадратів. З метою зв'язку коефіцієнта Херста H з отриманим β можна застосувати таку формулу:

$$H = 1 - \beta / 2. \qquad (3.3)$$

Результати моделювання в NS–2, представлені у трейс файлі, забезпечують інформацію про всі пакети, що передані в мережі. Аналіз цього файлу і використання графіків, таких як "Приклад агрегації даних" та "Метод аналізу графіка зміни дисперсії," має декілька важливих аспектів:

– оцінка зміни числа пакетів на шлюзі з часом. Аналізуючи трейс файл, можна визначити, як змінюється кількість пакетів, які надходять на шлюз з плином часу. Це дозволяє оцінити динаміку навантаження на мережу;

– агрегація даних для різних тимчасових інтервалів. Поділ тривалості моделювання на періоди дозволяє агрегувати дані для різних тимчасових інтервалів, що вказує на зміну навантаження в часі. Графіки агрегації, такі як "Приклад агрегації даних," допомагають візуалізувати цю зміну;

– розпізнавання фаз навантаження. За допомогою графіків, таких як "Метод аналізу графіка зміни дисперсії," можна визначити фази навантаження, такі як стаціонарний процес і перехідний процес. Це важливо для розуміння динаміки роботи мережі;

– визначення самоподібності навантаження. Характер графіків і аналіз самоподібності, такий як застосування коефіцієнта Херста, дозволяє визначити самоподібність процесів в мережі. Це може вказати на структурні особливості навантаження;

– розуміння впливу перехідних процесів. Виявлення перехідних процесів, таких як установлення початкових маршрутів, може допомогти зрозуміти вплив таких подій на пропускну здатність мережі.

Усі ці аспекти надають важливі дані для аналізу та оптимізації пропускної здатності мережі, дозволяючи вам приймати рішення щодо покращення ефективності та визначення оптимальних параметрів мережі.

3.2 Апроксимація автокореляційної функції та моделювання сценарію пропускної здатності в БСМ

Автокореляційна функція (АКФ) здатна охарактеризувати зв'язок між значеннями однакового випадкового процесу у рознесені періоди часу. Прийнято вважати, що процес має повільно спадаючу залежність (ПСЗ), якщо його характеризує АКФ, яка знижує гіперболічно при підвищенні тимчасової затримки. На відміну від ПСЗ є термін швидко спадання залежності (ШСЗ).

Визначивши коефіцієнт Херста, отримуємо графік апроксимації АКФ за допомогою формули:

$$r(k) = 1/2 \cdot ((k+1)^{2H} + 2k^{2H} - (k-1)^{2H}). \quad (3.4)$$

На рисунку 3.3 показаний приклад апроксимації АКФ для даних, отриманих у процесі моделювання додатків збору даних з нерухомих об'єктів. Під час побудови апроксимації АКФ для підсумків моделювання додатків збору зі змішаних (рухливих та нерухомих) об'єктів можна було помітити таку ж поведінку АКФ. Застосування коефіцієнта Херста до апроксимації АКФ дозволяє визначити тип залежності між значеннями, а саме, чи існують довготривалі залежності (повільне згасання) чи ні. Графічне уявлення апроксимації АКФ, представлене на рисунку 3.3, вказує на те, що вивчений потік має довготривалу залежність, оскільки гіперболічне згасання відбувається при підвищенні тимчасової затримки.

Це інформація важлива для аналізу пропускної здатності мережі, оскільки довготривалі залежності можуть вказувати на певні особливості в роботі мережі, які можуть впливати на її ефективність та можливості витримувати високі навантаження.

Графічне уявлення АКФ дає можливість візуально переконатися в тому,

що потік, що вивчається, має довготривалу залежність. Гіперболічне згасання автокореляційної функції на нескінченності вважається показником не підсумовуваності, ряд, що утворився значеннями кореляційної функції, розходиться. Гіперболічне повільне згасання вважається показником процесів із довготривалою залежністю, які відрізняються від процесів із сумованою АКФ, короткочасною залежністю, що зменшується за показовим законом.

Довготривала залежність вважається результатом чітко проявлених пульсацій процесу. Втім, можна відзначити деяку передбачуваність у невеликих межах часу.

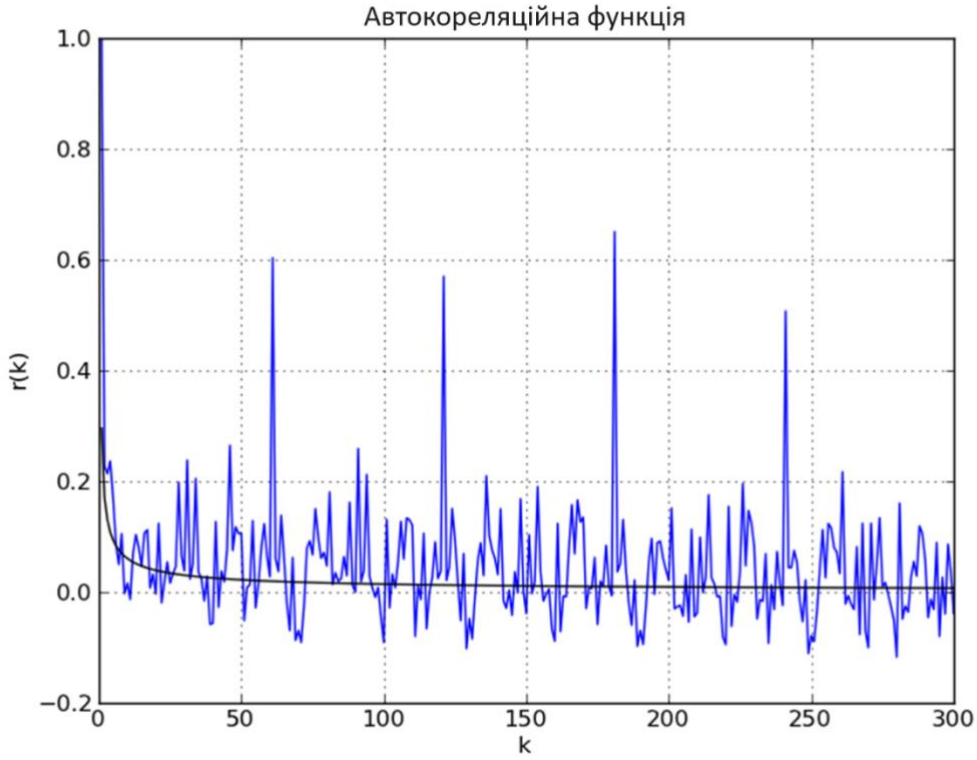

Рисунок 3.3 – Апроксимація АКФ

Ще одним важливим ознакою самоподібних процесів вважатимуться повільно спадаючу дисперсію. Коли здійснюється усереднення процесу, згасання дисперсії вибіркового середнього відбувається повільніше за величину, зворотну розміру вибірки. Така якість свідчить про можливість

значних викидів, які не згладжуються усередненням у випадковій процедурі, та поєднує самоподібність з таким визначенням, як розподіл з важкими хвостами.

