Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра _____Автоматизації проектування обчислювальної техніки_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
(рівень вищої освіти)

_____Алгоритми самоорганізації бездротових сенсорних систем_____.
_____.
_____.
(тема)

Виконав: студент 2 курсу, групи СКСм-18-1
_____Бєлоусов В.О._____
(прізвище, ініціали)
Спеціальність _123 – Комп'ютерна інженерія_
(код і повна назва спеціальності)
Тип програми___Освітньо-професійна__
_____
(освітньо-професійна або освітньо-наукова)
Освітня програма_____
_____Спеціалізовані комп'ютерні системи____
_____
(повна назва освітньої програми)
Керівник ___доц. Філіппенко І.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ___Чумаченко С.В.__
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
Кафедра Автоматизації проектування обчислювальної техніки
Рівень вищої освіти другий (магістерський)
Спеціальність 123 – Комп'ютерна інженерія
Тип програми Освітньо-професійна
Освітня програма Спеціалізовані комп'ютерні системи
(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ
НА КУРСОВУ РОБОТУ

студентові Бєлоусову Владиславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Алгоритми самоорганізації бездротових сенсорних систем

затверджена наказом по університету від 04 листопада 2019 р. № 1624 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 12 грудня 2019 р.

3. Вихідні дані до роботи сенсорна мережа, LORA RN2483, Ds18d20, STM32F103

4. Перелік питань, що потрібно опрацювати в роботі алгоритми самоорганізації , вузол сенсорної мережі, протоколи маршрутизації, стандарти бездротового зв'язку

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____
_____
_____
_____
_____

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	03.09.2019-07.09.2019	
2	Аналіз предметної області	11.09.2019-21.09.2019	
3	Аналіз джерел з проблемної галузі	25.09.2019-05.10.2019	
4	Розробка моделі сенсорного вузла	08.10.2019-19.10.2019	
5	Розробка моделі сенсорної мережі	22.10.2019-02.11.2019	
6	Розробка програмної частини	05.11.2019-16.11.2019	
7	Проведення тестування	19.11.2019-30.11.2019	
8	Оформлення пояснювальної записки	03.12.2019-14.12.2019	

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи _____ _____Філіппенко І.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 80 сторінки, 32 рисунки, 1 таблицю, 44 джерела за переліком посилань

СЕНСОРНІ МЕРЕЖІ, СЕНСОРНІ СИСТЕМИ, МАРШРУТИЗАЦІЯ, САМООРГАНИЗАЦІЯ, WI-FI, WIMAX, ZEGBEE, HOMERF.

Об’єкт дослідження – самоорганізована розподілена бездротова сенсорна система (БСС). Предмет дослідження – методи організації передачі даних у розподілених бездротових сенсорних системах. Мета роботи – дослідження методів організації передачі даних у розподілених бездротових сенсорних системах.

Оглянуті основні протоколи маршрутизації, алгоритми самоорганізації бездротових сенсорних мереж. Проведений аналіз апаратних засобів, за допомогою яких можна пообдувати сенсорну мережу.

Запропоновані алгоритми, як для обробки інформації на вузлах так і обробки інформації на серверній стороні, програмно реалізовано ці алгоритми. Проведено тестування як на фізичних пристроях, так і у програмі для моделювання сенсорної мережі.

ABSTRACT

Master's thesis contains 80 pages, 32 figures, 1 tables, 44 sources according to the list of links.

SENSOR NETWORKS, SENSOR SYSTEMS, ROUTE, SELF-ORGANIZATION, WI-FI, WIMAX, ZEGBEE, HOMERF.

The object of study is a self-organized distributed wireless sensor system. The subject of the study is methods of organizing data transmission in distributed wireless sensor systems. The purpose of the study is to investigate the methods of organizing data transmission in distributed wireless sensor systems.

Basic routing protocols, algorithms for wireless sensor network self-organization are examined. An analysis of the hardware by which it is possible to cultivate the sensor network is carried out.

Algorithms, both for processing information on the nodes and for processing information on the server side, have been programmatically implemented. Tests have been carried out both on physical devices and in a program for modeling the sensor network.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

БС – базова станція

БСМ – бездротові сенсорні мережі

БСС – бездротові сенсорні системи

ІКТ – інформаційно-комунікаційні технології

ОС – операційна система

ПЗП – постійний запам'ятовуючий пристрій

ЦУ – центр управління

APTEEN – Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol

CHR – Cluster-Head Relay Routing

DES – Data Encryption Standard

HEED – Hybrid, Energy-Efficient Distributed Clustering

IBSS – Independent Basic Service Set

IDSQ – Information-Driven Sensor Query

LEACH – Low-energy adaptive clustering hierarchy

LPWAN – Low-power Wide-area Network

LQI – Link Quality Indicator

MCN – Master Cluster Node

PEGASIS – Power-Efficient Gathering in Sensor Information Systems

PKM – privacy and key management protocol

QoS – QualityofService

SA – Security Association

SSID – Service Set Identifier

TEEN – Threshold Sensitive Energy Efficient Sensor Network Protocol

TEK – Traffic Encryption Key

ВСТУП

Перспективність розвитку бездротових сенсорних мереж очевидна. Вже зараз у багатьох галузях починають використати БСС. Це і моніторинг екології, автотрафіку, моніторинг погоди, зважаючи на легкість монтажу, відсутності дротів і недорогої апаратної частини. Мініатюрність вузлів мережі забезпечують низьке енергоспоживання, вузли можуть працювати аж до декількох років без заміни джерел живлення. Вузли сенсорної мережі можуть бути як стаціонарними, так і мобільними. Стосовно бездротових сенсорних мереж (БСМ) використовується стандарт ZigBee. З вдосконаленням технологій і ускладнення різних виробництв потреба у бездротових сенсорних мережах тільки ростиме. Але перш ніж впроваджувати мережі їх необхідно ретельно протестувати.

Основними цілями досліджень в області БСС є забезпечення масштабованості, підвищення надійності доставки результатів вимірів, забезпечення необхідної довговічності, узгодження роботи вузлів (синхронізація), підвищення швидкості доставки повідомлень, внутрішньомережева обробка і агрегація результатів. БСС буде повністю функціональною тільки досягши усіх цілей, досягнення окремих цілей без урахування інших немає сенсу. Наприклад, вимогу підвищення довговічності спричиняє за собою необхідність організації дискретного режиму. Для узгодження роботи вузлів в дискретному режимі потрібно синхронізацію. Дискретний режим накладає обмеження на вживані протоколи маршрутизації. Синхронізація вимагає тісної взаємодії з апаратурою, тому повинна тісно взаємодіяти з фізичним і канальним рівнями стека протоколів. Вибір протоколу маршрутизації впливає на масштабованість БСС. Велика кількість вузлів в мережі призводить до довших маршрутів, що знижує довговічність БСС. Наявність конкуруючих сенсів і цілей є однією з характеристик систем, що самоорганізується.

Узгодження значень критеріїв (масштабованість, надійність, довговічність, швидкість доставки повідомлень) має бути виконане у рамках розробки методу самоорганізації БСС, встановленого правила локальних взаємодій вузлів, що у результаті забезпечує потрібну поведінку БСС в цілому. Замість розробки алгоритмів досягнення окремих цілей повинен розроблятися комплексний метод функціонування, ґрунтований на самоорганізації, і спрямований на спільне досягнення необхідних значень названих критеріїв.

Атестаційна робота присвячена розробці алгоритма самоорганізації бездротових сенсорних систем для збору даних від різноманітних сенсорів, для подальшого їх оброблення.

1 БЕЗДРОТОВІ Ad Hoc МЕРЕЖІ

1.1 Бездротові сенсорні мережі. Інфраструктура

В даний час бурхливо розвивається технологія бездротових сенсорних мереж. БСМ – це розподілені мережі, що самоорганізуються, вони стійкі до відмови окремих елементів, та використовують бездротовий зв'язок. Кожен елемент мережі має автономне джерело живлення, мікрокомп'ютер, приймач / передавач. Область покриття мережі може становити від декількох метрів до декількох кілометрів, в залежності від типу модуля і антени, а також за рахунок здатності ретрансляції повідомлень від одного елемента до іншого. Обмін даними між двома кінцевими пристроями може здійснюватися через ретранслятор, в тому випадку, якщо дальність роботи цих пристроїв не дозволяє їх взаємне виявлення. Таким чином, пристрої з малим радіусом дії за допомогою системи ретрансляторів можуть спілкуватися один з одним.

Бездротові мережі будуються за допомогою різноманітних режимів роботи. Одним із таких мережевих режимів роботи є Ad Hoc режим [1].

Ad Hoc – це децентралізований режим бездротової мережі, коли клієнтські станції взаємодіють безпосередньо один з одним без точки доступу або Wi-Fi роутера. Цей режим також називають Independent Basic Service Set (IBSS) або режим Peer to Peer (точка-точка). Для режиму Ad Hoc потрібно мінімум устаткування – досить, щоб кожна станція була оснащена бездротовим адаптером Wi-Fi [2]. При такій конфігурації не потрібно створення якої-небудь мережевої інфраструктури. У цьому режимі кожен вузол бере участь в маршрутизації шляхом пересилки даних для інших вузлів, тому визначення того, які вузли пересилають дані, робиться динамічно на основі мережевого з'єднання і використання алгоритму маршрутизації. Режим Ad Hoc застосовується в основному для створення тимчасових мереж, наприклад, коли треба швидко з'єднати два комп'ютери

для передачі даних [3]. Бездротові мобільні мережі Ad Hoc є самоналагоджувальними динамічними мережами, в яких вузли можуть вільно переміщатися. Бездротовим мережам бракує складнощів в налаштуванні і адмініструванні інфраструктури, що дозволяє пристроям створювати і приєднуватися до мереж «на льоту» – у будь-якому місці і у будь-який час [1].

Стандарт IEEE 802.11 визначає два режими роботи бездротової локальної мережі (WLAN): режим Ad Hoc і режим Інфраструктури.

Інфраструктурний режим (infrastructure mode) застосовується для підключення бездротових клієнтів до існуючої дротяної мережі за допомогою спеціального пристрою, що називається бездротовою точкою доступу (wireless access point). Принцип дії інфраструктурного режиму зображено на рисунку 1.1.

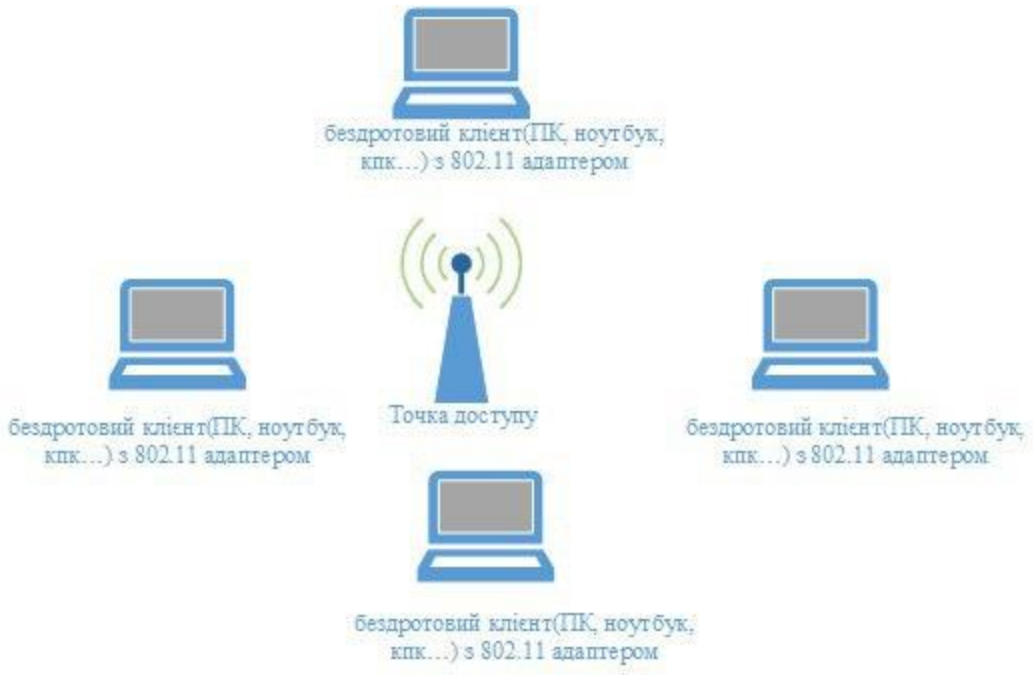

Рисунок 1.1 – Інфраструктурний режим

Одноранговий режим (Ad Hoc mode) застосовується для побудови одноранговых бездротових мереж без застосування точки доступу.

Однорангова бездротова мережа може містити до 9 комп'ютерів, кожен з яких безпосередньо зв'язується з іншими комп'ютерами. На рисунку 1.2 зображено режим Ad Hoc [2].

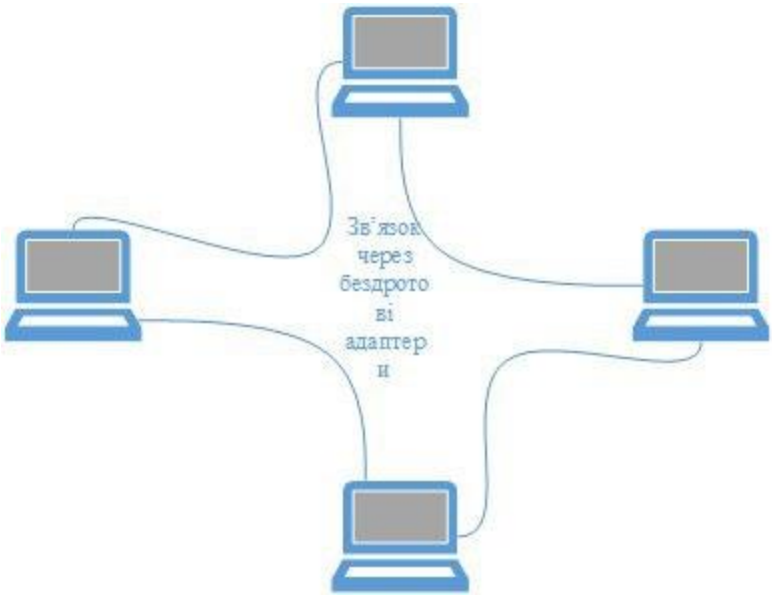

Рисунок 1.2 – Режим Ad Hoc

У режимі Ad Hoc абонентські станції взаємодіють безпосередньо один з одним без використання точки доступу або Wi-Fi роутера [4]. Цей режим називають також IBSS або режим Peer to Peer (рівний з рівним). При такій конфігурації не потрібно створення якої-небудь мережевої інфраструктури. При цьому створюється тільки одна зона обслуговування, що немає інтерфейсу для підключення до дротяної локальної мережі. Будь-які пристрої, оснащені бездротовим мережевим адаптером або інтерфейсом Bluetooth і такі, що знаходяться в межах дії радіосигналу, можна об'єднати один з одним через мережу Ad Hoc. Вона оптимально підходить для швидкого обміну даними між декількома комп'ютерами, стільниковими телефонами, КПК або ноутбуками, які необхідно локально і лише на деякий час з'єднати один з одним.

Мережею Ad Hoc є мережа, що динамічно змінюється, з довільною структурою [2]. Кожен вузол мережі пересилає дані призначені іншим вузлам. При цьому визначення того, якому вузлу передавати дані, робиться динамічно, на підставі зв'язності мережі. Це є їх основною відмінністю від дротяних мереж і керованих бездротових мереж, в яких завдання управління потоками даних виконують маршрутизатори або точки доступу.

Кожен з абонентських пристроїв, залежно від його потужності, має свій радіус дії. Якщо абонент, який знаходиться «на периферії» посилає пакет абонентові, що знаходиться в центрі мережі, відбувається так званий багатострибковий процес передачі пакету через вузли, що знаходяться на шляху заздалегідь прокладеного маршруту. Таким чином, кожен новий абонент за рахунок своїх ресурсів збільшує радіус дії мережі. Отже, потужність кожного окремого пристрою може бути мінімальною. А це припускає як менші вартості абонентських пристроїв, так і кращі показники безпеки і електромагнітної сумісності. Приблизний вигляд Ad Hoc мережі зображено на рисунку 1.3 [2].

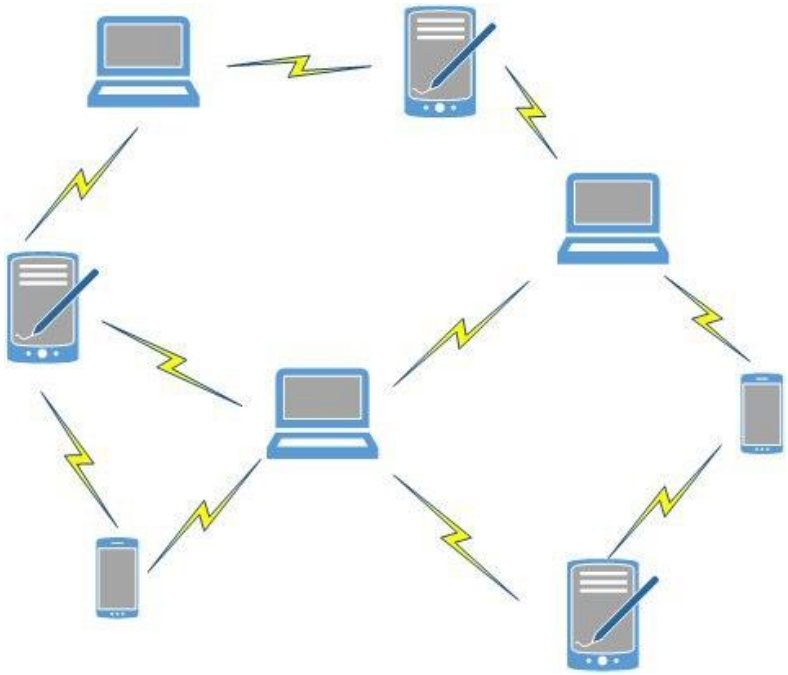

Рисунок 1.3 – Приблизний вигляд Ad Hoc мережі

1.2 Особливості функціонування сенсорної мережі

Особливості бездротових Ad Hoc мереж [3]:

– загальне середовище передачі даних;
– усі вузли мережі спочатку рівноправні;
– мережа є такою, що є самоорганізованою;
– кожен вузол виконує роль маршрутизатора;
– топологія мережі може вільно мінятися;
– в мережу можуть вільно входити нові і виходити старі вузли.

Розглянемо умови успішної побудови бездротової мережі в режимі Ad Hoc [3].

1. Пряма видимість між комп'ютерами, що підключаються. При підключенні в режимі Ad Hoc дуже важливим чинником, що впливає на швидкість роботи мережі, є розташування комп'ютерів в межах прямої видимості. Це пов'язано з тим, що потужність передавачів бездротових адаптерів дещо нижча, ніж, потужність точок доступу. Відповідно, радіус дії такої мережі приблизно удвічі менше, ніж радіус мережі, побудованої із застосуванням інфраструктурного режиму (з використанням точки доступу). Збільшити радіус дії мережі Ad Hoc можна, якщо застосувати потужніші антени [2]. Якщо між комп'ютерами існують перешкоди, наприклад, стіни офісу, то радіус роботи мережі і швидкість різко скоротиться.