Щоб оцінити параметр Херста, було виконано неодноразовий запуск моделюючого сценарію. Сценарій із нерухомими об'єктами виконувався 1000 разів, також 1000 разів був виконаний і сценарій зі змішаними (рухомими та нерухомими) об'єктами. Це забезпечило отримання чисельних оцінок середнього та дисперсії параметра Херста.

Значення параметра Херста більше 0,5 є необхідною підставою для того, щоб визнати процес самоподібним. Важливо помітити, що значення H, яке близьке до одиниці, означає, що процес вважається детермінованим, тобто не є випадковим: для деяких точно визначених процесів детермінованих структура на будь–якому масштабі суворо повторюється, що забезпечує одиничне значення параметра Херста.

Середнє значення параметра Херста для сценарію з нерухомими об'єктами становило 0,675. Цим доводиться, що навантаження від вузлів сенсорної мережі докладання збору даних із нерухомих об'єктів має властивості самоподібності із середнім ступенем самоподібності.

Середнє значення параметра Херста для сценарію зі змішаними (рухомими та нерухомими) об'єктами становило 0,687. Цим доводиться, що навантаження від вузлів сенсорної мережі додатку збору даних зі змішаних об'єктів також має властивості самоподібності із середнім ступенем самоподібності.

Проаналізувавши результати багаторазового запуску сценарію зі змішаними (рухомими та нерухомими) видами вузлів, побудовано графік залежності коефіцієнта Херста від загальної кількості подій у процесі запуску сценарію (рисунок 3.4).

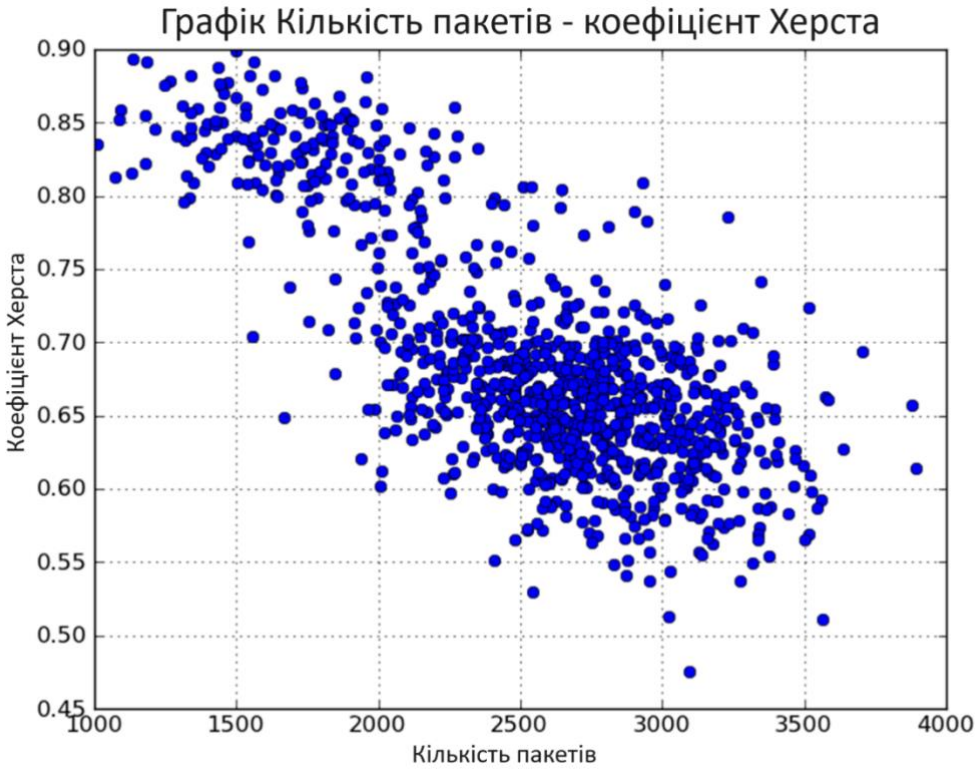

Рисунок 3.4 – Значення коефіцієнта Херста для змішаних вузлів

На даному графіку можна чітко виділити два кластери. Перший є навантаженням реконфігурації та сигналізації, а другим представлені всі види навантаження разом: телеметрія, сигналізація та реконфігурація.

Є можливість визначити середнє значення параметра Херста для навантаження сигналізації та реконфігурації, воно становило 0.829. Отже, навантаження сигналізації та реконфігурації для застосування збору даних зі змішаних (рухливих і нерухомих) об'єктів, має властивості самоподібності з високим ступенем самоподібності.

Значення параметра Херста в контексті самоподібних процесів та його використання для аналізу навантаження мережі дає наступне.

1. Повільно спадаюча дисперсія. Ця властивість є ще однією характеристикою самоподібних процесів. Вона означає, що при усередненні процесу згасання дисперсії відбувається повільніше, ніж при збільшенні розміру вибірки. Така якість свідчить про можливість значних викидів, які не

згладжуються усередненням, та вказує на розподіл з важкими хвостами.

2. Оцінка параметра Херста. Використовуючи неодноразовий запуск моделюючого сценарію, автори отримали чисельні оцінки середнього та дисперсії параметра Херста. Значення параметра Херста більше 0,5 вважається підставою для визнання процесу самоподібним. Значення Херста, близьке до одиниці, свідчить про детермінований процес, тобто не випадковий.

3. Результати. Середнє значення параметра Херста для сценарію з нерухомими об'єктами та сценарію зі змішаними об'єктами становило відповідно 0,675 та 0,687. Ці результати підтверджують наявність самоподібності в навантаженні мережі.

4. Графік коефіцієнта Херста. На графіку залежності коефіцієнта Херста від загальної кількості подій виділяються два кластери: один відповідає навантаженню реконфігурації та сигналізації, а інший – усім видам навантаження разом. Високе значення параметра Херста для навантаження сигналізації та реконфігурації (0,829) свідчить про його властивості самоподібності з високим ступенем.

5. Діагностування самоподібності. Використання вейвлет перетворення Пуассонівського та порівняння показників змодельованого потоку може слугувати одним із способів діагностування самоподібності навантаження.

Всі ці аспекти дозволяють зрозуміти і характеризувати самоподібність в навантаженні мережі, що, в свою чергу, може бути важливим для аналізу та оптимізації пропускної здатності мережі.

3.3 Проблематика синхронізації годинників та її вплив на пропускну здатність

Розглянемо проблеми синхронізації годинників у сенсорних мережах та їх вплив на пропускну здатність. Вдалий сеанс показує ефективну

синхронізацію, де приймаючий вузол починає прослуховування трохи раніше передавального вузла. Неефективний сеанс вказує на неадекватну синхронізацію, що призводить до зайвих витрат енергії приймаючого вузла. Невдалий сеанс показує порушення синхронізації, що призводить до невдалого обміну даними. Залежність пропускної здатності від тривалості прослуховування підкреслює, що краща синхронізація призводить до менших втрат пропускної здатності приймаючого вузла.

Проблеми синхронізації годинників у сенсорних мережах і їх вплив на витрати електроенергії можуть впливати на пропускну здатність мережі. Вдалий сеанс і ефективна синхронізація можуть сприяти покращенню пропускної здатності, оскільки вузли можуть ефективно обмінюватися даними. Наприклад, якщо приймаючий вузол точно знає, коли починається передача даних, він може вчасно активувати свій приймач, що зменшить час очікування та поліпшить ефективність обміну.

З іншого боку, незадовільна синхронізація та великі витрати енергії при прослуховуванні можуть призвести до неефективного використання електроенергії та зниження пропускної здатності. Наприклад, якщо велика кількість вузлів постійно слухає ефір, очікуючи дані, це може призвести до конфліктів та зниження загальної продуктивності мережі.

Таким чином, ефективна синхронізація годинників у сенсорних мережах може впливати на пропускну здатність шляхом поліпшення часу обміну даними та зменшення витрат енергії. Наслідком цього може бути оптимізація роботи мережі та підвищення її продуктивності.

Дамо опис випробуваному на практиці механізму оптимізації прослуховування ефіру раніше початку відправки пакета передавальний вузлом, який дозволяє знизити втрати пропускної здатності на роботу пристрою, при цьому не допустивши втрати в точності визначення часу, також запропонуємо шляхи коригування розбіжності годинників пристроїв та обліку температурних змін.

Розберемо сеанс зв'язку, зображений рисунку 3.5. Приймаючим вузлом починається прослуховування ефіру трохи раніше початку відправки пакета, що передає вузлом.

Рисунок 3.5 – Вдалий сеанс. Вузлом–приймачем починається прослуховування ефіру трохи раніше початку відправки пакета передавальний вузлом

На рисунку 3.6 показано неефективний сеанс зв'язку. Незадовільна синхронізація годинника призвела до того, що приймаючим вузлом більше часу витрачається на очікування пакета, ніж його отримання. Втім, сеанс зв'язку виконано успішно, приймаючою стороною отриманий переданий пакет.

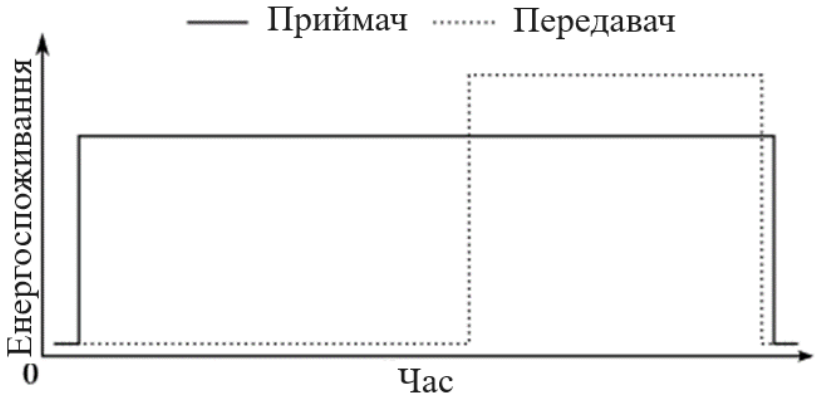

Рисунок 3.6 – Неефективний сеанс. Приймаючим вузлом на очікування пакета витрачається занадто багато часу

На рисунку 3.7 представлений невдалий сеанс: інтервал прослуховування приймаючим вузлом закінчено раніше, ніж передавальним вузлом почалася відправка пакет. Порушено синхронізацію вузлів, не виконано передачу пакета. Слід вжити заходів щодо її відновлення.

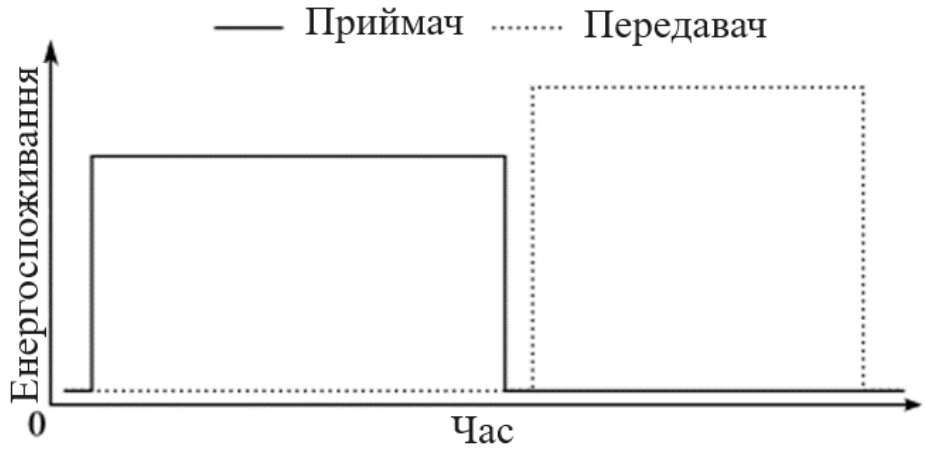

Рисунок 3.7 – Невдалий сеанс. Порушено синхронізацію вузлів

Приймач є основним джерелом витрати електроенергії в сенсорному вузлі. Якщо мінімізувати тривалість його роботи, можна досягти відчутних результатів в економії електроенергії.