2. Стандарт бездротових адаптерів. Як відомо, від стандарту, в якому працюють мережеві адаптери, залежить швидкість передачі даних в мережі. Якщо на одному комп'ютері встановлений пристрій, стандарт якого підтримує нижчу швидкість передачі даних, то швидкість роботи усієї мережі дорівнюватиме швидкості цього адаптера. Тому рекомендується використати адаптери єдиного стандарту.

3. Кількість підключених комп'ютерів. Це пов'язано в першу чергу з особливостями процесу обміну інформацією між комп'ютерами. Для бездротових мереж, особливо при використанні режиму Ad Hoc, цей чинник

є особливо важливим. Тому для успішного функціонування мережі в режимі Ad Hoc слід обмежити кількість підключень (від двох до дев'яти). Якщо їх кількість перевищує рекомендоване, то вигіднішим рішенням в цій ситуації буде використання точки доступу і режиму інфраструктури.

Нині існує декілька «базових» технологій для побудови Ad Hoc мереж:

– Bluetooth;

– ZigBee;

– Wi-Fi.

Для побудови мережі Ad Hoc використовуються адаптери, що підключається через слот розширення PCI, PCMCI, CompactFlash. Існують також адаптери з підключенням через порт USB 2.0. Wi-Fi-адаптер виконує ту ж функцію, що і мережева карта в дротяній мережі [4]. Він служить для підключення комп'ютера користувача до бездротової мережі. Завдяки платформі Centrino усі сучасні ноутбуки мають вбудовані адаптери Wi-Fi, які сумісні з багатьма сучасними стандартами. Wi-Fi-адаптерами, як правило, забезпечені і КПК (кишенькові персональні комп'ютери), що також дозволяє підключати їх до бездротових мереж.

Основні достоїнства режиму Ad Hoc – швидке розгортання мережі і простота організації (не потрібно точки доступу).

До недоліків такого варіанту побудови мережі відносяться малий радіус дії і низька перешкодозахищеність.

Режим Ad Hoc в основному застосовується для створення тимчасових мереж передачі даних, наприклад, транспортні, офісні мережі, військовий зв'язок [3].

1.3 Огляд вузла сенсорної мережі

БСМ складаються з мініатюрних обчислювальних пристроїв, побудованих з використанням датчиків, актуаторами і трансиверами (прийомо / передавачами), що працюють в заданому діапазоні радіочастот.

Габаритні розміри сенсорного вузла становить кілька квадратних сантиметрів. На платі пристрою розміщуються процесор, пам'ять, цифро-аналогові і аналого-цифрові перетворювачі, радіочастотний приймач, джерело живлення і різноманітні датчики, актуатори.

Таким чином, апаратна частина вузла бездротової мережі може бути розділена на наступні чотири підсистеми:

а) комунікаційна підсистема, що забезпечує бездротовий зв'язок з іншими вузлами в сенсорної мережі і містить радіо приймач;

б) обчислювальна підсистема, яка забезпечує обробку даних і функціональність вузла і складається з мікроконтролера MCU, до складу якого входять процесор, оперативна SRAM, незалежна EEPROM і флеш-пам’ять, аналого-цифровий перетворювач ADC, таймер, порти введення / виводу;

в) сенсорна підсистема, що забезпечує з'єднання сенсорного бездротового вузла із зовнішнім світом, до складу якої можуть входити аналогові і цифрові сенсори, актуатори;

г) підсистема електроживлення,яка забезпечує енергетичне постачання всіх елементів бездротового сенсорного вузла і включає пристрої генерації і акумулювання енергії, а також регулювання напруги.

Отримані від датчика електричні сигнали часто не готові для обробки, тому вони проходять в мотелі через стадію перетворення. Наприклад, сигнал часто вимагає посилення для збільшення амплітуди, можливе застосування фільтрів для усунення небажаного шуму в певних діапазонах частот і т.п. Перетворений сигнал трансформується за допомогою аналого-цифрового перетворювача (АЦП) в цифровий сигнал. В результаті сигнал виходить в цифровій формі, і він готовий до подальшої обробки в процесорі і зберігання в пам’яті мікроконтролера. При наявності виконавчих механізмів існує можливість застосовувати вплив на зовнішнє середовище через актуатор вузлів мережі. Крім розмірів, є й інші жорсткі обмеження для вузлів БСС. Структура сенсорного вузла зображена на рисунку 1.4.

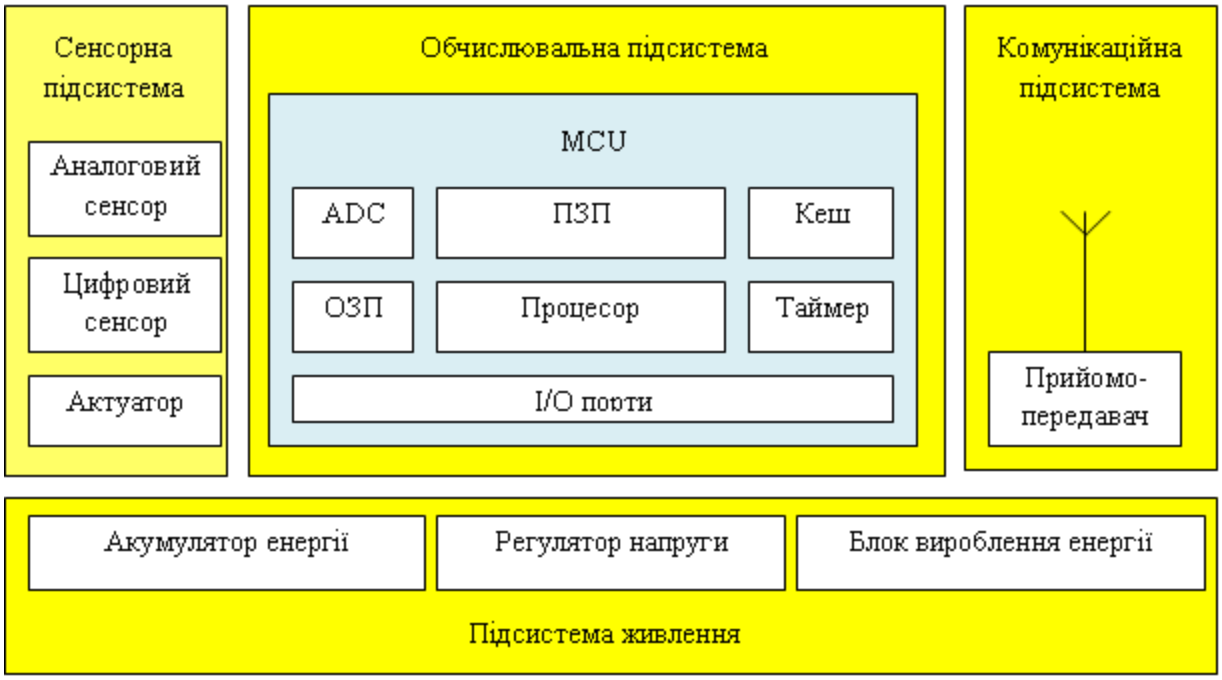

Рисунок 1.4 – Структура сенсорного вузла

Вони повинні:

– споживати мало енергії;

– працювати з великою кількістю вузлів;

– мати низьку вартість виробництва;

– бути автономними і працювати без обслуговування;

– адаптуватися до навколишнього середовища.

Для виконання функцій на сенсорні вузли може встановлюватися операційна система (ОС). ОС дозволяє сенсорам автоматично встановлювати зв'язки з сусідами і формувати сенсорну мережу заданої топології. Оскільки однією з найважливіших функцій сенсорів є автоматичний вибір схеми організації мережі і маршрутів передачі даних, БСМ по суті є самоналагоджувальна. Найчастіше сенсорний вузол повинен мати можливість самостійно визначити своє місце розташування, по відношенню до того іншому сенсора, якому він буде передавати дані. Тобто спочатку відбувається ідентифікація всіх сенсорів, а потім вже формується схема маршрутизації.

Сенсорні вузли можуть закріплюватися стаціонарно, а також мати відносну мобільність, тобто довільно переміщатися одна відносно одної в деякому просторі, не порушуючи при цьому логічної зв'язаності мережі. В останньому випадку сенсорна мережа не має фіксованої постійної топології, і її структура динамічно змінюється з плином часу.

1.4 Типова архітектура бездротової сенсорної мережі

Типова архітектура бездротової сенсорної мережі включає три типи вузлів [4]:

– координатор;
– маршрутизатор;
– кінцевий вузол.

Архітектура бездротової сенсорної мережі на рисунку 1.5.

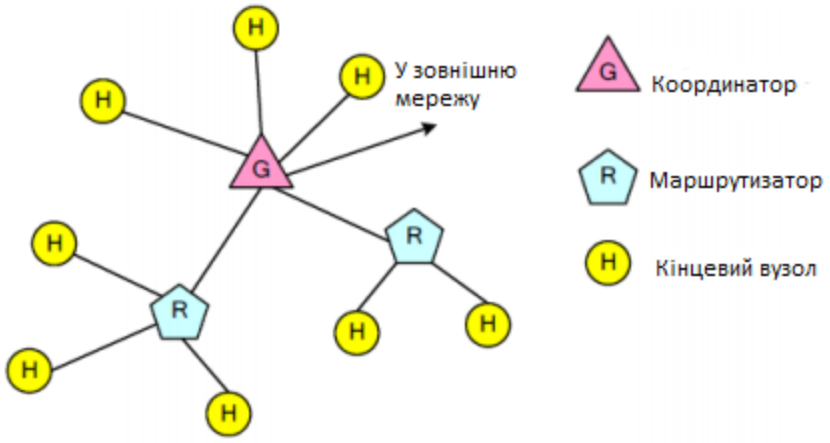

Рисунок 1.5 – Архітектура бездротової сенсорної мережі

Координатор – здійснює глобальну координацію, організацію та установку параметрів мережі, є найбільш складним пристроєм БСМ, вимагає найбільший об’єм пам’яті і найбільшу потужність джерела живлення. В одній мережі повинен бути присутнім тільки один координатор. З

координатора здійснюється вихід в зовнішню мережу (він реалізує функцію шлюзу - gateway). Часто координатор називають базовою станцією (БС) [3].

Координатор виконує наступні функції:

– визначає незадіяні канали з переліку каналів, доступних для організації мережі і визначаються розробником і організовує мережу;

– передає мережеві сигнальні пакети з інформацією про існуючої мережі;

– управляє мережевими підлеглими пристроями, встановлює параметри мережі визначає максимальну глибину вкладених підмереж, число;

– мережевих маршрутизаторів і число підлеглих пристроїв;

– забезпечує маршрутизацію інформації між підлеглими пристроями;

– більшу частину часу перебуває в режимі прийому;

– забезпечує організацію таблиць маршрутизації;

– дозволяє маршрутизаторів і кінцевим пристроям входити в мережу.

Маршрутизатор – приймає, буферизує і передає дані від інших вузлів БСС, а також визначає напрямок передачі.

Маршрутизатор виконує наступні функції:

– визначає активні канали, підключається до мережі і дозволяє кінцевим пристроїв входити в мережу – використовує додаткові, визначені додатком, списки активних каналів;

– ретранслює сигнальні мережеві пакети з параметрами мережі від координатора;

– адмініструє мережеві адреси підключених до маршрутизатора підлеглих пристроїв;

– підтримує наступні класи пристроїв маршрутизації: пристрій з таблицею маршрутизації і з функцією деревовидної маршрутизації, пристрій тільки з функцією деревовидної маршрутизації, підтримка функції аварійної деревовидної маршрутизації;

– підтримує два режими роботи пристроїв: без переходу в «сплячий режим» і з переходом в «сплячий» режим в періоди, які визначаються координатором мережі і параметрами мережевої синхронізації;

– підтримує функції маршрутизації багатоячейкових мереж: створює таблиці сусідніх мережевих вузлів з параметром якості зв'язку з кожним з них, створює таблиці мережевої маршрутизації, ретранслює пакети запиту і підтвердження визначення маршрутів між пристроями;

– підтримує функції маршрутизації багатоячейкових мереж: створює таблиці сусідніх мережевих вузлів з параметром якості зв'язку з кожним з них, створює таблиці мережевої маршрутизації, ретранслює пакети запиту і підтвердження визначення маршрутів між пристроями;

– підтримує функції маршрутизації по деревовидному принципом транслює повідомлення вгору і вниз по ієрархічній структурі дерева гілки в залежності від адреси одержувача повідомлення.

Кінцеве (кінцеве) пристрій (сенсорний вузол) – виконує тільки прикладні дії (збір інформації та управління віддаленим об’єктом) і не здійснює ретрансляцію даних.

Сенсорний вузол має так і особливості [3]:

– завжди шукає і намагається увійти в існуючу мережу – використовує додаткові, визначені додатком, списки активних каналів і сигнальні пакети синхронізації існуючої мережі для визначення параметрів мережі та маршрутизатора для входу в мережу;

– живиться від автономного джерела (батареї);

– з пакетів синхронізації визначає наявність даних від координатора;

– запрошує дані від координатора;

– здатний знаходитися тривалий час в «сплячому» режимі (до 99,99% від всього часу роботи).

По виконуваних наборам функцій все вузли БСМ можна віднести до двох видів:

– пристрій з повним набором функцій FFD (Fully Function Device):

– підтримка стандарту IIIEE 802.15.4;

– додаткова пам’ять і енергоспоживання дозволяють виконувати роль координатора мережі;

– підтримка всіх типів топологій («точка-точка», «зірка», «дерево», «чарункова мережа»);

– здатність звертатися до інших пристроїв в мережі.

– пристрій з обмеженим набором функцій RFD (Reduced Function Device):

– підтримує обмежений набір функцій стандарту IIIEE 802.15.4;

– підтримка топології «точка-точка», «зірка»;

– не виконує функції координатора;

– звертається до координатора мережі і маршрутизатора.

2 ОСНОВНІ СТАНДАРТИ БЕЗДРОТОВИХ МЕРЕЖ

2.1 Стандарт Wi-Fi

Wi-Fi – торгова марка Wi-FiAlliance для бездротових мереж на базі стандарту IEEE 802.11[4]. Ноутбук або комунікатор без підключення до мережі Інтернет сьогодні є практично марним шматком «заліза». Завдяки широкому використанню Wi-Fi для вирішення проблеми підключення до Інтернету цей термін став добре відомим.

Продукти, що призначалися спочатку для систем касового обслуговування, були виведені на ринок під маркою WaveLAN і забезпечували швидкість передачі даних від 1 до 2 Мбіт / с. Творець Wi-Fi – Вік Хейз (Vic Hayes) знаходився в команді, що брала участь в розробці таких стандартів, як IEEE 802.11b, IEEE 802.11a і IEEE 802.11g. зазвичай схема мереж Wi-Fi містить не менше однієї точки доступу і не менше одного клієнта [4].

Точка доступу передає свій ідентифікатор мережі (Service Set Identifier (SSID)) за допомогою спеціальних сигнальних пакетів на швидкості 0,1 Мбіт / с кожні 100 мс, тому 0,1 Мбіт / с – найменша швидкість передачі даних для Wi-Fi. Знаючи SSID мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних про рівень сигналу. Стандарт Wi-Fi дає клієнтові повну свободу при виборі критеріїв для з'єднання.

Для організації бездротової мережі в замкнутому просторі застосовуються передавачі зі всеспрямованими антенами. Слід мати на увазі, що через стіни з великим вмістом металевої арматури (в залізобетонних будівлях такими є несучі стіни) радіохвилі діапазону 2,4 ГГц іноді можуть взагалі не проходити, тому в кімнатах, розділених подібної стіною,

доведеться ставити свої точки доступу. Потужність, яку випромінює передавачем точки доступу або ж клієнтської станції, що працює за стандартом IEEE 802.11, не перевищує 0,1 Вт, але багато виробників бездротових точок доступу обмежують потужність лише програмним шляхом, і досить просто підняти потужність до 0,2-0,5 Вт [4].

2.2 Стандарт WiMAX

WiMAX – це система далекої дії, що покриває кілометри простору, яка зазвичай використовує ліцензовані спектри частот (хоча можливо використання і неліцензованих частот) для надання з'єднання з Інтернетом типу точка-точка провайдером кінцевому користувачеві. Різні стандарти сімейства 802.16 забезпечують різні види доступу, від мобільного (схожий з передачею даних у мобільних телефонів) до фіксованого (альтернатива провідного доступу, при якому бездротове обладнання користувача прив'язане до розташування) [5].

WiMAX і Wi-Fi мають абсолютно різний механізм QualityofService (QoS). WiMAX використовує механізм, заснований на встановленні з'єднання між БС і пристроєм користувача. Кожне з'єднання засноване на спеціальному алгоритмі планування, який може гарантувати параметр QoS для кожного з'єднання. Wi-Fi, в свою чергу, використовує механізм QoS подібний до того, що використовується в Ethernet, при якому пакети отримують свої пріоритети. Такий підхід не гарантує однаковий QoS для кожного з'єднання.

Набір переваг притаманний всьому сімейству WiMAX, однак його версії істотно відрізняються один від одного. розробники стандарту шукали оптимальні рішення як для фіксованого, так і для мобільного застосування, але поєднати всі вимоги в рамках одного стандарту не вдалося. Хоча ряд базових вимог збігається, націленість технологій на різні ринкові ніші

призвела до створення двох окремих версій стандарту (вірніше, їх можна вважати двома різними стандартами).

Кожна з специфікацій WiMAX визначає свої робочі діапазони частот, ширину смуги пропускання, потужність випромінювання, методи передачі та доступу, способи кодування і модуляції сигналу, принципи повторного використання радіочастот та інші показники. Тому WiMAX-системи,засновані на версіях стандарту IEEE 802.16 e і d, практично несумісні.

Основна відмінність двох технологій полягає в тому, що фіксований WiMAX дозволяє обслуговувати тільки статичних абонентів, а мобільний орієнтований на роботу з користувачами, що пересуваються зі швидкістю до 150 км / г [5].

У загальному вигляді WiMAX мережі складаються з наступних основних частин:базових і абонентських станцій, а також обладнання, що зв'язує БС між собою, з постачальником сервісів і з Інтернетом. Структура мереж сімейства стандартів IEEE 802.16 схожа з традиційними GSM-мережами (БС діють на відстанях до десятків кілометрів, для їх установки не обов'язково будувати вежі – допускається установка на дахах будинків при дотриманні умови прямої видимості між станціями). WiMAX застосовується як для вирішення проблеми «останньої милі», так і для надання доступу в мережу офісним та районним мережам [5].

2.3 Стандарт Bluetooth

Bluetooth забезпечує обмін інформацією між такими пристроями як персональні комп'ютери (настільні, кишенькові, ноутбуки), мобільні телефони, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, недорогий,повсюдно доступній радіочастоті для ближнього зв'язку. Бездротовий канал дозволяє цим пристроям повідомлятися, коли вони знаходяться в радіусі від 1 до 200 м

один від одного (дальність сильно залежить від перешкод), навіть у різних приміщеннях. Варто відзначити, що компанія AIRcable випустила Bluetooth - адаптер Host XR з радіусом дії близько 30 км. Для спільної роботи Bluetooth - пристроїв необхідно, щоб всі вони підтримували загальний профіль. Профіль – набір функцій або можливостей, доступних для певного пристрою Bluetooth. Технологія Bluetooth спирається на неліцензованому (практично скрізь, крім Росії) частотний діапазон 2,4 ÷ 2,4835 ГГц. При цьому використовуються широкі захисні смуги: нижня межа частотного діапазону становить 2 ГГц, а верхня – 3,5 ГГц. Частота (положення центру спектра) задається з точністю ± 75 кГц. Дрейф частоти в цей інтервал не входить. Кодування сигналу здійснюється подворівневою схемою GFSK (Gaussian Frequency ShiftKeying). логічного 0і 1 відповідають дві різні частоти. В обумовленої частотній смузі виділяється 79 радіоканалів по 1 МГц кожен [6].

2.4 Стандарт HomeRF

HomeRF – бездротова технологія, спеціально орієнтована на мережі, створювані в домашніх умовах. Головна ідея HomeRF полягає втому, що у домашніх користувачів потреби зовсім відмінні від потреб корпоративних користувачів. Це означає, що і рішення,які для них потрібні, спеціально для них і розроблені. HomeRF прагне працювати в цій ніші ринку, поставляючи пристрої, які досить легко встановлюються, прості у використанні і більш доступні, ніж сучасні бездротові рішення масштабу підприємства.

HomeRF заснований на декількох існуючих стандартах передачі голосу і даних і об’єднує їх в єдине рішення. Воно працює в смузі частот ISM 2,4 ГГц з використанням FHSS. Скачки по частотах відбуваються зі швидкістю від 50 до 100 разів на секунду. Позбавлення від інтерференції відбувається за допомогою рознесення сигналів за часом і частоті.

HomeRF використовує радіопередавачі низької потужності, які подібні до тих, що використовуються в персональних бездротових мережах

стандарту 802.15 на основі технології Bluetooth. Різниця між двома технологіями полягає в тому, що HomeRF орієнтована тільки на ринок домашніх користувачів, включаючи SWAP (Standard Wireless AccessProtocol – стандартний протокол бездротового доступу), який в рамках HomeRF дає можливість більш ефективно обробляти мультімедіа додатки. Передавачі діють на відстані 40 – 50 м від БС і можуть бути вбудовані в картки типу CompactFlash [7].

2.5 Стандарт ZigBee

ZigBee – назва набору мережевих протоколів верхнього рівня, використовують маленькі, малопотужні радіопередавачі, засновані на стандарті IEEE 802.15.4. Цей стандарт описує бездротові персональні обчислювальні мережі (WPAN). ZigBee націлена на додатки, яким потрібен тривалий час автономної роботи від батарей і висока безпека передачі даних при невеликих швидкостях їх передачі.

Основна особливість технології ZigBee полягає в тому, що вона при відносно невисокому енергоспоживанні підтримує не тільки прості топології бездротового зв'язку («точка-точка» і «зірка»), а й складні бездротові мережі з комірчастою топологією з ретрансляцією і маршрутизацією повідомлень. Області застосування даної технології – це побудова бездротових мереж датчиків, автоматизація житлових і споруджуваних приміщень, створення індивідуального діагностичного медичного обладнання, системи промислового моніторингу та управління, а також при розробці побутової електроніки і персональних комп'ютерів.

Мережі, утворені за протоколом ZigBee почали розглядатися з1998 року, коли виникла необхідність в самоорганізованих системах зв'язку ZigBee, націлений на додатки, яким потрібен тривалий час автономної роботи від батарей і висока безпека передачі даних, при невеликих швидкостях передачі. ZigBee працює в промислових, наукових і медичних

(ISM-діапазон) радіодіапазоні: 868 МГц в Європі, 915 МГц в США і в Австралії і 2,4 ГГц в більшості країн в світі.

Так як ZigBee – пристрій велику частину часу перебуває в сплячому режимі, рівень споживання енергії може бути дуже низьким, завдяки чому досягається тривала робота від батарей. ZigBee – пристрій може активуватися (тобто переходити від сплячого режиму до активного) за 15 мс або менше, затримка його відгуку може бути дуже малою, особливо в порівнянні з Bluetooth, для якого затримка, що утворюється при переході від сплячого режиму до активного,зазвичай досягає трьох секунд.

Беручи до уваги такі критерії, як ціна чіпів, дешевизна і швидкість освоєння технології, низьке енергоспоживання і перешкодозахищеність, можна сказати, що ZigBee нерідко є зараз найкращим вибором. Чіпи для реалізації ZigBee випускають такі відомі фірми, як TexasInstruments, Freescale, Atmel, STMicroelectronics, OKI і т.д. Це гарантує низькі ціни на комплектуючі для даної технології. ZigBee – це технологія, що заповнює нішу низькошвидкісних бездротових мереж з низьким енергоспоживанням, призначених для систем управління з великою кількістю вузлів, таких як системи освітлення в будівлях, системи спостереження за парком промислового обладнання і т.д. [8].

Порівняння деяких параметрів популярних стандартів бездротових систем надано в таблиці 2.1.

Таблиця 2.1 – Порівняння бездротових систем

Стандарт	Wi-Fi (IEEE 802.11b)	Bluetooth (IEEE 802.15.1)	ZigBee (IEEE 802.15.4)
1	2	3	4
Частотний діапазон	2,4-2,48ГГц	2,4-2,483ГГц	2,4-2483 ГГц

Продовження таблиці 2.1

1	2	3	4
Пропускна спроможність кбіт / с	11000	723,1	250
Розмір стека протоколу, кбайт	Більше ніж 1000	Більш ніж 250	32-64
Час безперервної роботи від батареї, дні	0,5-5	1-10	100-1000
Максимальна кількість вузлів в мережі	10	7	65536
Діапазон дії, м	20-300	10-100	10-100
Галузь застосування	Передача мультимедійної інформації (Інтернет, пошта, відео)	Заміна дротового з’єднання	Віддалений моніторинг і управління

3 БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

3.1 Загальні принципи безпеки передачі даних у БСМ

Забезпечення безпечної передачі даних у бездротових сенсорних мережах є дуже важливою задачею.

При рішенні задач, пов'язаних із забезпеченням безпечної передачі даних у бездротових сенсорних мережах, слід враховувати наступні чинники:

– обмежені обчислювальні ресурси вузла мережі (об'єм оперативної пам'яті мікроконтролера може складати від 1 до 4 Кб, тактова частота – 20 Мгц), а в деяких випадках і обмежені ресурси самої мережі (середня швидкість передачі між вузлами може складати до 100 байт / с);

– відсутність центрального (головного) вузла – відсутність єдиної точки ухвалення рішень з огляду на те, що в основі бездротових сенсорних мереж лежить однорангова фізична топологія;

– невеликий розмір пакету даних, що передається по бездротовому каналі між вузлами мережі, який, як правило, складає 10 – 100 байт.

Таким чином, традиційні криптографічні алгоритми не можуть бути використані для забезпечення безпеки даних у БСМ зважаючи на приведені вище причини. Нині є актуальним рішення наступних завдань:

– розробка алгоритмів шифрування, орієнтованих на застосування в пристроях з обмеженими обчислювальними ресурсами;

– розробка алгоритмів шифрування, які можуть працювати з різними довжинами блоків, враховуючи при цьому енергоспоживання пристрою і вірогідності колізій;

– розробка алгоритмів обміну ключовою інформацією.

В результаті проведених досліджень був обраний блоковий симетричний алгоритм шифрування даних для застосування у вузлах БСМ. Схема шифрування алгоритму ґрунтована на використанні мережі Фейстеля і

дискретною хаотичного відображення. Подібна комбінація структурних елементів дозволяє балансувати між розміром шифрованого блоку, криптографічною стійкістю, вихідної послідовності і тривалістю процедури шифрування.

Розроблений алгоритм реалізований на платформі 8-бітових мікроконтролерів Atmel і вбудований у базову функціональність бездротового приймача типу ППС – 40а. Робочі характеристики вказаної реалізації алгоритму: використання пам'яті для зберігання програм – 762 байт, використання оперативної пам'яті – 241 байт, максимальна швидкість обробки даних – 88,2 Кбіт / с.

3.2 Безпека в мережах Wi-Fi

Безпека у Wi-Fi забезпечується завдяки шифруванню. Стандарт шифрування WEP може бути відносно легко зламаний, навіть при правильній конфігурації (через слабку стійкість алгоритму). Незважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і WPA2, багато старих точок доступу немає підтримки його і вимагають заміни.

Прийняття стандарту IEEE 802.11i (WPA2) в червні 2004 року зробило доступною більш ефективну схему аутентифікації і шифрування, яка застосовується в новому обладнанні. Для реалізації протоколів WPA і WPA2 потрібно більш надійний пароль, ніж той, який зазвичай призначається користувачем.

Продукти для бездротових мереж, що відповідають стандарту IEEE802.11, пропонують чотири рівні засобів безпеки: фізичний, ідентифікатор набору служб (SSID), ідентифікатор управління доступом до середовища (MAC ID - Media Access Control ID) і шифрування.

Багато організацій використовують додаткове шифрування (наприклад, VPN) для захисту від вторгнення. На даний момент основним методом злому

WPA2 є підбір пароля, тому рекомендується використовувати складні цифро-буквені паролі для того, щоб максимально ускладнити завдання підбору пароля [9].

3.3 Безпека в мережах WiMAX

Питання безпеки в мережах WiMAX, заснованих на стандарті IEEE 802.16, а також як і в мережах WiFi (IEEE 802.11), стоять дуже гостро в зв'язку з легкістю підключення до мережі.

Стандартам IEEE 802.16 визначає протокол privacy and key management protocol (PKM), протокол приватності і управління ключем.

У мережах WiMAX поняття захищеного зв'язку SA (Security Association) – це одностороннє з'єднання для забезпечення захищеної передачі даних між пристроями мережі.

SA бувають двох типів:

– Data Security Association, захищена мережа для даних;

– Authorization Security Association, захищена мережа для авторизації.

Захищений зв'язок для даних в свою чергу буває трьох типів:

– первинний (основний) (Primary SA);

– статичний (Static SA);

– динамічний (Dynamic SA).

Первинний захищений зв'язок встановлюється абонентською станцією на час процесу ініціалізації. БС потім надає статично захищений зв'язок. Що стосується динамічних захищених зв'язків, то вони встановлюються і ліквідуються в міру необхідності для сервісних потоків. Як статично, так і динамічно захищений зв'язок може бути одним для декількох абонентських станцій.

Захищений зв'язок для даних визначається.

1) 16-бітовим ідентифікатором зв'язку.

2) Методом шифрування, вживаним для захисту даних в з'єднанні.

3) Двома Traffic Encryption Key (TEK, ключ шифрування трафіку), поточний і той, який використовуватиметься, коли у поточного TEK закінчиться термін життя.

4) Двома 2-бітовими ідентифікаторами, по одному на кожного TEK. Часом життя TEK може мати значення від 30 хвилин до 7 днів. Значення за умовчанням 12 годин.

5) Двома 64-бітовими векторами ініціалізації, по одному на TEK (вимагається для алгоритму шифрування Data Encryption Standard (DES)).

6) Індикатором типу зв'язку (первинний, статичний або динамічний).

Захищений зв'язок для авторизації визначається.

1) сертифікатом X.509, що ідентифікує абонентську станцію, а також сертифікатом X.509, що ідентифікує виробника абонентської станції.

2) 160-бітовим ключем авторизації (authorization key, AK). Використовується для аутентифікації під час обміну ключами TEK.

3) 4-бітовим ідентифікатором ключа авторизації.

4) Часом життя ключа авторизації. Може набувати значення від 1 дня до 70 днів. Значення за умовчанням 7 днів.

5) 128-бітовим ключем шифрування ключа (Key encryption key, KEK).

6) Використовується для шифрування і розподілу ключів TEK.

7) Ключем HMAC для низхідних повідомлень (downlink) при обміні ключами TEK.

8) Ключем HMAC для висхідних повідомлень (uplink) при обміні ключами TEK.

9) Списком data SA, для якого ця абонентська станція авторизована.

10) Ключ шифрування ключа KEK обчислюється таким чином:

11) Проводиться конкатенація шістнадцятиричного числа 0x53 з самим собою 64 рази. Виходять 512 біт.

12) Справа приписується ключ авторизації.

13) Обчислюється хэш-функция SHA - 1 від цього числа. Виходять 160 біт на виході.

14) Перші 128 біт беруться в якості KEK, інші відкидаються.

Ключі HMAC обчислюються таким чином.

1) Проводиться конкатенація шістнадцятиричного числа 0x3a (uplink) або 0x5c (downlink) з самим собою 64 рази.

2) Справа приписується ключ авторизації.

3) Обчислюється хэш-функция SHA - 1 від цього числа. Виходять 160 біт на виході. Це і є ключ HMAC.

У мережах WiMAX використовуються наступні протоколи аутентифікації.

1. Extensible Authentication Protocol (EAP, розширюваний протокол аутентифікації) – це протокол, що описує гнучкішу схему аутентифікації в порівнянні з сертифікатами X.509. EAP- повідомлення кодуються прямо в кадри управління. У зв'язку з цим в протокол PKM було додано два нові повідомлення PKM EAP request (EAP- запит) і PKM EAP response (EAP-відповідь). Стандарт IEEE 802.16e не встановлює який-небудь певний метод аутентифікації EAP, ця область зараз активно досліджується [10].

2. Privacy and Key Management Protocol (PKM Protocol) – це протокол для отримання авторизації і ключів шифрування трафіку TEK.

Стандарт IEEE 802.16 використовує алгоритм DES в режимі зчеплення блоку шифрів для шифрування даних. Нині DES вважається небезпечним, тому в доповненні до стандарту IEEE 802.16e для шифрування даних був доданий алгоритм AES.

Стандарт 802.16e визначає використання шифрування AES в чотирьох режимах:

– Cipher Block Chaining (CBC, режим зчеплення блоку шифрів);

– Counter Encryption (CTR, шифрування лічильника);

– Counter Encryption with Cipher Block Chaining message authentication code (CCM, счетчикове шифрування з message authentication code, отриманим

зчепленням блоку шифрів). Додає можливість перевірки достовірності зашифрованого повідомлення до режиму CTR;

– Electronic Code Book (ECB, режим електронної кодової книги), використовується для шифрування ключів TEK

Уразливості в стандарті IEEE 802.16.

1. Атаки фізичного рівня, такі як глушення передачі сигналу, що веде до відмови доступу або лавинний наплив кадрів (flooding), що має на меті виснажити батарею станції. Ефективних способів протистояти таким загрозам на сьогодні немає.

2. Самозвані БС, що пов'язано з відсутністю сертифікату БС. У стандарті проявляється явна несиметрична в питаннях аутентифікації. Запропоноване рішення цієї проблеми – інфраструктура управління ключем у бездротовому середовищі (WKMI, wireless key management infrastructure), ґрунтована на стандарті IEEE 802.11i. У цій інфраструктурі є взаємна аутентифікація за допомогою сертифікатів X.509.

3. Уразливість, пов'язана з невипадковістю генерації БС ключів авторизації. Взаємна участь базової і абонентської станції, можливо, розв'язала б цю проблему.

4. Можливість повторно використати ключі TEK, чий термін життя вже збіг. Це пов'язано з дуже малим розміром поля EKS індексу ключа TEK. Оскільки найбільший час життя ключа авторизації 70 діб, тобто 100800 хвилин, а найменший час життя ключа TEK 30 хвилин, те необхідне число можливих ідентифікаторів ключа TEK - 3360. А це означає, що число необхідних біт для поля EKS – 12.

5. Ще одна проблема пов'язана, як уже згадувалося, з небезпекою використання шифрування DES. При досить великому часі життя ключа TEK і інтенсивному обміні повідомленнями можливість злому шифру представляє реальну загрозу безпеки. Ця проблема була усунена з введенням шифрування AES в поправці до стандарту IEEE 802.16e. Проте, велике число користувачів досі має устаткування, що підтримує лише старий стандарт IEEE 802.16 [11].

3.4 Вбудовані системи безпеки у Bluetooth

Для захисту Bluetooth-з'єднання передбачено шифрування переданих даних, а також виконання процедури авторизації пристроїв. Шифрування даних відбувається з ключем, ефективна довжина якого – від 8 до 128 біт, що дозволяє встановлювати рівень стійкості результуючого. Тому варто відразу відмітити, що правильно зконфігуровані Bluetooth- пристрої самовільно з'єднуватися не можуть, тому випадкових витік важливої інформації до сторонніх осіб не буває.

Залежно від виконуваних завдань специфікація Bluetooth передбачає три режими захисту, які можуть використовуватися як окремо, так і в різних комбінаціях.

1. У першому режимі – мінімальному (який зазвичай застосовується за умовчанням) ніяких заходів для безпечного використання Bluetooth-пристрою не робиться, дані кодуються загальним ключем і можуть прийматися будь-якими пристроями без обмежень.

2. У другому режимі здійснюється захист на рівні пристроїв, тобто активуються заходи безпеки, ґрунтовані на процесах упізнання / аутентифікації (authentication) і дозволи / авторизації (authorization). У цьому режимі визначаються різні рівні довіри (trust) для кожної послуги, запропонованої пристроєм. Рівень доступу може вказуватися безпосередньо в чіпі, і відповідно до цього пристрій отримуватиме певні дані від інших пристроїв.

3. Третій режим – захист на рівні сеансу зв'язку, де дані кодуються 128-бітовими випадковими числами, що зберігаються в кожній парі пристроїв, що беруть участь в конкретному сеансі зв'язку. Цей режим вимагає упізнання і використовує кодування / шифрування даних (encryption).

Другий і третій режими часто застосовуються одночасно. Головне завдання процесу аутентифікації полягає в тому, щоб перевірити, чи дійсно пристрій, що ініціює сеанс зв'язку, є саме тим, за яке себе видає.

Служба Bluetooth- шифрування має, у свою чергу, три режими:

– режим без кодування;

– режим, де кодується тільки встановлення зв'язку з пристроями, а інформація, що передається, не кодується;

– режим, при якому кодуються усі види зв'язку.

Захисні функції Bluetooth повинні забезпечувати безпечну комунікацію на усіх рівнях зв'язку, але на практиці, незважаючи на передбачену стандартом безпеку, в цій технології є цілий ряд істотних вад.