Чим краще виконана синхронізація між собою часу приймаючого та передавального вузлів, тим менший ресурс протягом прослуховування буде допускатися приймаючим вузлом, і тим менше електроенергії він витратить на порожнє прослуховування радіоефіру. Незадовільна синхронізація спричинить непродуктивну витрату енергії приймаючим вузлом. На рис. 3.8 зображено залежність середнього енергоспоживання приймача від тривалості інтервалу прослуховування.

Рисунок 3.8 – Залежність середнього споживання енергії від тривалості інтервалу прослуховування

Залежність середнього споживання енергії від тривалості інтервалу прослуховування розраховано для швидкості 250 Кбіт/с. Інтервал сеансів зв'язку дорівнює 15 с. Енергоспоживання в режимі прийому склало 13,2 мА, в режимі сну – 0,02 мкА. Витрати енергії у разі скорочення тривалості інтервалу прослуховування зі 100 мс до 1 мс знижуються приблизно в 20 разів за довжини пакета 127 байт.

Рекомендований підхід ґрунтується на застосуванні апаратної платформи, що має два години:

– повільні (32768 Гц), які мають невисоку стабільність (36 ppm) та невелике електроспоживання (0,01 мА);

– швидкі (1 МГц), які мають високу стабільність (3,3 ppm), а й відносно високе електроспоживання (приблизно 1 мА [24]).

Повільний годинник функціонує завжди і забезпечує вихід із режиму сну сенсорного вузла. Вони тактуються від кварцового камерного резонатора типу. Він вважається характерним істотне зміна частоти залежно від температури (рис. 3.9).

Швидкий годинник не працює в режимі сну, що дає можливість мінімізувати енергоспоживання. У період активності пристрою швидкий годинник використовується для того, щоб визначити точний час включення приймача.

Щоб зменшити швидкість розбіжності годинника вузлів, будь–яким з вузлів автономно виконується калібрування повільного годинника по швидким годинникам і враховується температурна поправка при розрахунку часових інтервалів. Щоб усунути розбіжність, що залишилася при будь–якому сеансі зв'язку здійснюється синхронізація.

Важливо зауважити, що внаслідок роботи представлених алгоритмів насправді не виконується підведення годинників пристроїв, є лише коефіцієнти, які впливають на розрахунок часових інтервалів.

Рекомендований у проекті метод дає можливість забезпечити попарну синхронізацію пристроїв. Цим мається на увазі, що кожним із вузлів сенсорної мережі підтримується актуальна інформація про розбіжність його особистих годинників з годинником виключно тих вузлів, з якими такий вузол зв'язується. Є моделі синхронізації часу, в яких час у синхронізованому стані підтримується по всій мережі, але це призводить до ускладнення алгоритмів і спричиняє значну витрату енергії і не надає значних переваг у більшості випадків.

Зміна частоти роботи кварцових резонаторів залежить від температури, причому швидкий і повільний кварцові резонатори піддаються її впливу. На рисунках 3.9 та 3.10 представлені залежності величин зміни частот швидкого та повільного кварцових резонаторів щодо температури. Побудовано графіки на основі даних виробників.

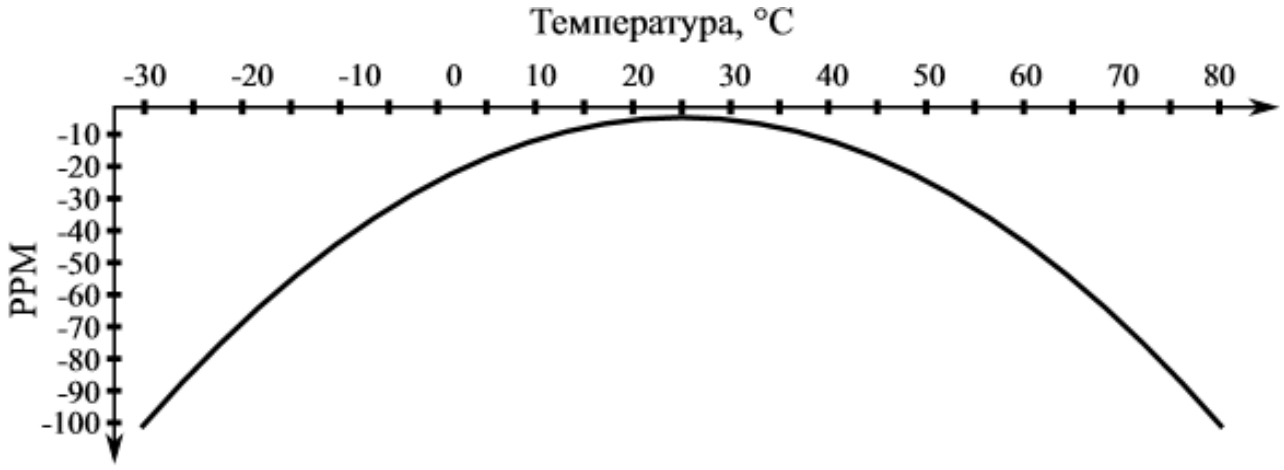

Рисунок 3.9 – Залежність частоти повільного кварцового резонатора від температури. Частота зменшується при відхиленні температури від номінальної (25 °C)

Так як швидкий годинник застосовується, щоб відміряти тільки відносно короткі часові інтервали, можна знехтувати впливом на них температурного режиму. Більшу частину часу вузлами використовуються повільні годинники.