Наприклад, слабким місцем захисту Bluetooth-пристроїв є те, що виробники прагнуть надати користувачам широкі повноваження і контроль над пристроями і їх конфігурацією. В той же час сучасна Bluetooth-технологія має недостатні засоби для упізнання користувачів (тобто система безпеки Bluetooth не бере до уваги особу або наміри користувача), що робить Bluetooth-пристрій особливо уразливими до так званих spoofing- нападів (радіодезінформації) і неправильного застосування розпізнавальних пристроїв.

Можливість використання коротких паролів, що допускається стандартом, є ще однією причиною уразливості Bluetooth-з'єднання, що, як і у випадку з використанням простих паролів системними адміністраторами комп'ютерних мереж, може привести до їх вгадування (наприклад, при автоматичному порівнянні з базою звичайних / поширених паролів). Такі паролі значно спрощують ініціалізацію, але роблять ключі зв'язку дуже простими в плані витягання з перехоплених передач [12].

3.5 HomeRF

Слід визнати, що прибічники технології HomeRF упродовж декількох років повторювали, що стандарт 802.11 не підходить для будинку і що відповідні завдання треба вирішувати саме на основі HomeRF. Як відомо, стандарт HomeRF базується на технології частотних стрибків (frequency-hopping spread spectrum, FHSS). Точка доступу і клієнтський пристрій перемикаються з однієї частоти на іншу при пересилці кожної порції даних. Якщо інтерференція чинить на сигнал негативну дію, пристрій переходить на вільну частоту. Подібна схема окрім іншого забезпечує ще і безпечнішу передачу.

Оскільки конфіденційність є головною турботою для багатьох користувачів бездротових технологій, HomeRF пообіцяв зробити технологію максимально безпечною. Перша форма безпеки в HomeRF – це 24-бітова IP-адреса мережі, специфічна для кожної персональної мережі. Ця мережева IP-адреса запобігає перехопленню і використанню пристроїв, що знаходяться за межами локальної мережі користувача, інформацією, що відправляється з видаленої персональної мережі. Візьміть як приклад багатоквартирний будинок, облаштування HomeRF з однієї системи можуть потенційно заважати роботі іншої квартири HomeRF.

HomeRF забезпечує 128-бітове шифрування, ґрунтоване на 32-бітовому векторі ініціалізації. Тут немає «відкритих» мод доступу, як в WEP, і облаштування цього стандарту не можуть передавати різнорідні пакети даних поверх MAC [13].

3.6 Алгоритми безпеки ZigBee

Система безпеки відповідно до специфікації ZigBee побудована на 128-бітовому AES алгоритмі. Передбачені специфікацією ZigBee служби безпеки визначають створення ключів, управління пристроями і захист даних.

ZigBee використовує 128-бітові ключі для реалізації механізмів безпеки. Ключ може бути асоційований або з мережею (і використовуватися рівнями ZigBee і MAC підрівнем) або з каналом зв'язку. Ключ може бути отриманий шляхом попередньої установки, угоди або передачі. Створення ключів каналу зв'язку ґрунтоване на використанні головного ключа, який контролює відповідність ключів каналу зв'язку. Первинний головний ключ має бути отриманий через безпечне середовище (передачею або попередньою установкою), оскільки безпека усієї мережі залежить від нього. Головний ключ і ключі каналів зв'язку видно тільки на рівні додатків. Різні сервіси використовують різні варіації ключа каналу зв'язку щоб уникнути витоку і ризику для безпеки.

Розподіл ключів є однією з найбільш важливих функцій безпеки мережі. У захищеній мережі призначається одно спеціальний пристрій, якому інші пристрої довіряють розподіл ключів безпеки, – центр управління (ЦУ) безпекою. У ідеалі кожен пристрій в мережі повинен мати заздалегідь завантажені адреса центру управління безпекою і первинний головний ключ. Додатки без особливих вимог до безпеки можуть використати мережевий ключ, що передається центром управління безпекою через не захищений на момент передачі канал.

Таким чином ЦУ безпекою підтримує ключ мережі і забезпечує безпеку точка-точка. Пристрої прийматимуть тільки повідомлення, зашифровані з використанням ключа, наданого центром управління безпекою, за винятком первинного головного ключа.

Архітектура безпеки розподіляється між мережевими рівнями.

1. Підрівень MAC здатний встановлювати надійний зв'язок з сусіднім пристроєм. Як правило, він використовує рівень безпеки, визначуваний верхніми рівнями.

2. Мережевий рівень управляє маршрутизацією, обробляє отримані повідомлення і може направляти запити. Вихідні фрейми використовуватимуть ключ відповідного каналу зв'язку згідно

маршрутизації, якщо він доступний; інакше для захисту корисного навантаження від зовнішніх пристроїв використовуватиметься мережевий ключ.

3. Рівень додатків встановлює ключі і робить транспортні послуги як об'єкту пристрою (ZDO), так і додаткам. Він відповідає також за поширення повідомлень про зміни в пристроях усередині мережі, які можуть виходити як від самих пристроїв (наприклад, проста зміна статусу), так і від центру управління безпекою (який може повідомити, що певний пристрій видаляється з мережі). Рівень також маршрутизує запити облаштувань центру управління безпекою і оновлення мережевого ключа від центру управління безпекою усім пристроям. Об'єкт облаштування ZDO підтримує політики безпеки пристрою.

ЦУ може періодично оновлювати ключ мережі і переходити на новий ключ. Спочатку він транслює новий ключ, зашифрований за допомогою старого ключа мережі. Потім повідомляє усі пристрої про перехід на новий ключ. Зазвичай центром управління безпекою за сумісництвом є координатор мережі, але це може бути і виділений пристрій.

ЦУ грає наступні ролі в забезпеченні безпеки:

– перевіряє достовірність пристроїв, що бажають приєднатися до мережі;

– підтримує і поширює мережеві ключі;

– забезпечує безпеку взаємодії пристроїв.

– ZigBee використовує три типи ключів для управління безпекою:

– головний ключ;

– мережевий ключ;

– ключ каналу зв'язку.

Головний ключ – цей ключ не використовується для шифрування. Він використовується, як що розділяється двома пристроями секретний код при виконанні облаштуваннями процедури генерації ключа каналу зв'язку. Головні ключі, що створюються центром управління безпекою, називаються

головними ключами центру безпеки, усі інші ключі називаються основними ключами рівня додатків.

Мережеві ключі – ці ключі забезпечують безпеку мережевого рівня. Мережевий ключ має кожен пристрій в мережі ZigBee. По бездротових каналах мережеві ключі високої безпеки повинні пересилатися тільки в зашифрованому виді. Стандартні мережеві ключі можуть пересилатися, як в зашифрованому, так і в не зашифрованому виді.

Ключі каналів зв'язку – ці ключі забезпечують безпечну одноадресну передачу повідомлень між двома пристроями на рівні додатків.

У режимі стандартної безпеки перелік пристроїв, головні ключі, ключі каналів зв'язку і мережеві ключі можна зберігати як в центрі управління безпекою, так і в самих пристроях. ЦУ безпекою, проте, відповідає за підтримку стандартного мережевого ключа і контролює політику прийому в мережу. У цьому режимі вимоги до ресурсів пам'яті центру управління безпекою набагато нижче, ніж для режиму підвищеної безпеки.

У режимі підвищеної безпеки ЦУ безпекою зберігає перелік пристроїв, головні ключі, ключі каналів зв'язку і мережеві ключі, необхідні для контролю і застосування політики оновлення мережевих ключів і доступу в мережу. У цьому режимі у міру зростання кількості пристроїв в мережі швидко зростає необхідний центру управління безпекою об'єм пам'яті [14].

4 ПРОТОКОЛИ МАРШРУТИЗАЦІЇ СЕНСОРНИХ МЕРЕЖ

Протоколи маршрутизації БСМ вирішують такі завдання, як:

– самоорганізація вузлів мережі (самоконфігурація, самовідновлення та самоконтроль);

– маршрутизація та адресація вузлів;

– мінімізація споживання енергії одиницями та продовження загального терміну експлуатації всієї мережі;

– збір та агрегація даних;

– швидкість передачі та обробки даних у мережі;

– максимальне охоплення мережі;

– якість обслуговування (QoS);

– захист від несанкціонованого доступу.

Протоколи маршрутизації для БСМ відповідають за підтримку маршрутів у мережі та повинні гарантувати надійну комунікацію навіть у важких несприятливих умовах. Багато протоколів маршрутизації, управління енергією та розповсюдження даних спеціально розроблені для BSS, де економія електроенергії є суттєвою проблемою, яку вирішує протокол. Інші були розроблені для загального використання в бездротових мережах, але вони також знайшли застосування в БСМ.

Протоколи маршрутизації БСМ можна розділити на сім категорій:

– на основі розташування вузла;

– для узагальнення даних;

– ієрархічна;

– засновані на мобільності;

– орієнтовані;

– засновані на неоднорідності;

– виходячи з якості обслуговування (QoS).

Весь набір датчиків в ієрархічних протоколах поділяється на кластери (групи, шари). Кожен кластер управляється спеціальним вузлом під назвою Master Cluster Node (MCN), який відповідає за координацію передачі та передачі даних, розпізнаних у його кластері та БС. Кластеризація може продовжити термін експлуатації колишнього бюджету [16].

Адаптивна ієрархія кластерів низької енергії (LEACH).

На початку LEACH [17] вузли організовуються в кластери, вибираючи основні вузли кластера (MCN), при цьому кожен вузол пропонується як MCN з деякою ймовірністю. Після вибору GCU, всі вузли починають надсилати розпізнані дані до свого MCN . Це створює кластери, якими керують вузли, які надсилають усі дані, розпізнані зовнішнім середовищем. Кожен MCN отримує дані, обробляє їх та надсилає до БС. LEACH іноді знову вибирає MCN на основі випадкової вибірки одиниць високої енергії. Результатом є перекласифікація, необхідна для розподілу енергії в мережі

Системи виявлення та датчиків енергозбереження (PEGASIS).

PEGASIS – це розширення протоколу LEACH, який створює сенсорні ланцюги замість кластерів у LEACH, так що кожен вузол надсилає та приймає від сусіда [18]. Однак від схеми надсилається лише один вузол для передачі даних на базову станцію. Дані агрегуються і передаються від вузла до вузла, об'єднуються і в підсумку доходять до БС.

Гібридна, енергоефективна розподілена кластеризація (HEED).

HEED розширює основну схему протоколу LEACH, використовуючи залишкову енергію та рівень чи щільність вузлів як метрику вибору кластерів для досягнення енергетичного балансу в кластерах [19, 20]. Відповідно до алгоритму, існує періодичний відбір основних вузлів кластера в HEED відповідно до комбінації двох параметрів кластера. Основним параметром є кінцева енергія кожного вузла датчика (використовується для обчислення ймовірності присвоєння статусу MCN), а другий параметр – це значення зв’язку в кластері як функція щільності кластера або рівня вузла (тобто, кількість сусідів). Базовий параметр використовується для імовірнісного

вибору першої групи основних вузлів кластера, тоді як другий параметр використовується для розриву зв'язків. Кластеризація HEED продовжує термін служби краще, ніж LEACH, оскільки останній вибирає основні вузли кластера (і, таким чином, розмір кластера), що може призвести до швидшого виходу з ладу деяких вузлів.

Поріг для енергочутливого мережевого датчика (TEEN).

TEEN – це протокол ієрархічного групування, який групує чутливі вузли в кластери, коли обраний відповідний MCN [21,22]. Він використовує кілька ієрархічних рівнів кластерів, кожен з яких має свій MCN, кожен з яких агрегує дані та відправляє MCN на більш високий рівень. На найвищому рівні MCN передають дані БС. Важливою особливістю TEEN є його придатність для застосування критичних датчиків часу. Крім того, передача повідомлень споживає більше енергії, ніж отримання даних. Однак TEEN не підходить для збору даних, коли повідомлення доводиться часто надсилати, оскільки користувач може взагалі не отримувати жодних даних, якщо пороги тригера не досягнуті.

Адаптивний періодичний поріг енергочутливого мережевого датчика (APTEEN)

APTEEN – це протокол маршрутизації на основі гібридного кластеру, який є розширеною версією TEEN. У протоколі вузли датчиків регулярно надсилають свої дані та реагують на будь-яку різку зміну значення вимірюваного параметра та повідомляють про відповідні значення їх MCN. Архітектура APTEEN така ж, як і TEEN, використовуючи концепцію ієрархічної групування для забезпечення енергоефективного зв'язку між датчиками джерела та приймачем. APTEEN включає три різні запити: історичний запит для аналізу попередніх значень даних; разовий запит на доступ до перегляду мережі; Постійні вимоги до аналізу подій протягом періоду APTEEN включають підсумок споживання енергії, ніж TEEN та більш високі значення залежних датчиків [23].

Протоколи, що передаються на мобільність, вимагають мобільності одержувача. Тут вимога до гарантованого постачальника даних, породженого джерелами датчиків, висувається мобільним БС

Joint Mobility and Routing Protocol.

У цьому протоколі сенсорні вузли, що оточують мобільний БС, внаслідок руху та зміни свого положення з часом [24]. У цьому випадку кожен вузол датчика може періодично виконувати функцію повторювача даних, що надсилаються на базову станцію. Набір для еквівалентної маршрутизації даних на всіх вузлах датчиків. У протоколі є кілька стратегій передачі БС і з'єднань, якими поле з вузлом датчика є коло: рух по концентричних колах; рухатися по колу; симетрична стратегія (трафік через межі мережі). Якщо використовується певна стратегія, остання є останньою.

Scalable Energy-Efficient Asynchronous Dissemination (SEAD).

У протоколі дані з вихідного джерела можуть бути адаптовані до різних базових станцій [25]. Протокол складається з трьох основних елементів: побудова розмножувальних дерев (d-дерев); поширення даних; підтримка мобільного системного зв'язку, що використовується. Передбачається, що датчики знають власні географічні дані. Усі джерела формують своє власне дерево розподілу даних, в якому знаходиться кореневий каталог. Усі дерева розподілу для кожного джерела даних створюються окремо.

Dynamic Proxy Tree-Based Data Dissemination.

Протокол будує дерево для кожного джерела датчика, яке з'єднує їх з декількома мобільними BS блоками [26]. Таким чином, самі датчики джерела вважаються нерухомими, але цілі є рухомими. Цільова мобільність може змінити джерело датчика, з якого БС отримує дані. Це відбувається, коли досягнуто певної граничної відстані. Тому найближчий до цілі вузол датчика може бути джерелом. Кожне джерело є джерелом проксі. Це ж стосується і БС (приймачів). Джерела та проксі-сервери є тимчасовими, тому що вони змінюються в міру зміни джерел залежно від місця розташування цілі та

способу переміщення приймачів. Проксі-сервери знижують витрати на надсилання та запит даних до джерел та проксі-серверів.

При розгляді передачі даних між датчиками джерела та приймачами існують дві парадигми маршрутизації: одна маршрутизація та кілька маршрутів маршрутизації. При одній маршрутизації кожен джерело датчика надсилає свої дані до приймача найкоротшим шляхом. У багатьох маршрутах кожне джерело датчика знаходить перші найкоротші k шляху до приймача і розподіляє навантаження рівномірно між цими стежками.

Роз'єднані шляхи.

Протокол множинної маршрутизації для маршрутизації безсполучникових датчиків, який обчислює кілька альтернативних шляхів передачі даних, що не мають нічого спільного з маршрутом головного вузла датчика [27, 28]. У маршрутизації неспоріднених датчиків найкраще доступний основний шлях, тоді як альтернативні шляхи менш бажані, оскільки у них довший час очікування. Незалежність робить ці альтернативні шляхи незалежними від мейнстріму. Отже, якщо на основному шляху відбувається збій, це залишається локальною проблемою і не зачіпає жодного з альтернативних шляхів. Приймач може визначити, який із сусідніх датчиків датчика може надати йому дані найвищої якості, тоді як останні характеризуються низькими втратами або найменш затримкою затоплення мережі. Окремі шляхи є більш гнучкими у разі виходу з ладу датчиків, але можуть бути довшими за основний шлях і, отже, менш енергоефективними.

Це протокол маршрутизації [27, 28] з декількома плетеними шляхами, що, в свою чергу, є версією протоколу Disjoint Paths з більш розслабленими правилами створення альтернативних шляхів. Різниця полягає в тому, що альтернативні шляхи можуть включати деякі вузли в основний шлях. Перш ніж створити альтернативні маршрути, слід спочатку обчислити первинний маршрут. Тому ці альтернативні шляхи іноді називають нетрадиційними.

У архітектурі різнорідної сенсорної мережі є два типи сенсорних вузлів: датчики ліній електропередач без обмеження енергії; датчики, що

працюють на батареях, які мають обмежуючий час ефект і тому повинні бути економічними з наявними джерелами енергії, мінімізують витрати на обробку та передачу даних.

Інформаційно керований запит датчика (IDSQ).

Протокол щодо економії енергії вимагає, щоб в активному стані було встановлено лише певну підмножину датчиків, оскільки в різних частинах мережі відбуваються певні події [27, 28]. Вибір підмножини активних датчиків з найбільш корисною інформацією компенсується необхідними витратами на зв'язок між цими датчиками. Корисну інформацію можна знайти на основі наближення часу та простору – де та коли можуть відбуватися події. Першим кроком протоколу IDSQ є вибір датчика як головного в кластері датчиків. Цей спікер відповідає за оптимальний вибір датчиків на основі деякої ділової інформації [29].

Маршрутизація реле кластерної головки (CHR).

Протокол передбачає формування гетерогенної мережі з використанням двох категорій датчиків: великої кількості низької якості та малої високої якості. Перші позначаються L, а другі – H. Усі датчики мають інформацію про місцезнаходження. Протокол розділяє мережу на кластери, які складаються з датчиків L на чолі з одним з датчиків H. Датчики L записують дані та надсилають один одного, використовуючи «мульти-стрибки» на деякій відстані від їхнього основного датчика в межах цього кластера, який вибирається з датчиків H. Останні передають дані на великі відстані іншим H-датчикам по дорозі до приймача [30].

5 АЛГОРИТМИ САМООРГАНІЗАЦІЇ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Самоорганізація у БСМ – це процес незалежної установки зв'язку, конфігурації та роботи бездротової мережі, який здатний регулювати його параметри та логіку роботи у відповідь на зміни зовнішніх факторів, таких як навантаження, структурні зміни, викликані зміною відмови вузла Зниження енергії з джерел живлення через помилку при передачі / отриманні повідомлень по радіо та ін. Метою самоорганізації в ССУ є створення повністю автономної мережі, яка може працювати після використання без втручання оператора.

При розробці алгоритмів самоорганізації слід враховувати різні аспекти:

– підтримка продуктивності різної кількості пристроїв у мережі (масштабованість);

– організація мереж з мінімальним споживанням енергії (енергозбереження);

– обмежена доступність BSU (обмежена обчислювальна потужність, мало оперативної пам’яті тощо).

До теперішнього часу розроблені більше 100 різних алгоритмів самоорганізації у БСМ , які можна умовно розбити на групи [31, 32].