Запропоновано наступний метод обліку температурних поправок, які виконуються регулярно (наприклад, 1 раз на кілька секунд) і включають такі дії:

1) опитується датчик температури;

2) на підставі його показань та даних на рисунку 3.9 розраховується відхилення поточної частоти кварцового резонатора від номінальної: $d = \frac{32768}{1000000} \times p$, де d – шукане відхилення (Гц), а p – Зміна частоти при поточній температурі (ppm);

3) розрахунок часу t_1, що пройшов з попереднього запуску процедури (тривалість інтервалу корекції);

4) розрахунок часу $t_2 = \frac{t_1 \times 32768}{32768 - d}$, Що пройшло з попереднього запуску процедури, враховуючи відхилення частоти;

5) розрахунок різниці між t_1 і t_2 : $t_d = t_2 - t_1$ та збереження набутої величини у змінну, яка накопичує поправку.

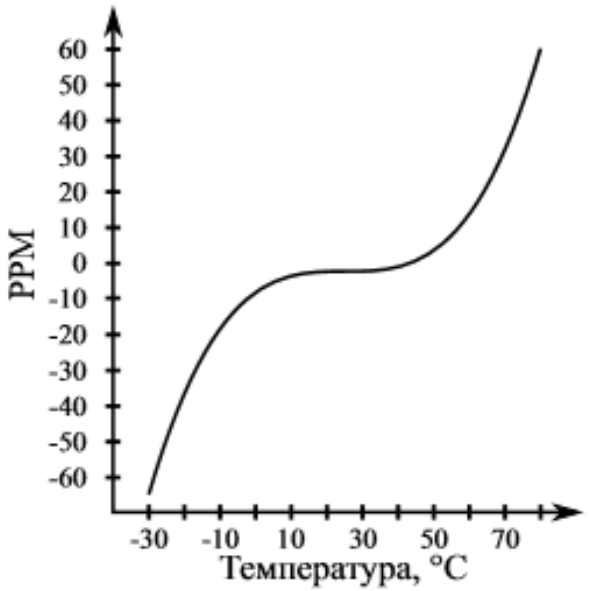

Рисунок 3.10 – Залежність частоти швидкого кварцового резонатора від температури

Таким чином, розглянута проблема енергоспоживання та синхронізації годинників у сенсорних мережах. Одним із аспектів є регулювання енергоспоживання за допомогою двох годинників: повільного, який використовується для виходу з режиму сну, та швидкого, який застосовується для точного визначення часу під час активності пристрою.

Крім того, важливою є синхронізація годинників між вузлами для забезпечення правильної координації. Коригування годинників виконується автономно через калібрування повільного годинника відносно швидкого, а також врахування температурних впливів.

Зміна частоти годинників відбувається відповідно до температурних змін, і врахування цього фактора дозволяє забезпечити точність вимірювань.

Запропонований метод синхронізації пристроїв дозволяє зберігати актуальні дані про розбіжність годинників між взаємодіючими вузлами,

сприяючи ефективній роботі сенсорної мережі при мінімізації витрат енергії.

Ефективна синхронізація годинників та оптимізація енергоспоживання можуть впливати на загальну продуктивність та функціональність сенсорної мережі, що, в свою чергу, може вплинути на пропускну здатність.

Наприклад, ефективне використання ресурсів та оптимізоване енергоспоживання може забезпечити більш довгий термін служби сенсорних вузлів та збільшити стійкість мережі. Це може мати позитивний вплив на завантаження мережі та її здатність ефективно обробляти та передавати дані.

Надалі перед застосуванням значень повільного годинника слід додати до нього накопичену величину поправки.

Зміна температури вважається поступовим процесом, однак у запропонованій процедурі це передбачається і температура протягом інтервалу коригування вважається рівною температурі в кінці інтервалу коригування. Якщо частота виклику процедури буде достатньою, то на результат, що отримується, цей факт сильного впливу не вплине.

Як альтернативу можна нагадати про температурно-компенсовані генератори, але вони витрачають більшу кількість електроенергії та відрізняються високою вартістю. Ще одним способом є побудова корекційних таблиць за підсумками калібрування будь–якого певного зразка кварцового резонатора в термокамері.

Процедура калібрування полягає в тому, щоб виміряти один і той же досить тривалий часовий проміжок і повільним, і швидким годинником, а потім обчислити коефіцієнт, який дозволить компенсувати невідповідність повільного годинника. Даний випадок вважається єдиним у робочому процесі пристрою, коли швидкий годинник застосовується, щоб відміряти тривалий часовий інтервал. Раціональним буде застосувати до них процеси обліку температурних поправок, описаних у попередньому розділі.

Процедурою передбачено такі дії:

1) перемикається простий перехід у режим сну. Це необхідно для того, щоб у процесі калібрування не зупинявся швидкий годинник;

2) виконується зняття показань повільного годинника, одночасно знімаються показання та швидких годинників;

3) виконується очікування протягом тривалого інтервалу (> 900 мс);

4) виконується зняття показань повільного годинника, одночасно знімаються показання та швидких годинників;

5) взявши за основу отримані показання годинника, визначається калібрувальний коефіцієнт: $C_c = 1 + \frac{\Delta_f - \Delta_s}{\Delta_s}$, де C_c – Шуканий калібрувальний коефіцієнт, Δ_f —час, який минув між пунктами 2 та 4 відповідно до швидких годин, Δ_s – час, який минув між пунктами 2 та 4 відповідно до повільного годинника.

Процес виконується замість одного з тривалих (> 900 мс) етапів сну пристрою. Отже, довготривале монополізування процесора залишається невиявленим і створює перешкод роботі інших процесів на пристрої. Придбаний калібрувальний коефіцієнт незмінно використовується при зверненні до показань повільного годинника.

Процес калібрування дає можливість знизити вплив відхилення робочої частоти певного екземпляра кварцового резонатора від номінальної. Калібрування здійснюється один раз при старті пристрою, але може періодично повторюватися, щоб компенсувати можливе накопичення помилки.

Проводилися експерименти, які показали, що відкалібрований повільний годинник двох вузлів розходяться зі швидкістю~4 ppm. Отже, швидкість розбіжності знижена майже мінімально допустимої (3,3 ppm) на поточної апаратної платформі.

Вище описані механізми дають можливість досягти найменшого розбіжності годинника на одному пристрої, але з часом годинники різних пристроїв відносно один одного будуть розходитися. Головною причиною цього є зміна температурного режиму пристроїв. Ще однією причиною вважається короткочасна нестабільність кварцових резонаторів (з часом змінюється робоча частота), яку не вдається подолати шляхом калібрування, оскільки і повільний, і швидкий кварцові резонатори, згідно з паспортними даними, мають однакову тимчасову нестабільність, що дорівнює ±3 ppm/год. Це підтверджує необхідність застосування способу корекції розбіжності годинника в процесі роботи пристроїв.