1. Створення кластерів [33]. Цей підхід групує багато вузлів. Заголовок кластера вибирається з вузлів цієї групи. Усі вузли кластера збирають інформацію та надсилають її до заголовка кластера. Потім заголовок кластера обробляє отриману інформацію та надсилає її до вузла збору даних.

2. Створіть ланцюги зв’язку [34]. Ланцюги створюються декількома сенсорними пристроями для формування вузла, який потім відправляє зібрані дані у вузол збору даних.

3. Створіть структуру дерева [35]. Цей підхід схожий на попередній. Різниця полягає в тому, що ланцюги не створюються, а дерево прив'язується до кореневої директорії, вузол якої – збір даних.

4. Географічні підходи [36]. Географічні підходи використовують знання про положення вузлів, які визначаються, наприклад, за допомогою модулів позиціонування GPS / Glonass у пристрої. Ці дані можуть бути використані для організації вузлів у відповідній структурі.

5. Підхід із використанням неоднорідності мережевих вузлів [37]. Передбачається, що в мережі є різні типи вузлів. Один тип вузла займається лише збиранням даних, а інший тип вузла стосується лише поширення зібраних даних у мережі. У цьому випадку вузли організовуються в групи, а групи об'єднуються в ще більші групи. Це створює ієрархічну структуру груп у мережі.

Алгоритм на основі оптики – це розробка алгоритмів просторового кластеризації для самоорганізації сенсорних мереж однорангових [38]. Цей алгоритм організовує сенсорні вузли незалежно один від одного для формування кластера. Кластери створюються за допомогою процесу сортування, схожого на відомий раніше оптичний алгоритм.

Існують обмежені алгоритми групування на основі розширення пошукового кільця. Алгоритм кільця розширення характеризується переходами між раундами, починаючи з максимальної межі стрибка один [39].

У програмі Rapid ініціатор отримує бюджет B, частину якого він звільняє для себе, а решту передає своїм сусідам, надсилаючи повідомлення кожному з них [39]. Коли бюджет вичерпується, батьківський вузол отримує інформацію про всі його дочірні вузли і алгоритм закінчується. Підтвердження можна використовувати для отримання розміру та глибини дерева та максимальної кількості стрибків. Стійкий алгоритм – це поліпшення швидкого алгоритму та покращує поведінку при обмеженні розміру мережевого кластера [39].

Алгоритм платіжної схеми використовує схему платежів, використовуючи потужність передачі в якості посередника, що вимагає знання місця розташування вузлів [40]. Кожен датчик показника якості зв'язку (LQI) може обчислити мінімальну потужність, необхідну для надійної передачі даних іншим двигунам або координаторам. Можна зменшити цю потужність передачі і, таким чином, збільшити термін служби вузла, знайшовши ретранслятор, що знаходиться між цим мотоциклом та одержувачем інформації.

Алгоритм на основі біоінспірованих механізмів – це багатодисциплінарний алгоритм негативного зворотного зв'язку, заснований на передачі клітинних біологічних механізмів у мережеву взаємодію між вузлами датчиків [41]. Основна увага приділяється самоорганізації та здатності працювати з ненадійними каналами зв'язку. Цей алгоритм вирішує проблему інформування мережевих двигунів про наявні ресурси та маршрутизації для передачі керуючих повідомлень.

Алгоритм SIDA (Призначення самоорганізованого ідентифікатора) дозволяє оптимізувати обмін даними між датчиками та координатором для самоорганізації за допомогою ідентифікатора (Ідентифікація змінної довжини) [42]. Основна ідея – створити бінарне дерево, що перекривається.

Широкосмугова технологія (NSS) пропонує ряд переваг для самоорганізації в сенсорних мережах, таких як В. Простота та низька потужність передачі (енергоефективність). Використання UWB-TR знижує вимоги до тісної синхронізації та якості радіоканалів [43].

Алгоритм BOOTUP економить енергію, зменшуючи кількість повідомлень, необхідних для побудови мережі [44]. Це досягається комбінуванням фази виявлення з'єднання з фазою з'єднання з'єднання, і мережева синхронізація не потрібна.

6 АПАРАТНА РЕАЛІЗАЦІЯ СЕНСОРНОГО ВУЗЛА

6.1 Вибір радіомудуля

На сьогоднішній день багато виробників пропонують свої рішення для побудови сенсорних мереж. Розглянемо декілька з таких модулей.

Порівняємо декілька найбільш використовуємих радіомодулей NRF24l01, ESP8266 та loraRN2483.

Для початку порівняняємо затухання сигналу у приміщенні та на відкритому просторі радіомодуля NRF24l01 (рисунок 6.1).

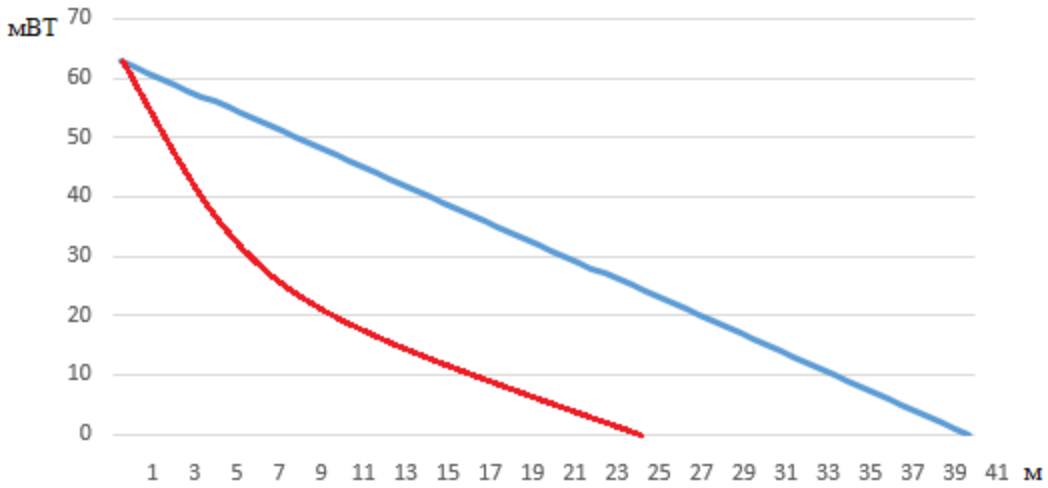

Рисунок 6.1 – Порівняння затухання потужності сигнала у NRF24l01

З графіку можна побачити, що на відкритій місцевості сигнал затухає прямолінійно (синій графік). У приміщенні більш сильне затухання сигналу, та радіус дальності сигнала падає з 40 до 24 метрів (червоний графік).

Наступним розглянемо ESP8266, це модуль на базі якого зроблено багато пристроїв для обслуговування різних датчиків, використовується в побудові систем розумного дому. Порівняння затухання потужності сигнала у ESP8266 на рисунку 6.2.

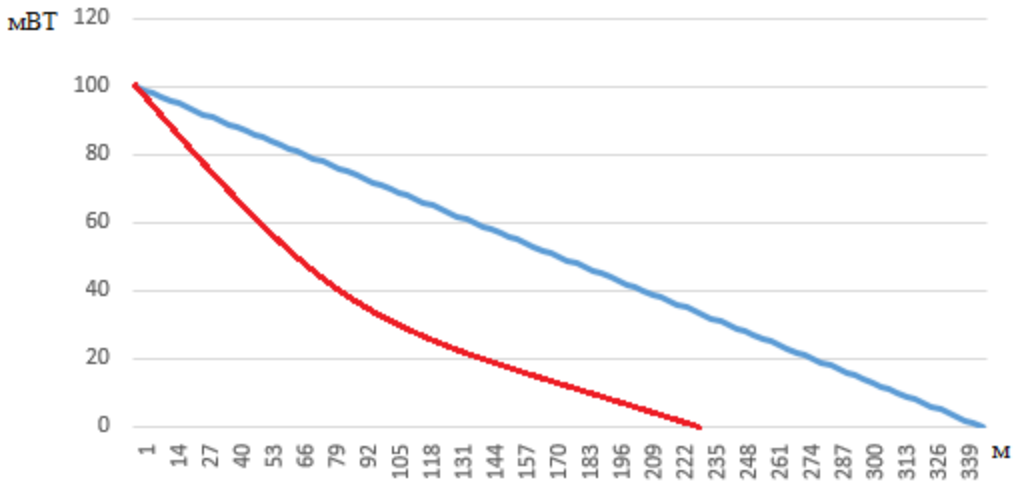

Рисунок 6.2 – Порівняння затухання потужності сигнала у ESP8266

З графіку приведеного на рисунку 8.2 можна зробити висновок, що потужність радіомодуля більше ніж у NRF24l01, завдяки цьому збільшується і відстань зв'язку, навіть у приміщенні.

Далі проаналізуємо модуль LORA RN2483. Він має велику потужність до 1,5Вт при максимальній напрузі (рисунок 6.3).

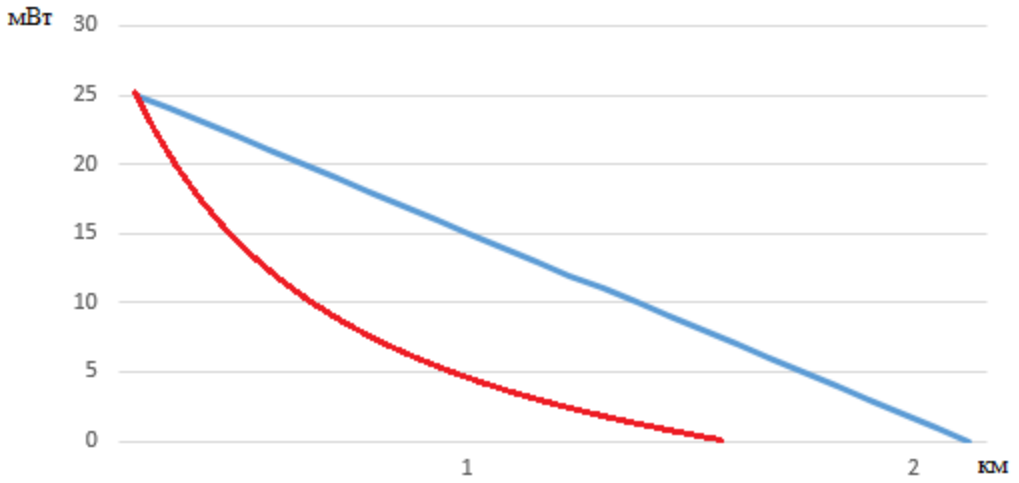

Рисунок 6.3 – Порівняння затухання потужності сигнала у LORA RN2483

Під час тестування було виявлено, що при заявленій від виробника максимальній дальності до 15 км не є достовірною, на справді дальність при прямій видимості сягнула трохи більше ніж 2 км, а в приміщенні 1.6 км.

Порівняємо струм споживання модулей, що розглядаються. Максимальний струм поживання у NRF24l01 складає 12,3мА. В той же самий час ESP8266 має максимальний струм живлення до 160мА. Але для LORA RN2483 він складає 14,2 мА. Показники максимального струму живлення для радіомодулей на рисунку 6.4.

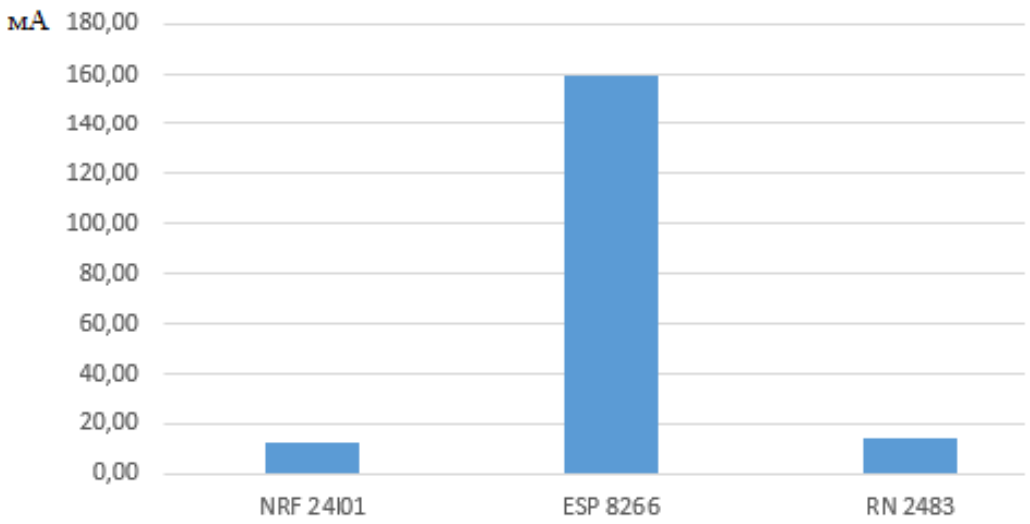

Рисунок 6.4 – Показники максимального струму живлення для радіомодулей

Важливим параметром для радіомодулей являється поживання струму у сплячему режимі. У NRF 24l01 цей режим зовсім відсутній, у ESP8266 споживання до 10мкА, в той час, коли у LORA RN2483 споживання току у сплячему режимі складає всього 1,8 мкА. Порівняльний графік приведено на рисунку 6.5.

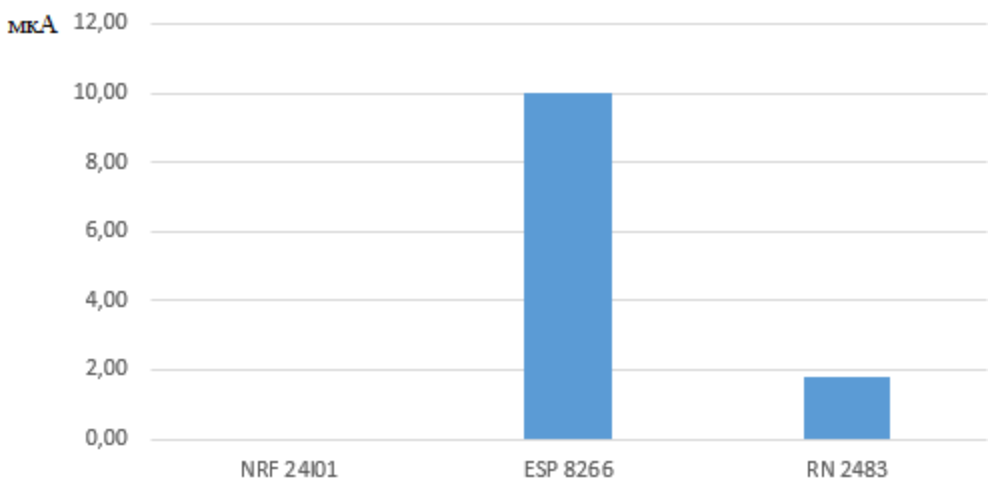

Рисунок 6.5 – Порівняння струму живлення у сплячему режимі

Важливо зазначити, що модуль NRF 24l01 не підтримує жодних допоміжних технологій (такі, як Wi-Fi, Bluetooth та інші). В той час коли ESP8266 підтримує весь стек протоколів стандартів WiFi 802.11n і BT4.2, забезпечуючи даний функціонал через інтерфейси SPI / SDIO або I²C / UART. Та Wi-Fi безпеку: WEP, WPA, WPA2, WAPI. В той же самий час LORA RN2483 має свій стек протоколів LORAWAN.

З приведоного вище аналізу було обрано модуль LORA RN2483, так як вона має декілька значних переваг. LORA RN2483 має значно більший радіус зв'язку, що дозволяє не використовувати проміжні передатчики у випадках, коли вузли стоять дуже далеко. Наявність сплячого режиму дуже важливо, що допоможе скоротити витрати на енергоживлення, тут знов LORA RN2483 стає найбільш підходящим радіомодулем.

Для реалізації сенсорної мережі було обрано модуль loraRN2483, у якості радіомодуля, зі своїм стандартом LoRa та технологією LoRaWAN. Фізичний вигляд модуля lora RN2483 на рисунку 6.6.

Рисунок 6.6 – Фізичний вигляд модуля lora RN2483 з обв'язкою

Це технологія зв'язку на великі (Long Range) відстані, запатентована компанією Semtech, і реалізована в їх чіпах SX1272 та SX1276. LoRa це протокол низького рівня, поверх якого можуть реалізовуватися більш високорівневі протоколи, наприклад LoRaWAN.

Особливість стандарту LoRa – це передача невеликих пакетів даних з невисоким енергоспоживанням. За запевненням виробника, дальність на відкритому повітрі може досягати 10 км, а час роботи від батареї може становити від п'яти до семи років. У той час як інші технології бездротового зв'язку, такі як Bluetooth і BLE (а в деякій мірі Wi-Fi і ZigBee), неможливо встановити для передачі даних на великі відстані, Low-power Wide-area Network (LPWAN), навпаки, забезпечує обмін невеликими обсягами даних на значній дистанції. Робочі частоти залежать від країни, і складають 433 або 868МГц (EU-версія) або 915МГц (USA-версія).

Для розробки були обрані модулі RN2483. Вони доволі прості в програмуванні і підтримують різні режими роботи. RN2483 містить чіп SX1276 і контролер в одному корпусі, управляється командами UART, що дозволяє підключити його до будь-якого пристрою (ПК, Arduino, мікроконтролер, тощо).

Для обробки даних на вузлу було використано Stm32f103. Фізичний вигляд плати наведено на рисунку 6.7.

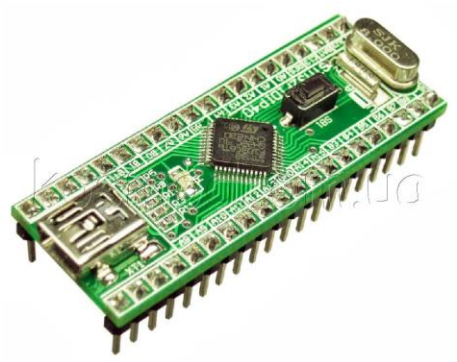

Рисунок 6.7 – Фізичний вигляд плати на базі STM32F103 з обв’язкою

STM32F103 молодша лінійка мікроконтролерів компанії STMicroelectronics на базі ядра Cortex-M3. Мікроконтролери включають в себе широкий набір інтерфейсів і великий об'єм вбудованої пам'яті: ядро Cortex-M3 з частотою процесора до 24 МГц, Flash до 512 кБ, до 32 кБ RAM, більшу кількість таймерів, годинник реального часу (RTC), до 5 UART, до 2 I2C, до 3 SPI, 12-бітний АЦП і 12-бітний ЦАП, вбудований температурний датчик, а так же контролер зовнішньої пам'яті (EMC). Випускаються в корпусах: LQFP48, LQFP64, TFBGA64, LQFP100, LQFP144.

Для отримання інформації від різноманітних об’єктів можуть бути використані різні датчики, сенсори або мікроелектромеханічні системи, а також їх поєднання. Нижче на рисунку 6.8 наведено схематичний вигляд вузла.

Рисунок 6.8 – Модель вузла сенсорної мережі

Для тестування сенсорної мережі та отримання достовірних даних було вибрано наступний датчик. DS18B20 – це цифровий вимірювач температури, з дозволом перетворення 9 – 12 розрядів і функцією тривожного сигналу контролю за температурою. Параметри контролю можуть бути задані користувачем і збережені в енергонезалежній пам’яті датчика (вигляд датчика приведено на рисунку 6.9).

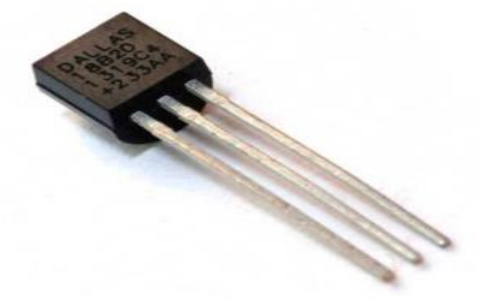

Рисунок 6.9 – температурний датчик DS18B20

Діапазон вимірювання температури становить від -55 до +125 ° C. Для діапазону від -10 до +85 ° C похибка не перевищує 0,5 ° C.

У кожної мікросхеми DS18B20 є унікальний серійний код довжиною 64 розряду, який дозволяє декільком датчикам підключатися на одну загальну лінію зв'язку. Тобто через один порт мікроконтролера можна обмінюватися даними з декількома датчиками, розподіленими на значній відстані. Режим вкрай зручний для використання в системах екологічного контролю, моніторингу температури в будівлях, вузлах устаткування.

Система з шиною 1-Wire складається з одного ведучого пристрою, яке управляє одним або декількома відомими пристроями.

7 ПРОГРАМНА РЕАЛІЗАЦІЯ

7.1 Опис алгоритму

При початковій синхронізації серверна сторона відкрита на прийом, кожен датчик повідомляє свій випадково сгенерований ID і до якого типу пристроїв воно відноситься (датчик температури, пристрій введення-виведення, датчик руху). Після чого на сервері створюється список з пристроїв, цей список має такі поля:

– ID пристроя;

– тип пристроя;

– пріоритет пристроя;

– граничні значення на пристрої.

Потім будується початкова таблиця маршрутизації. Потік даних при першій синхронізації на рисунку 7.1.

Рисунок 7.1 – Потік даних при першій синхронізації

Після того, як буде відомо про усі пристрої у системі, оператор присвоює пріоритет до кожного пристрою та граничні значення для кожного пристрою. За для швидкого реагування під час обробки критичної інформації. Після присвоєння пріоритету, на датчики передається наступний потік даних. Потік даних на вузол при першій синхронізації на рисунку 7.2.

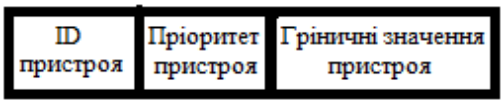

Рисунок 7.2 – Потік даних на вузол при першій синхронізації

Після того, як вузол отримав данні для роботи він починає отримувати та обробляти данні з датчика. Якщо данні в допустових межах, тоді данні передаються до сервера і заносяться до таблиці. Але, якщо данні виходять з межі допустових значень, то починається аналіз критичного значення. Перевіряється, пріоритет датчика, якщо він дорівнюється 0, тоді це означає що це датчик з назвищем пріоритетом і після надходження інформації з нього реагування буде найшвидше. Але, якщо інший пріоритет тоді вираховується коефіцієнт важливості проблеми, та також передається на сервер, формується черга і приймається рішення. Алгоритм обробки інформації на вузлі на рисунку 7.3.

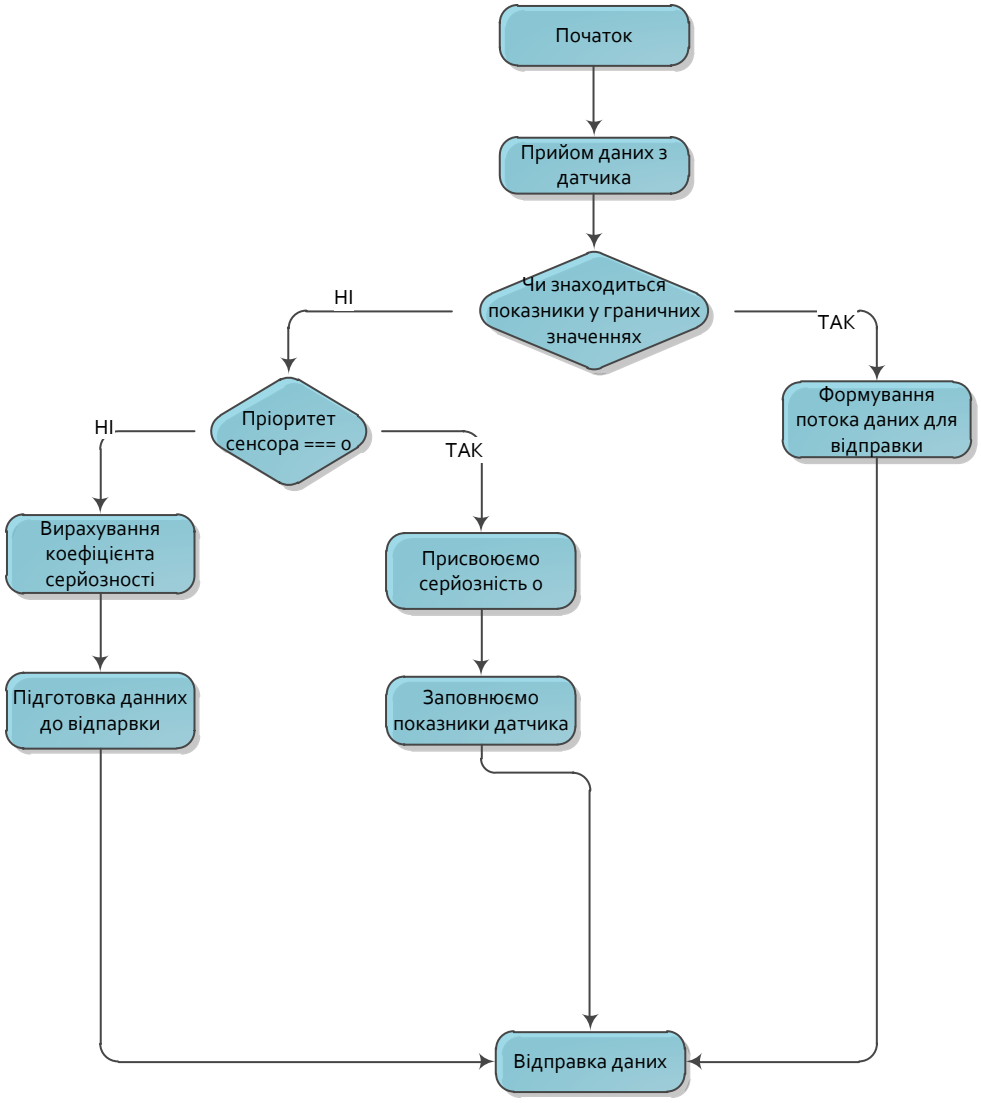

Рисунок 7.3 – Алгоритм обробки інформації на вузлі

Ініціалізація радіомодулю здійснюється на етапі ініціалізації пристрою, де задається йому необхідний режим роботи: обирається потрібну швидкість передачі даних, діапазон та частоту роботи, а також параметри вбудованого протоколу (рисунки 7.4, 7.5).

```
157  int32_t protoPollSensors(void) {
158      int64_t sensorValue;
159      SensorMessage msg;
160
161      for (uint32_t idx=0; idx<sensorsNumber; idx++) {
162          SensorItem sensor = deviceSensorList[idx];
163
164          // Отримуємо дані з сенсора
165          sensorValue = sensor.handler();
166
167          if (!isInRange(sensorValue, sensor.setup.range)) {
168              // перевіряємо діапазон значення сенсора
169              if (sensor.setup.priority == 0) {
170                  msg.importance = 0;
171                  msg.msg = getImportanceMessage(sensor.setup.id, sensorValue);
172              } else {
173                  msg.importance = calcImportance(sensor.setup.priority, sensorValue, sensor.setup.range);
174              }
175          }
176
177          msg.id = sensor.setup.id;
178          msg.value = sensorValue;
179
180          pushPriorityQueue(sensor.setup.priority, msg);
181      }
182
183      return 0;
184  }
```

Рисунок 7.4 – Лістінг реалізації алгоритму обробки інформації на вузлі

```
23  int32_t protoInit() {
24      // Configure LoRa module
25      loraConfigStruct loraConfig;
26
27      loraConfig.frequency    = sx1276_7_8FreqTbl;
28      loraConfig.txPower      = PWR_11DBM;
29      loraConfig.bandWidth    = BW_500KHZ;
30      loraConfig.codingRate   = CR_4_5;
31      loraConfig.headerType   = IMP_HEADER;
32      loraConfig.spreadFactor = SF_RATE_12;
33      loraConfig.crcEnable    = CRC_EN;
34      sx1276_7_8_Config(&loraConfig);
35
36      return 0;
37  }
```

Рисунок 7.5 – Лістінг ініціалізації радіомодулю

Критична інформація – це інформація с датчиків, що виходить за межі граничних значень, та потребує скорішої обробки на серверній стороні. При підготовці передачі критичної інформації розраховується важливість цих даних.

$$Ser = abs * (data / priority) \quad (7.1)$$

де Ser – це важливість даних;

data – данні з датчика;

priority – пріоритет датчика.

Якщо Priority дорівнює 0, це значить що інформація повинна бути негайно передана та оброблена. Потік даних при передачі критичної інформації на рисунку 7.6.

Рисунок 7.6 – Потік даних при передачі критичної інформації

При надходженні критичної інформації на серверній стороні починає працювати наступний алгоритм.

Після того, як прийшла інформація, яка потребує найскорішої обробки в першу чергу оператора сповіщають, про надходження такої інформації. Після чого проходить оцінка важливості інформації. Якщо, інформація, що тільки надійшла єдина із критичною, то вона становиться в першу чергу виконання, якщо вже є критична інформація, то порівнюються коефіцієнти важливості, та проблема з вищим коефіцієнтом становиться на перше місце, з меншим перемішується на нижчу позицію, якщо коефіцієнт буде дорівнюватися 0 у такому випадку буде негайно сповіщено про проблему. Коли прийшла черга до інформації, то треба вирішити, чи можна самостійно

вирішити проблему, або потрібне рішення оператора. У випадку якщо система може самостійно вирішити проблему, вона сповіщає про спосіб вирішення, після чого приймаються дії. У варіанті, якщо система не в змозі вирішити проблему самостійно, то вона віддає керування оператору, який приймає рішення, та усуває проблему. У будь-якому випадку, після усунення проблеми відбувається журнулювання критичної події.

При журнулюванні подій заповнюються наступні поля:

– ID події;

– дата, коли була зафіксована подія;

– ID пристроя;

– тип пристроя;

– короткий опис події (підвищення/зниження тиску, відсутність освітлення тощо);

– дії, які були використані для вирішення проблеми.

У повторних випадках виникнення подібної проблеми, може бути використаний журнал подій, задля вирішення подібної проблеми.

Формування пріоритету на рисунку 7.7.

Пріоритет формується за допомогою простих чисел від 0 до n. Де 0 датчик з найважливішими даними. Та буде стояти вище у списку задач на серверній стороні та інформація буде оброблена скоріше, ніж у датчиків з нижчим пріоритетом.

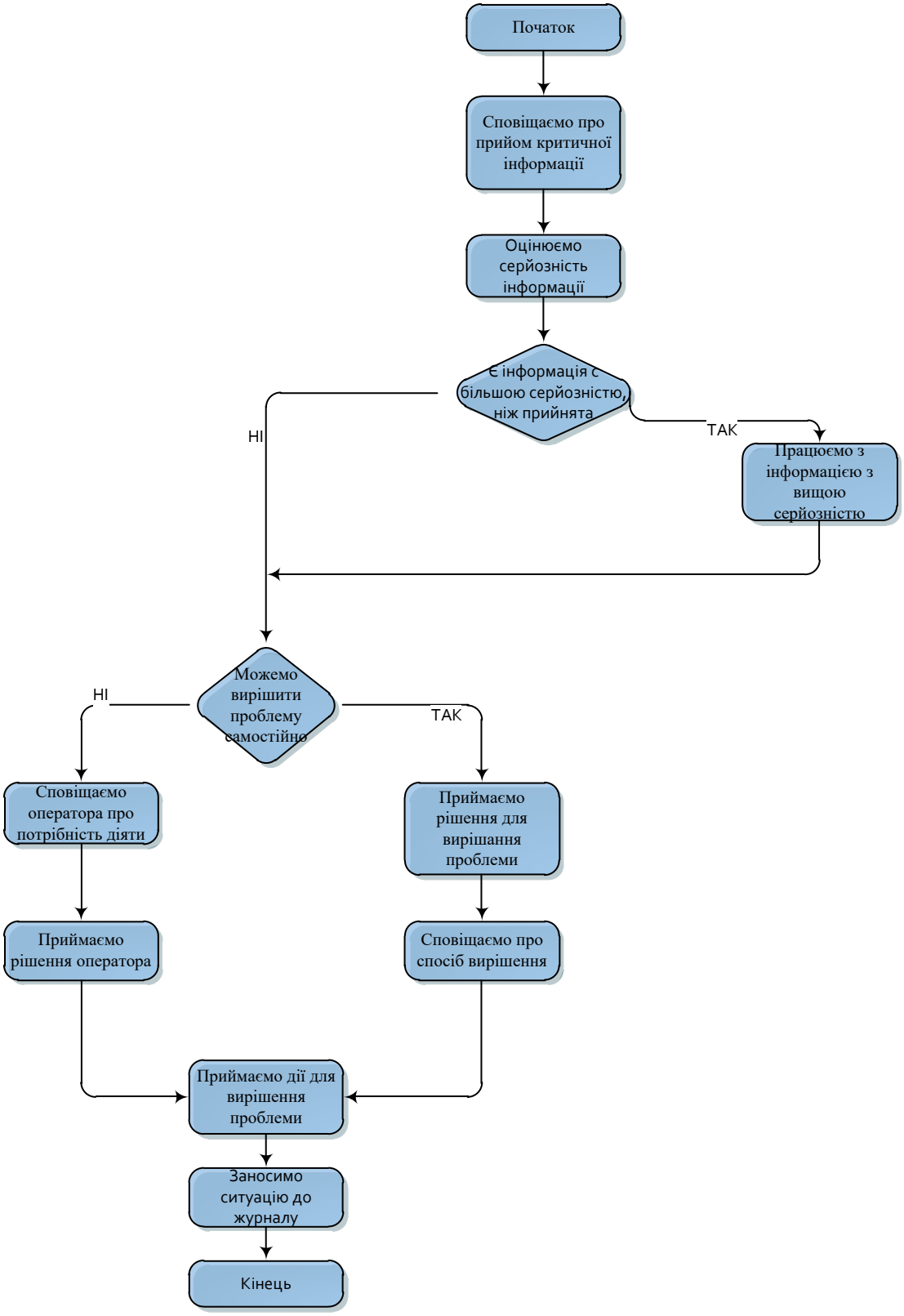

Рисунок 7.7 – Формування пріоритету

7.2 Черга оброблення інформації

Черга обробки даних формується за декількома параметрами – це час надходження інформації, пріоритет інформації, важливості інформації. Після того, як інформація була прийнята, робиться перевірка і вирішується до якого типу належить інформація, чи потребую вона моментальної обробки. Якщо ні, тоді інформація записується згідно до свого пріоритету, якщо однакові пріоритети, то обробляється спочатку та інформація, яка прийшла раніше.

Якщо при перевірки інформації, що надійшла, є поле важливості, то це означає, що є відхил в роботі системи. І тоді ця інформація становиться на вище місце, згідно зі своєю важливістю. Алгоритм побудови черги наведений на рисунку 7.8.

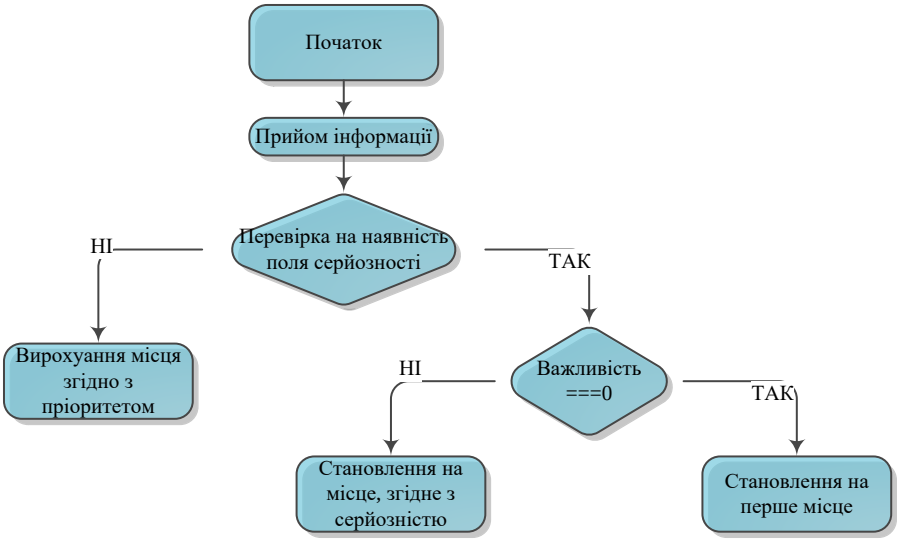

Рисунок 7.8. – Алгоритм побудови черги

Для відправки даних використовується пріоритетна черга, реалізація якої представлена на рисунку нижче. Згідно запропонованого алгоритму, критичні данні повинні бути у пріоритеті. Тому вони будуть відправлені у першочергово. Дана реалізація використовує циклічний буфер для

збереження повідомлень у черзі – це не створює додаткове навантаження при обчисленні (рисунок 7.9).

```
53  // Приоритетные очереди для отправки по протоколу
54  #define MSG_QUEUE_NUMBER 3
55  #define MSG_QUEUE_SIZE 8
56  SensorMessage msgQueue[MSG_QUEUE_NUMBER][MSG_QUEUE_SIZE];
57  uint32_t msgQueueRdIdx[MSG_QUEUE_NUMBER] = {0, 0, 0}; // индекс ячейки для считывания
58  uint32_t msgQueueWrIdx[MSG_QUEUE_NUMBER] = {0, 0, 0}; // игдекс ячейки на запись
59
60
61  uint32_t getPriorityQueueSize(uint32_t priority) {···
77  }
78
79  int32_t pushPriorityQueue(uint32_t priority, SensorMessage msg) {
80      if (priority >= MSG_QUEUE_NUMBER) {
81          return -1;
82      }
83
84      uint32_t idx = msgQueueWrIdx[priority];
85
86      msgQueue[priority][idx];
87      msgQueueWrIdx[priority] = (idx + 1) % MSG_QUEUE_SIZE;
88
89      return 0;
90  }
91
92  int32_t popPriorityQueue(uint32_t priority, SensorMessage * msg) {···
107 }
```

Рисунок 7.9 – Лістинг реалізації пріоритетної черги

Для відправки використовується пріоритетна черга, алгоритм якої показано у лістінгу на рисунку 7.10. Дана реалізація послідовно відправляє повідомлення, починаючи з більш пріоритетних.

```
188 int32_t protoSenderHandler(void) {
189     SensorMessage msg;
190
191     for (uint32_t prio = 0; prio < MSG_QUEUE_NUMBER; prio++) {
192         while (popPriorityQueue(prio, &msg) == 0) {
193             transmitPacket((uint8_t *) &msg, sizeof(msg));
194         }
195     }
196
197     return 0;
198 }
199
200
```

Рисунок 7.10 – Лістинг реалізації відправки повідомлень за пріоритетом

При надходженні інформації з датчиків, на серверній стороні виконується алгоритм, оцінки інформації. Після прийому впершу чергу з'ясовується, чи є інформація критичною, чи потрібна їй негайна обробка. Якщо ні, та показники датчиків не вийшли за граничні значення, то інформація вноситься до показників відповідного сенсора. Алгоритм оброблення прийнятої інформації рисунок 7.11.