Початкову синхронізацію пристроїв можна досягти в процесі конфігурації, в момент підключення нового сенсорного вузла до наявної мережі. Далі необхідно підтримувати синхронізацію за допомогою описаного нижче алгоритму:

а) у період планування наступного сеансу зв'язку приймаючим вузлом оцінюється час, через який виконуватиметься сеанс. Чим більше залишилося часу до наступного сеансу, тим більше часу прослуховування буде більшим. Планується сеанс таким методом, щоб момент прийому пакета від передавального вузла знаходився точно в середині інтервалу;

б) настає час сеансу, що передає вузлом виконується одна з дій:

1) якщо є дані для відправки, то вузлом передається простий пакет з даними;

2) якщо відсутні дані, то для підтримки синхронізації передається пакет найменшої довжини (15 байт для мереж 802.15.4);

в) приймаючим вузлом, застосовуючи переривання RX_START, зберігається тимчасова мітка початку одержання пакета (рисунок 3.11). Пристрій обробляє пакет як завжди. Далі визначається різниця D між очікуваним і фактичним часом початку отримання пакета і виконується зсув часу чергового сеансу за допомогою формули $C_s^{'} = C_s + D$.

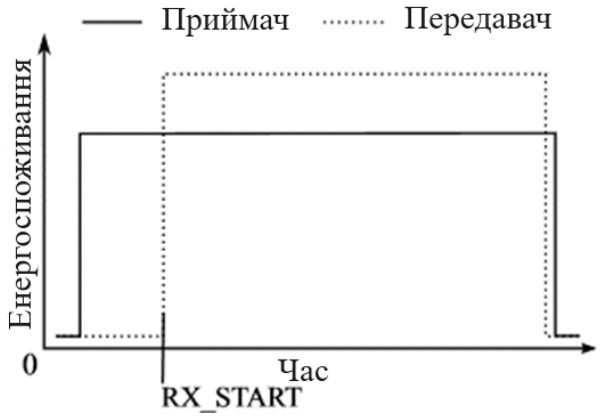

Рисунок 3.11 – Час початку отримання пакета зберігається обробником переривання RX_START

Крім цього, отримання $D \neq 0$ має на увазі, що з різною швидкістю йде годинник пристроїв. Можна оцінити швидкість розбіжності годинника і застосовувати її під час планування часу чергового сеансу. Швидку швидкість розбіжності можна визначити за допомогою формули $S = \frac{D}{T_{sync}}$, де T_{sync} – час, що минув з моменту попередньої синхронізації, знак S вказує напрямок розбіжності. Величину компенсації визначають таким чином: $C_d = T_{next} \times S$, де T_{next} – час до чергового сеансу зв'язку. Позначимо, що метод синхронізації, що представляється, вважається пасивним, що не передбачає наявності спеціально переданих даних з метою синхронізації.

Під час планування сеансу за своїм годинником вузлом враховується:

C_c – калібрувальна поправка;

C_t – температурне виправлення;

C_s – поправка на відому розбіжність;

C_d – компенсація різниці швидкостей годин;

C_u – запас на неперебоpну розбіжність годинника за час, що минув з моменту заключної синхронізації.

При отриманні показань повільного годинника слід враховувати калібрувальну та температурну поправки: $t = t' \times C_c + C_t$, де t' – початкові показання повільного годинника, t – свідчення повільного годинника, враховуючи поправки.

Припустимо, що черговий сеанс зв'язку за протоколом повинен виконатися через час T. Тоді сеанс, щогодини пристрою необхідно проводити через час $T' = T + C_s + C_d - \frac{C_u}{2}$, причому тривалість інтервалу прослуховування сеансу зв'язку необхідно також збільшити на $\frac{C_u}{2}$. Базову тривалість інтервалу прослуховування T_ω прийматимемо рівної подвоєної точності синхронізації.

Швидкість розбіжності, що визначає виправлення C_d, може порівняно швидко змінюватися в процесі роботи пристроїв (наприклад, через зміну температури будь–якого з пристроїв). Тому виправлення C_d не використовується, коли швидкість розбіжності визначалася на основі даних, які отримані більш ніж N секунд тому, де N – параметр, який встановлюється адміністратором мережі.

Іноді сеанс, який запланований, може не здійснюватися, наприклад, через вплив сильної перешкоди у період, обраний для сеансу зв'язку. У цьому випадку наступна синхронізація годинника не буде здійснена, і при плануванні чергового сеансу приймаючим вузлом попередньо повинен збільшитися запас T_ω. Також збільшення T_ω відбувається, якщо не використовувалась поправка C_d.

Практичне здійснення описаних механізмів реалізується на модулях сенсорної мережі проекту Ботік-Сенсор.

На поточній апаратній платформі, яка має дві години, були виконані:

– процес калібрування повільного годинника по відношенню до швидкого годинника;

– механізм синхронізації годинників двох пристроїв.

На випробувальній мережі з лінійною топологією, що містить керуючу станцію і чотири сенсорні вузли, проводився експеримент, який полягав у передачі з керуючої станції на будь–який з вузлів ping-пакетів. Усі вузли, крім останнього, здійснили функцію ретрансляції пакетів. Досвід тривав 7 днів, за цей час на кожен із вузлів відправлено понад 66 тисяч ping-пакетів, з яких залишилися без відповіді лише 3 пакети до останнього в ланцюжку вузла. Досвід показав, що застосування описаних у роботі алгоритмів дало можливість вузлам не позбавлятися синхронізації та вдало здійснювати обмін пакетами протягом досить тривалого проміжку часу. Механізм обліку температурних поправок перебуває в стадії реалізації.

Таким чином, розглядається процедура калібрування годинників у сенсорних пристроях для забезпечення їхньої синхронізації та оптимізації роботи. Процес калібрування враховує вплив змін температури на годинники та використовується для компенсації невідповідностей у їхньому функціонуванні.

Також, описано процедуру синхронізації пристроїв у мережі, де приймаючий вузол оцінює час до наступного сеансу зв'язку і планує його так, щоб момент прийому пакета від передавального вузла знаходився в середині інтервалу. Для підтримки синхронізації передається пакет найменшої довжини, і приймаючий вузол використовує збережену мітку початку отримання пакета для корекції часу.

Враховуючи синхронізацію годинників і координацію передачі даних в мережі, можна підтримувати ефективну роботу сенсорних пристроїв і оптимізувати енергоспоживання, що потенційно може вплинути на пропускну здатність та продуктивність мережі.

Також розглядається процедура синхронізації годинників у сенсорних пристроях, зокрема застосування калібрування повільного годинника щодо швидкого. Описано механізми врахування поправок, таких як калібрувальна поправка та температурне виправлення. Процедура синхронізації враховує різноманітні параметри, такі як розбіжність годинників, різниця швидкостей годин та запас на непереборну розбіжність годинника.

Також згадується вплив температурних змін на точність годинників і висуваються методи корекції, такі як температурно–компенсовані генератори та корекційні таблиці. Детально описана процедура калібрування, що передбачає вимірювання показань годинників протягом тривалого часового інтервалу та обчислення калібрувального коефіцієнта для компенсації розбіжності повільного годинника.

У контексті пропускної здатності важливо враховувати, що процес синхронізації і калібрування може вимагати обчислень та обміну даними між пристроями, що може вплинути на пропускну здатність мережі. Крім того, описані процеси можуть викликати періодичні вимірювання та обчислення, що також потребує ресурсів пристроїв та може впливати на їхню продуктивність. Таким чином, здійснення синхронізації годинників пов'язане з управлінням ресурсами мережі та впливає на її пропускну здатність.

3.4 Висновки до третього розділу

У процесі моделювання різноманітних топологій БСМ при синхронізації навантаження визначено дві стадії обслуговування навантаження – стаціонарний процес та перехідний процес. Перехідний процес при цьому не перевищує 200 с для аналізованих додатків.

У процесі моделювання пропускної здатності, зокрема навантаження зі змішаних об'єктів, визначено, що перехідні процеси нижчого рівня з'являються протягом усього процесу моделювання.

Обґрунтовано, що навантаження в результаті синхронізації бездротових сенсорних мереж має властивості самоподібності із середнім ступенем самоподібності, що дає можливість більш точного опису моделі навантаження та може застосовуватися для розрахунку шлюзів між загальними та сенсорними мережами.

Обґрунтовано, що навантаження в бездротових сенсорних мережах зі змішаних об'єктів даних має властивості самоподібності з високим ступенем самоподібності.

За допомогою моделювання синхронізації було отримано значення Херста на її оцінки: з нерухомих вузлів середнє значення становило 0,675, для змішаних вузлів – 0.687, а навантаження сигналізації і реконфігурації – 0,829.

Описаний у роботі метод і алгоритм моделювання пропускної здатності вузлів бездротової сенсорної мережі надає можливість забезпечення точності синхронізації 0,5 мс при періодичності в сеансах зв'язку приблизно 15 с. Гарантується перевага в енергоспоживання більш ніж 20 разів у порівнянні з системами, які забезпечують синхронізацію з точністю 500 мс.

3.5 Питання з охорони праці

За ступенем небезпеки ураження електричним струмом згідно приміщення, в якому відбувається розробка автоматизованого модуля контролю якості поверхонь на основі технологій машинного навчання, належить до класу приміщень без підвищеної небезпеки ураження електричним струмом. Умови, які створюють підвищену і особливу небезпеку (підвищена вологість, струмопровідний пил, струмопровідні підлоги, можливість одночасного дотику до заземлених металоконструкцій будівлі і металевих поверхонь електроприладів), відсутні.

З метою зниження небезпеки ураження людини електричним струмом проектом передбачається використання таких технічних засобів захисту:

– необхідно проводити контроль ізоляції відповідно до вимог. Контроль проводити між нульовим і фазним провідниками і між фазами. Опір ізоляції не менше 500 кОм на фазу. Контроль проводити не рідше 1 разу на рік при відключеному електроживленні;

– в приміщенні використовується система живлючих провідників, трифазна, чотирипровідна з глухо заземленою нейтраллю напругою до 1000 В, тому, використовується система заземлення TN-C-S типу. Всі корпуси ПК з'єднані з глухо заземленою нейтраллю джерела живлення за допомогою нульового захисного провідника.

Автомат захисту вибирається за струмом короткого замикання, час відключення 0,2 с. Додатково застосовується повторне заземлення нульового проводу з метою зниження потенціалу корпусів і напруги дотику у випадках обриву нульового проводу.

Роботи в лабораторії відносяться до робіт категорії 1а – легка фізична робота, яка виконується сидячи.

ВИСНОВКИ

У даній роботі розроблялися та досліджувалися алгоритми пропускної здатності у бездротових сенсорних мережах.

Дослідження стандартів бездротових сенсорних мереж включало аналіз та класифікацію цих стандартів, а також визначення параметрів для різних типів обслуговування. Робота успішно відповідає цьому завданню.

Актуальність застосування бездротових сенсорних мереж у наукових дослідженнях та перспективи розвитку обґрунтовані в роботі, яка розглядає проблеми сучасних бездротових сенсорних мереж та їхні перспективи, зокрема в контексті пропускної здатності.

Дослідження протоколів бездротових сенсорних мереж включає аналіз найактуальніших протоколів, таких як IEEE 802.15.4 WPAN, ZigBee та 6LoWPAN, спрямований на вивчення їхньої пропускної здатності.

Оцінка агрегації даних та аналіз трафіку у роботі дозволяє оцінити агрегацію даних та визначити важливий аспект – зміну дисперсії трафіку, яка впливає на пропускну здатність бездротових сенсорних мереж.

Апроксимація автокореляційної функції та моделювання сценарію пропускної здатності розробленим методом дозволяє точно апроксимувати автокореляційну функцію та моделювати сценарії пропускної здатності вузлів бездротової сенсорної мережі.

Дослідження пропускної здатності даних сенсорних мереж за часом підтверджує ефективність розробленого методу та вказує на переваги в енергоспоживанні порівняно з іншими системами синхронізації.

Обґрунтовано, що навантаження в бездротових сенсорних мережах зі змішаних об'єктів даних має властивості самоподібності з високим ступенем самоподібності.