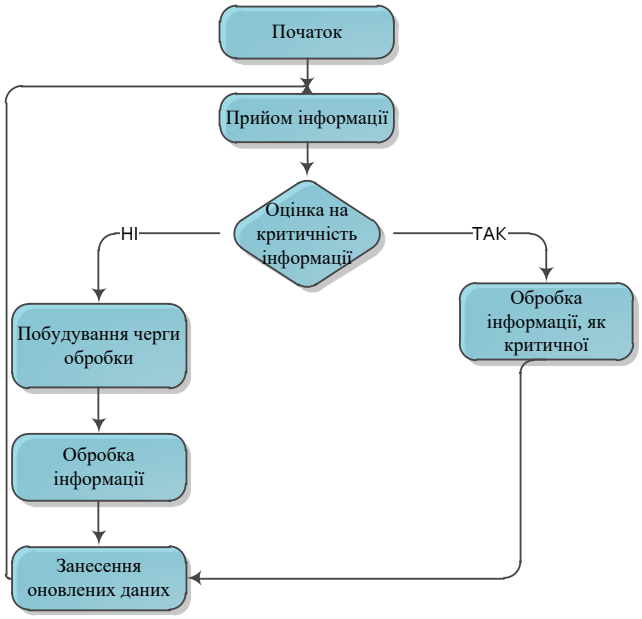

Рисунок 7.11 – Алгоритм оброблення прийнятої інформації

На першому етапі будується таблиця маршрутизації на основі метрики, тобто якісної або кількісної оцінки маршрутів. Оцінка маршруту визначається умовами, в яких працює мережа. Якщо відомо, що в середовищі діють потужні перешкоди, то слід використовувати якісну оцінку, в іншому випадку кількісну. Мережа починає працювати відповідно до наявної таблицею маршрутизації, яка в свою чергу, доповнюється значенням ваги для кожного маршруту. Спочатку всі маршрути мають однакову вагу. Далі з кожним успішно доставленим пакетом відповідному маршруту присвоюється нове значення ваги – більше ніж попередньому. У разі не підтвердження доставки пакета або доставки його з помилками, відповідним маршрутом

присвоюється менше значення ваги, ніж попереднє. Через деякий час Тгр вагові коефіцієнти стають більш пріоритетними, ніж метрика (якісна або кількісна оцінка) і оптимальним вважається той маршрут, у якого більша вага. Таким чином, БСМ пристосовується до змін зовнішнього середовища. Алгоритм маршрутизації рисунок 7.12.

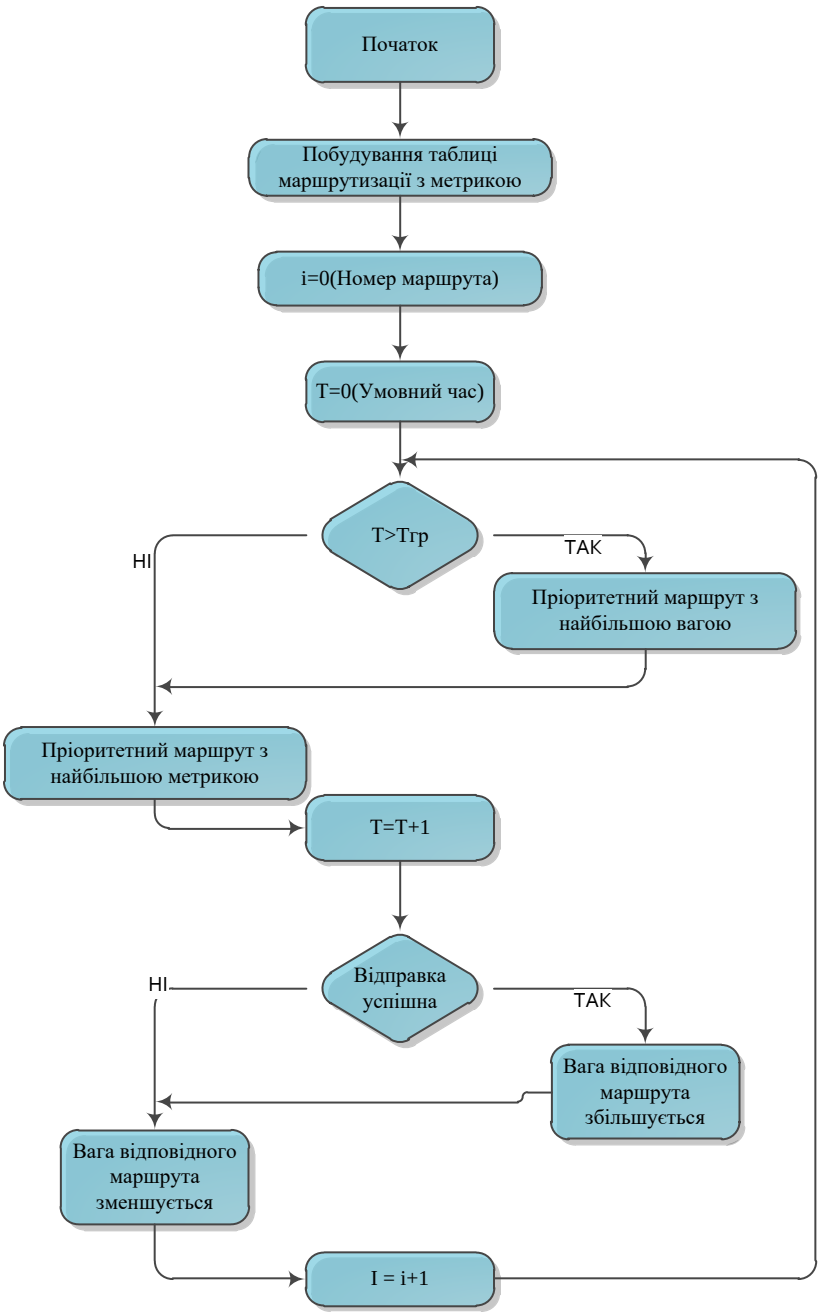

Рисунок 7.12 – Алгоритм маршрутизації

Запропонований алгоритм має такі переваги. Найбільш значиме це те що маршрути завжди вдосконалюються, знаходиться найбільш досконалий маршрут і після цього інформація буде передаватися по цьому маршруту. Також цей алгоритм на початку життя мережі використовує дві метрики для оцінки та побудови маршрутів, згідно до цих метрик можна побудувати найбільш оптимальний маршрут, після чого ці маршрути будуть порівняні між собою і будуть визначені коефіцієнти, за допомогою яких буде зрозуміло, який маршрут буде більш якісний.

8 ТЕСТУВАННЯ МЕРЕЖІ НА БАЗІ ЗАПРОПОНОВАНОГО АЛГОРИТМУ

Тестування проводилося на фізичному макеті, який складався з двох вузлів. Зв'язок був налагоджений по радіоканалу на частоті 868МГц, та було узгоджене підключення типу «точка-точка». Також було використано програмний продукт TOSSIMO, який був використаний у якості середи моделювання сенсорної мережі.

Сенсорні вузли випадково розміщенні на площині. Число вузлів сенсорної мережі сягає 50 пристрів. Усі вузли знаходяться на відстані, яка дозволяє зв'язуватися з сервером у режимі прямої передачі (рисунок 8.1).

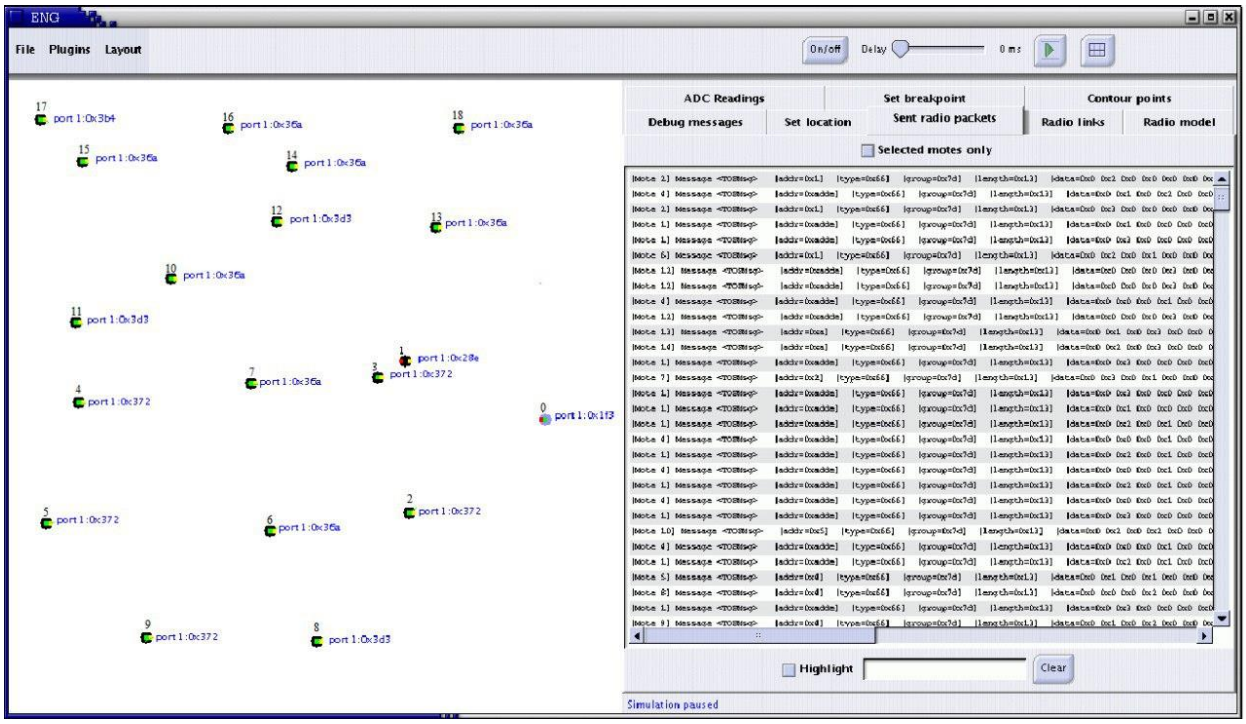

Рисунок 8.1 – Випадкове розміщення вузлів на площіні

При використанні алгоритму з прямою передачею сенсорний вузол передає данні саме на сервер, незважаючи на відстань від вузла управління. На початку життя сенсорної мережі, можна побачити, що усі вузли спілкуються з серверною частиною (рисунок 8.2).

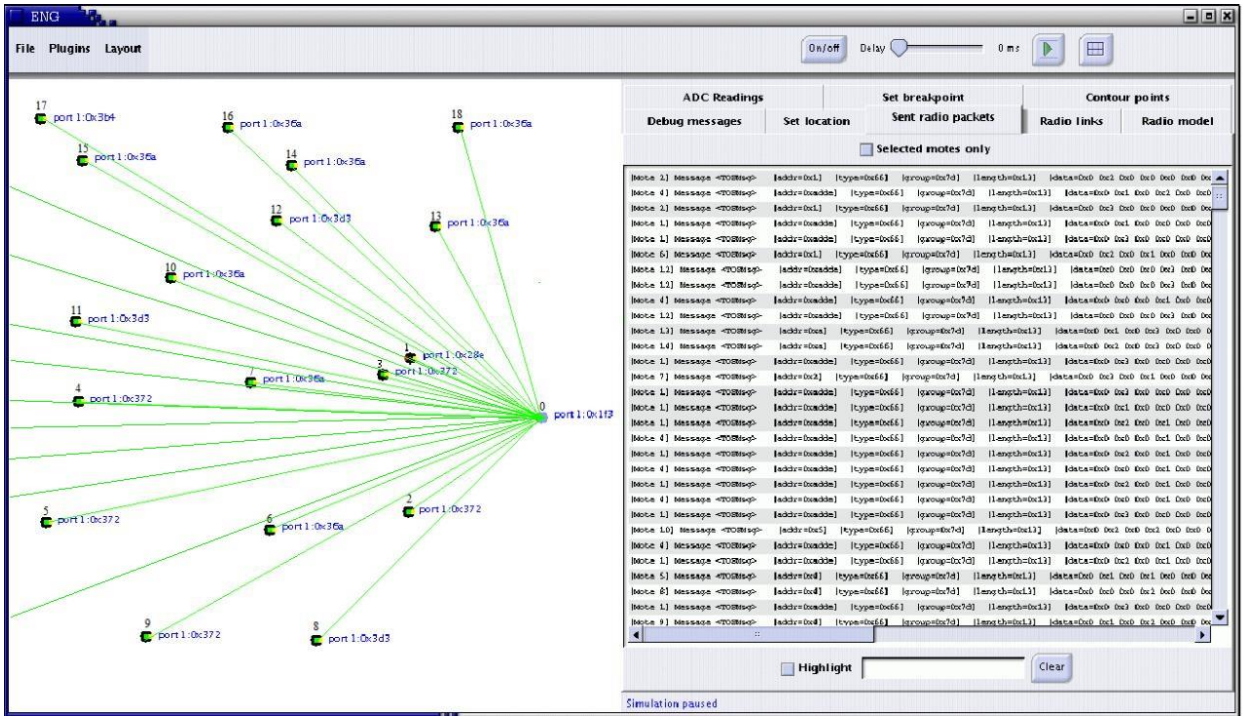

Рисунок 8.2 – Зв’язок вузла з сервером на перших раундах

Але через 130 раундів можна побачити, що вузли, які знаходяться на значній відстані перестають зв’язуватися з сервером. Через це можно зробити висновок, що такий алгоритм може бути застосований тільки для мереж дуже не великого розміру до десяти датчиків, які розташовані на рівній віддаленесті від сервера, щоб не було ситуацій, як в нашому експеременті. Зв’язок вузла з сервером після 130 раундів на рисунку 8.3.

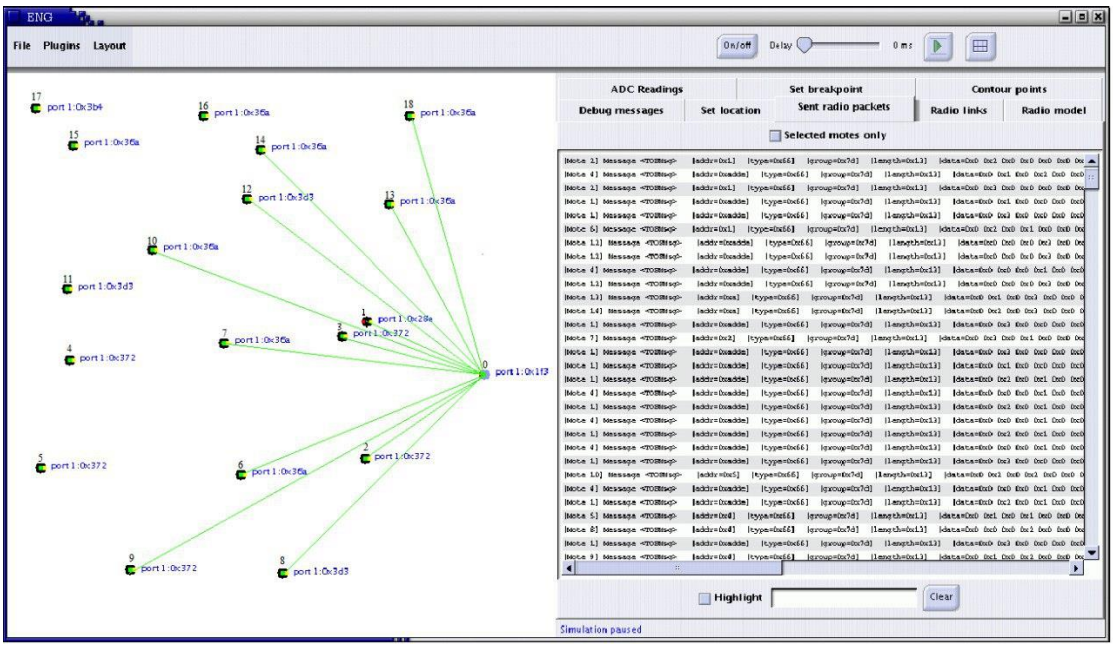

Рисунок 8.3 – Зв’язок вузла з сервером після 130 раундів

Проводимо той же експеремент, але з використанням розробленого алгоритма. Можна побачити, що на першомо етапі будується доволі багато маршрутів (рисунок 8.4).

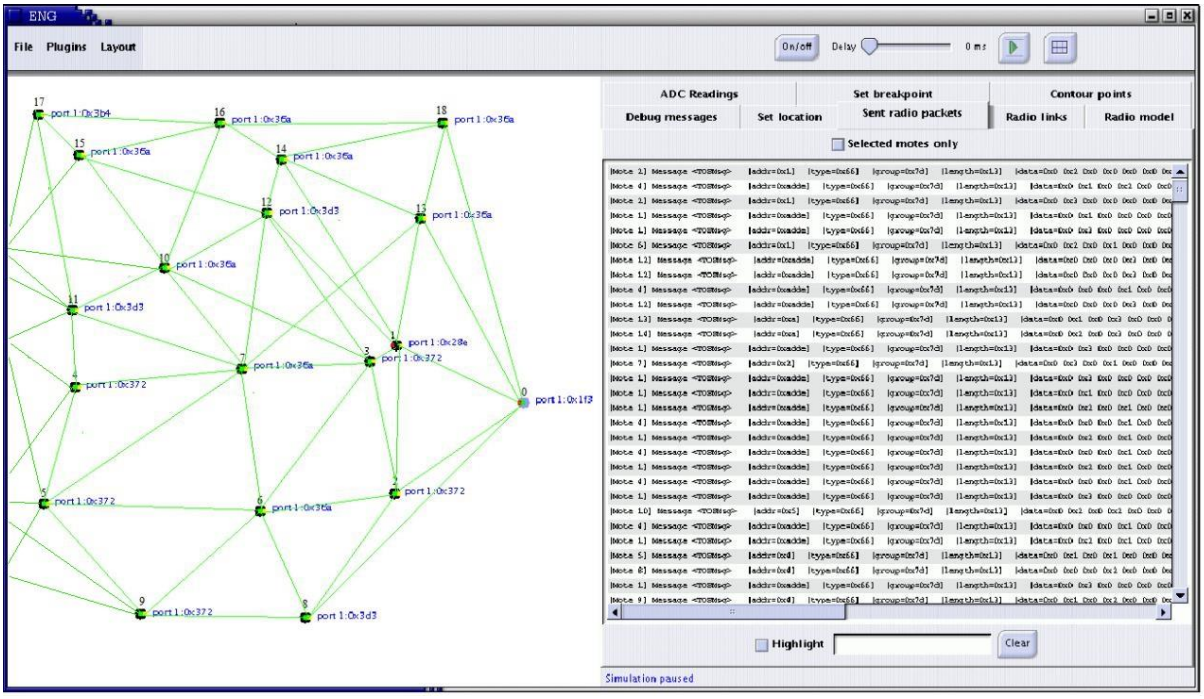

Рисунок 8.4 – Передача інформації з вузла на сервер на перших раундах

Але після 40 раундів, цих маршрутів стає менше, це є особливість даного алгоритму. За увесь час життя мережі маршрути зв'язку постійно удосконалюються, щоб прискорити передачу даних та зменшити відстань. Передача інформації з вузла на сервер після 40 раундів на рисунку 8.5.