За допомогою моделювання синхронізації було отримано значення Херста на її оцінки: з нерухомих вузлів середнє значення становило 0,675, для змішаних вузлів – 0,687, а навантаження сигналізації і реконфігурації – 0,829.

Описаний у роботі метод і алгоритм моделювання пропускної здатності вузлів бездротової сенсорної мережі надає можливість забезпечення точності синхронізації 0,5 мс при періодичності в сеансах зв'язку приблизно 15 с. Гарантується перевага в енергоспоживання більш ніж 20 разів у порівнянні з системами, які забезпечують синхронізацію з точністю 500 мс.

Узагальнюючи, висновки роботи дозволяють відповісти на поставлені завдання та підкреслюють важливість досліджень у сфері пропускної здатності бездротових сенсорних мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ 3008:2015. Документація. Звіти у сфері науки та техніки. структура та правила оформлення. Введ. 2015–06–22. К.: Держстандарт України, 2017. 29 с.

2. Методичні вказівки з підготовки та захисту кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 151 Автоматизація та комп’ютерно–інтегровані технології, освітньо–професійних програм: «Автоматизоване управління технологічними процесами», «Комп’ютерно–інтегровані технологічні процеси і виробництва», «Комп’ютеризовані та робототехнічні системи» / Упоряд. І. Ш. Невлюдов, Р. В. Артюх, В. В. Безкоровайний, Н. П. Демська, В. В. Євсєєв, О. І. Филипенко, О. М. Цимбал. – Харків: ХНУРЕ, 2021. – 55 с.

3. Карпов М.С. Аналіз бездротових сенсорних мереж. «Автоматизація та приладобудування» ADED-2023, Випуск 1. с. 270–277

4. Моделі та методи кіберфізичних виробничих систем в концепції Industry 4.0 : монографія / І. Ш. Невлюдов, В. В. Євсєєв, А. О. Андрусевич, С. С. Максимова; – Oktan Print – Prague. 2023. – 321 с.

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

6. Pathan A.–SK, Pathan M., Lee HY (eds.) Advancements in Distributed Computing and Internet Technologies. Trends and Issues. –IGI Global, 2012. – 430 p.

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

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

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

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

11. Bowick Chris. RF Circuit Design. –Newnes, 2007. – 256 p.

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

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

14. Міночкін А.І, Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць № 4. – К.: ВІТІ НТУУ “КПІ”. – 2007. – С. 112 – 119.

15. Тимченко О.В., Зеляновський М.Ю. Методи і протоколи обміну даними сенсорних мереж // Зб. наук. пр. ІПМЕ НАН України. – Вип.46. – К.: 2008. – С. 176–183.

16. Shorey R., Ananda A., Mun Choon Chan, Wei Tsang Ooi. Mobile, wireless, and sensor networks: technology, applications, and future directions // USA: A John Wiley & Sons, Inc. – 2011. – 430 p.

17. Cache J., Wright J, Liu V. Hacking Exposed Wireless (Second edition). –McGraw–Hill, 2010, – 512p.

18. Cache J., Wright J., Liu V. Hacking Exposed Wireless.2nd Edition. – McGraw–Hill, 2010. – 513 p.

19. Faludi R. Building Wireless Sensor Networks: з ZigBee, XBee, Arduino, і Processing.Robert Faludi. Building Wireless Sensor Networks: з ZigBee, XBee, Arduino, і Processing. O'Reilly Media Inc. ,2010. – 318 p.

20. Götz AG Coherent Time Difference of Arrival Estimation Techniques for Frequency Hopping GSM Mobile Radio Signals. –Oldenbourg Verlag München, 2013, 195 pages

21. Muneesawang P., Wu F., Kumazawa I., Roeksabutr A., Liao H.–YM, Tang X. (Eds.) Відповіді в Multimedia Information Processing – PCM 2009.10th Pacific Rim Conference on Multimedia, Bangkok, Thailand, December 15–18, 2009. Proceedings. – Springer, 2009. – XXXVII, 1323 p.

22. Hamilton Charles A. BeagleBone Black Cookbook. –Packt Publishing, 2016. – 358 p.

23. Igoe Tom. Making Things Talk: Using Sensors, Networks, і Arduino до статі, hear, and feel your world. –Maker Media, 2011. – 496 p.

24. Kim T., Hojjat A., Ma J., Fang W., Kang B.(eds.) U – та E–Service, Science and Technology. –Springer, 2012. – 362 p.

25. Komninos N. Sensor Applications, Experimentation, та Logistics. – Springer – 2010, 205 pages

26. Kooijman Matthijs. Building Wireless Sensor Networks Using Arduino. –Packt Publishing, 2015. – 192 p.

27. Kurniawan A. Raspberry Pi Wireless Networks. –Agus Kurniawani, 2015, 138 Pages

28. Liang Q., Wang W., Mu J., Liang J., Zhang B., Pi Y., Zhao C. (eds.) Communications, Signal Processing, and Systems. –Springer, 2012. – 532 pp.

29. Mason A., Mukhopadhyay SC, Jayasundera KP (eds.) Sensing Technology: Current Status and Future Trends III. –New York: Springer, 2014. – 430 p.

30. Meinel Christoph, Sack Harald. Internetworking: Technological Foundations and Applications. –Springer, 2013. – 910 p.

31. Microwave Journal 2009 №06. –Horison House. – 156 p.

32. Lin Z., Mak P.–I., Martins RP Ultra–Low–Power and Ultra–Low–Cost Short–Range Wireless Receivers in Nanoscale CMOS. –Springer International Publishing, 2016. – 110 p.

33. Mistry M. та ін. (Eds.) Advances in Autonomous Robotics Systems.– 15th Annual Conference, TAROS 2014 Birmingham, UK, September 1–3, 2014 Proceedings. – Springer Cham Heidelberg New York Dordrecht London, 2014. XIV, 284 p.

34. EEE Std 802.15.4 –2003 IEEE Standard for Information technology– Telecommunications and information exchange between systems– Local and metropolitan area networks– Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Phys.Institute of Electrical and Electronics Engineers (IEEE), IEEE Computer Society. Approved 12 May 2003. 679 грн.

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

36. Microwave Journal 2014 №05. –Horison House. – 288 p.