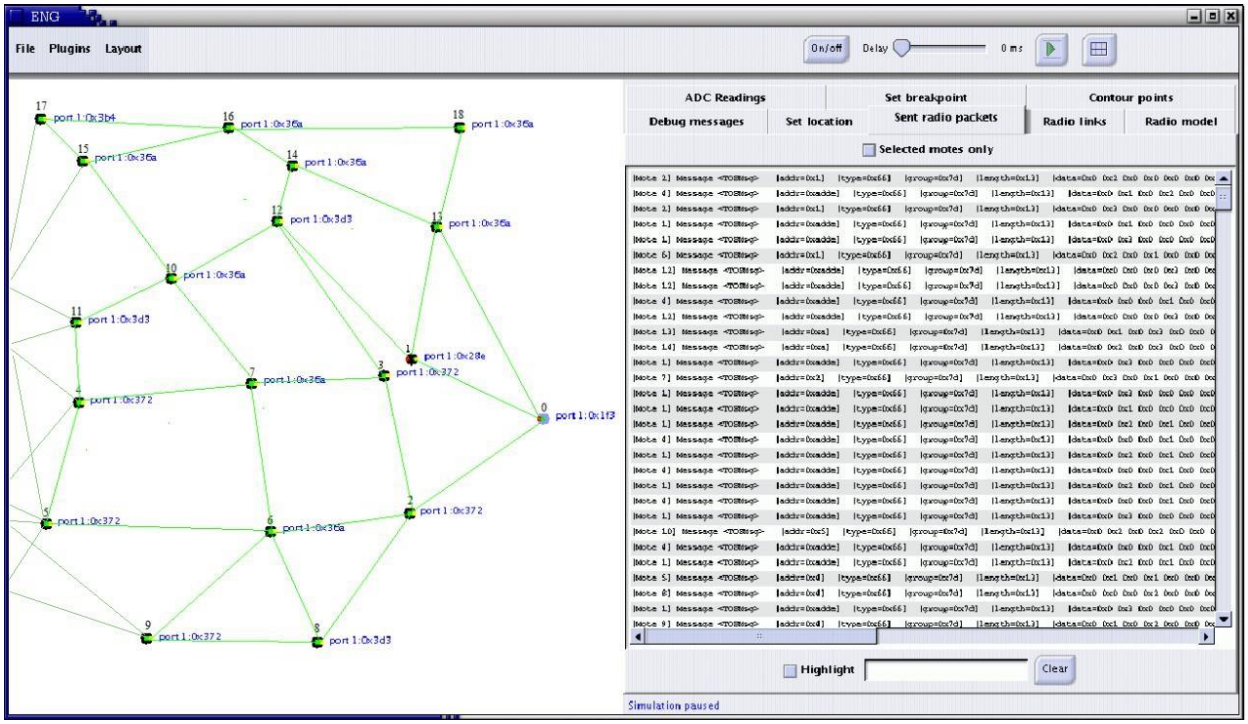

Рисунок 8.5 – Передача інформації з вузла на сервер після 40 раундів

Після 130 раундів. Маршрутів стало ще менше, і залишились найбільш перспективні. У випадку, коли датчики переміщуються маршрути не залишаються ті ж самі, вони теж перебудовуються. Передача інформації з вузла на сервер після 130 раундів на рисунку 8.6.

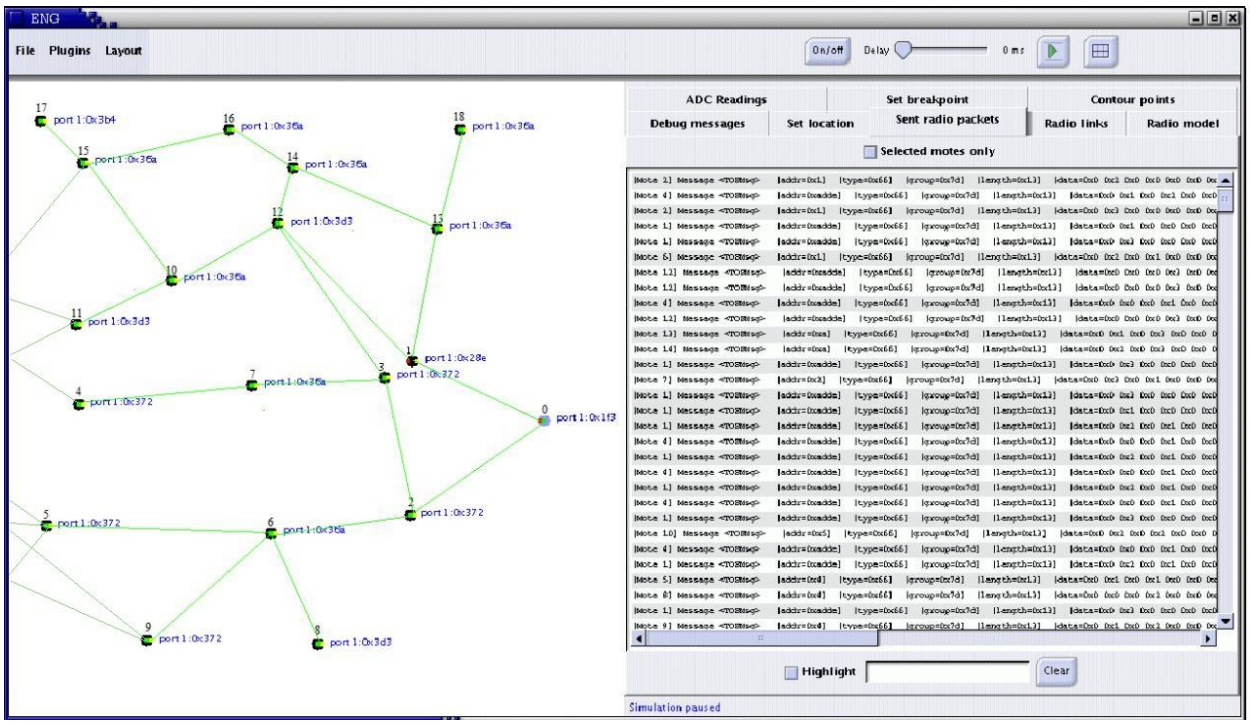

Рисунок 8.6 – Передача інформації з вузла на сервер після 130 раундів

При використанні запропонованого алгоритму мережа залишається маштабованою, та може змінюватися і при цих змінах мережа залишається життєздатною через великий час роботи. В поєднані з технологією LoRa збільшується радіус зв'язку на вузлах.

ВИСНОВКИ

У роботі розглянуті принципи роботи бездротової мереж Ad-Hoc. Розглянута інфраструктура роботи та побудови цих мереж, режими роботи та стандарт за яким працюють ці мережі. Виявленні особливості їх функціювання та розглянуті умови успішної побудови мережі в режимі Ad-Hoc, виявленні базові технології для побудування мере Ad-Hoc. Знайдені основні переваги та недоліки.

Був детально розглянуто вузол сенсорної мережі, з чого він складається, його функції та умови їх успішного функціювання. Розділені підсистеми апаратної частини вузла – це комунікаційна підсистема, обчислювальна підсистема, сенсорна підсистема, підсистема електроживлення. Були виявленні критерії, яким повинні відповідати сенсорні вузли.

Була розглянута типова архітектура та типи вузлів – це координатор, маршрутизатор, кінцевий вузол. Розглянуті основні функції кожного із типів вузлів.

Також були освітленні питання щодо стандартів, які використовуються при побудові сенсорних мереж. Такі як Wi-Fi, WiMAX, Bluetooth, HomeRF, ZigBee. Та наведена таблиця порівняння цих технологій. Було розглянуто питання, стосовно реалізації безпеки при використанні цих стандартів.

Оглянуті основні протоколи маршрутизації, які використовуються в сенсорних мережах. Виявленні завдання, які вони повинні вирішувати. Детально розглянуті ієрархічні протоколи, протоколи, ґрунтовані на мобільності, багатомаршрутизовані протоколи, протоколи гетерогенності.

Було проведено огляд на існуючі протоколи алгоритмів самоорганізації. Після чого був проведено аналіз апаратних засобів за допомогою яких можна пообдувати сенсорну мережу, після порівняння затухання сигналів у приміщенні і на відкритому просторі були побудовані

порівняльні графіки, за допомогою яких було виявлено, який з радіомодулей є найбільш оптимальний та перспективний. Після чого були розроблені алгоритми, як для обробки інформації на вузлах так і обробки інформації на серверній стороні. Та програмно реалізовано ці алгоритми. Наступним кроком було проведення тестування.

Тестування проводилося як на фізичних пристроях, та у програмі для моделювання сенсорної мережі. В результаті тестування були виявленні переваги запропонованого алгоритму перед прямим підключенням датчиків до управляючого модуля. Тестування підтвердило, що мережа життєздатна, масштабована та може навчатися.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ad-hoc Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.cfm.

2. Ad Hoc Networks [Електронний ресурс] – Режим доступу до ресурсу: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/index.html

3. Самоорганизующиеся (ad hoc) сети. Что это и зачем это нужно? [Електронний ресурс] – Режим доступу до ресурсу: http://wireless09.livejournal.com/334.html.

4. Пролетарский А. В. Беспроводные сети Wi-Fi / А. В. Пролетарский, И. В. Баскаков, Д. Н. Чирков – Москва: БИНОМ. Лаборатория знаний, 2007. – 178 с.

5. Fernandez, E.B. & VanHilst, M., Chapter 10, WiMAX Standards and Security (Edited by M. Ilyas & S. Ahson) [Електронний ресурс] – June 2007. Режим доступу до ресурсу: http://www.crcpress.com.

6. Технология Bluetooth [Електронний ресурс] – Режим доступу до ресурсу: http://www.sota1.ru/articles/articles_142.php3.

7. Семёнов Ю. Telecommunication technologies - телекоммуникационные технологии [Електронний ресурс] / Ю. А. Семёнов. – 2012. – Режим доступу до ресурсу: http://book.itep.ru/1/intro1.htm.

8. ZigBee Alliance. ZigBee Specification. Q4/2007 [Електронний ресурс] –
Режим доступу до ресурсу: http://www.zigbee.org/en/spec_download/zigbee_downloads.asp.

9. Гордейчик С. В. Безопасность беспроводных сетей / С. В. Гордейчик, В. В. Дубровин. – Москва: Горячая линия - Телеком, 2008. – 288 с.

10. Хенкин Петр. Защита данных в сетях LTE [Електронний ресурс] / Петр Хенкин, Ольга Трофимова – Режим доступу до ресурсу: http://advancedmonitoring.ru.

11. Fernandez, E.B. & VanHilst, M., Chapter 10, WiMAX Standards and Security (Edited by M. Ilyas & S. Ahson) [Електронний ресурс] – June 2007. Режим доступу до ресурсу: http://www.crcpress.com.

12. Татарников Олег. Bluetooth и безопасность [Електронний ресурс] / Олег Татарников – Режим доступу до ресурсу: https://compress.ru/article.aspx?id=10807.

13. Кистнер Т. Стандарт 802.11b для домашнего применения [Електронний ресурс] / Тони Кистнер. – 2002. – Режим доступу до ресурсу: https://www.osp.ru/nets/2002/07/146492/.

14. Солодунов С. Средства разработки Ember для быстрой реализации проектов ZigBee / С. Солодунов. // Беспроводные технологии. – 2014. – №3. – С. 55–61.

15. Йосипенко В. Телекомунікації в складних інженерних системах [Текст] / В.А. Йосипенко. // Зв'язок. – 2007. – №1. – С. 58 – 60.

16. Johnson D. Dynamic Source Routing in Ad Hoc Wireless Networks / D. Johnson, T. Imielinski, H. Korth // Mobile Computing / D. Johnson, T. Imielinski, H. Korth., 1996. – P. 153181.

17. Heinzelman W. Energyefficient Communication Protocol for Wireless Microsensor Networks / W. Heinzelman, A. Chandrakasan, H. Balakrishnan // in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00) / W. Heinzelman, A. Chandrakasan, H. Balakrishnan. – Washington, DC, USA, 2008. – P. 8020.

18. Heinzelman R. An ApplicationSpecific Protocol Architecture for Wireless Microsensor Networks / R. Heinzelman, A. Chandrakasan, H. Balakrishnan // IEEE Tmnsactions on Wireless Communications / R. Heinzelman, A. Chandrakasan, H. Balakrishnan., 2002. – P. 660670.

19. Lindsey S. PEGASIS: Powerefficient Gathering in Sensor Information System / S. Lindsey, C. Raghavendra, 2002. – P. 11251130.

20. Younis O. Distributed Clustering in Adhoc Sensor Networks: A Hybrid, Energyefficient Approach / O. Younis, S. Fahmy., 2002. – 240 p.

21. Younis O. Heed: A hybrid, Energyefficient, Distributed Clustering Approach for Adhoc Networks / O. Younis, S. Fahmy., 2004. – 310 p.

22. Manjeshwar A. TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks / A. Manjeshwar, D. Agrawal. // the Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA. – 2001. – 64 p

23. . Lou W. An Efficient Nto1 Multipath Routing Protocol in Wireless Sensor Networks / W. Lou. – (Proceedings of IEEE MASS'05, Washington DC, Nov). – P. 18

24. Manjeshwar A. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks / A. Manjeshwar, D. Agrawal. – San Francisco CA: IEEE The Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, 2001. – 20091015 p.

25. Karp B. GPSR: Greedy perime ter stateless routing for wireless networks / B. Karp, H. Kung – Boston, MA: Proceedings ACM MobiCom'00, 2000. – P. 243254.

26. Chang W. Dynamic proxy treebased data dissemination schemes for wireless sensor networks / W. Chang, G. Cao, T. La Porta – Fort Lauderdale, FL, 2004. – (Proceedings IEEE MASS'04). – P. 2130.

27. Lindsey S. Data gathering in sensor networks using the energy delay metric / S. Lindsey, C. Raghavendra, K. Siva – San Francisco, CA: Proceedings IPDPS 01, 2001. – P. 20012008.

28. Lindsey S. Data gathering algorithms in sensor networks using energy metrics / S. Lindsey, C. Raghavendra, K. Siva, 2002. – (IEEE Transactions on Parallel and Distributed Systems). – P. 924935

29. Chu M. Scalable informationdriven sensor querying and routing for ad hoc heterogeneous sensor networks / M. Chu, H. Haussecker, F. Zhao. // International Journal of High Performance Computing Applications. – 2002. – №16. – P. 293313.

30. Du X. Improving routing in sensor net works with heterogeneous sensor nodes / X. Du, F. Lin – Dallas, TX, 2005. – (Proceedings IEEE VTC'05). – P. 25282532.

31. Mills K. A brief survey of self-organization in wireless sensor networks / K.L. Mills // Wireless Communications and Mobile Computing / K.L. Mills., 2007. – P. 823–834.

32. Dressler F. A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks / F. Dressler // Computer Communications / F. Dressler., 2008. – P. 3018–3029.

33. Handy M. Low energy adaptive clustering hierarchy with deterministic Cluster-Heads selection / M. Handy, M. Haase, D. Timmermann, 2002. – (Proc. 4th International Workshop on Mobile and Wireless Communications Network). – P. 368–372.

34. Handy M. Low energy adaptive clustering hierarchy with deterministic Cluster-Heads selection / M. Handy, M. Haase, D. Timmermann. // Proc. 4th International Workshop on Mobile and Wireless Communications Network. – 2002. – P. 368–372.

35. Perkins C. Ad hoc On-Demand Distance Vector (AODV) Routing / C. Perkins, E. Belding-Royer, S. Das. // IETF RFC. – 2003.

36. Xu Y. Geography-informed energy conservation for ad hoc routing / Y. Xu, J. Heidemann, D. Estrin. // Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking. – 2001. – P. 70–84/

37. Subramanian L., Katz R.H. An architecture for building self-configurable systems // Proc. Mobile Ad Hoc Network Comput. Workshop. — 2000. — P. 63–73.

38. Kalita H. K., Kar A. A New Algorithm of Self Organization in Wireless Sensor Network // Wireless Sensor Network. 2010. № 2. P. 43–47. DOI: 10.4236/wsn.2010.21006.

39. Krishnana R., Starobinski D. Efficient clustering algorithms for self–organizing wireless sensor networks // Ad Hoc Networks. 2006. Vol. 4. Issue 1. P. 36–59. DOI: 10.1016/j.adhoc.2004.04.002.

40. Lin J., Liu Y., Ni L. M. SIDA: Selforganized ID Assignment in Wireless Sensor Networks // Proc. IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS'2007), 2007. P. 1–8. DOI: 10.1109/MOBHOC.2007.4428604.

41. Nekoogar F., Dowla F., Spiridon A. Self Organization of Wireless Sensor Networks Using Ultra– Wideband Radios // Proc. Radio and Wireless Conference, 2004. P. 451–454. DOI: 10.1109/RAWCON.2004.1389174.

42. Rogers A., David E., Jennings N. R. Self-organized routing for wireless microsensor networks // IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans. 2005. Vol. 35. Issue 3. P. 349–359. DOI: 10.1109/TSMCA.2005.846382.

43. Dressler F. Bio– Inspired Networking – Self–Organizing Networked Embedded Systems. Berlin, Germany: Springer Berlin Heidelberg, 2008. P. 285–302. DOI: 10.1007/978–3–540–77657–4_13.

44. Self Organizing Wireless Sensor Network / K. Sohrabi, J. Gao, V. Ailawadhi, G. Pottie// Proc. 37th Annu. Allerton Conference on Communication, Control and Computing, 1999. P. 1201–1210.