

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»
УДК _____

До захисту допущено
Завідувач кафедри

_____ Сергій КРАВЧУК
(підпис) (Ім'я, прізвище)

“ ____ ” _____ 2020 р.

Магістерська дисертація
на здобуття освітнього ступеня «магістр»

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

За освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

на тему: Методика побудови сенсорної мережі моніторингу стану об'єктів спеціального призначення

Виконав: студент 2 курсу, групи ТЗ – 91 мп
(шифр групи)

_____ Тарасенко Ярослав Петрович _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник _____ доцент каф. ТК, к.т.н., доцент Явіся В.С. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____
(назва розділу) (науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент _____ доцент каф. ІТМ, к.т.н., доцент Правило В.В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць інших
авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020 р.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
Явіся В.С.
(підпис) (ініціали, прізвище)

« 20 » січня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Тарасенку Ярославу Петровичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Методика побудови сенсорної мережі моніторингу стану об'єктів спеціального призначення

науковий керівник дисертації Явіся Валерій Сергійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «03» « листопада » 2020 р. № 3208-с

2. Строк подання студентом дисертації 15.12.2020

3. Об'єкт дослідження Процес функціонування об'єктів спеціального призначення

4. Предмет дослідження БСМ моніторингу об'єктів спеціального призначення

5. Перелік завдань, які потрібно розробити Аналіз особливостей функціонування БСМ; Детальний аналіз існуючих концепцій побудови сенсорних мереж; Розробка нової методики побудови сенсорних мереж для

моніторингу станів об'єктів спеціального призначення; Розробка стартап проекту;

6. Орієнтовний перелік ілюстративного матеріалу

Слайд №1 Тема, актуальність та мета

Слайд №2 Безпроводові сенсорні мережі

Слайд №3 Аналіз методів збору інформації в БСМ

Слайд №4 Аналіз існуючих методів побудови БСМ

Слайд №5 Аналіз методу забезпечення інформаційного захисту БСМ

Слайд №6 Завдання та цілі проєктованої БСМ

Слайд №7 Розроблена методика побудови сенсорних мереж для функціонування на об'єктах спеціального призначення

Слайд №8 Висновки

7. Орієнтовний перелік публікацій _____

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 28.10.2019

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Отримання технічного завдання	28.10.2019	
2	Аналітичний огляд інформаційних матеріалів	01.03.2020 – 01.09.2020	
3	Розгляд особливостей функціонування БСМ. Написання першого розділу	01.09.2020 – 01.10.2020	
4	Аналіз існуючих методів та моделей побудови сенсорних мереж.	01.10.2020 – 15.10.2020	
5	Аналіз існуючих методів забезпечення інформаційного захисту БСМ. Написання другого розділу	15.10.2020 – 01.11.2020	
6	Розробка методу побудови сенсорних мереж для функціонування на об'єктах спеціального призначення. Написання третього розділу.	01.11.2020 – 15.11.2020	

7	Розробка стартап проекту для запропонованої методики. Написання четвертого розділу.	15.11.2020 – 01.12.2020	
8	Оформлення дисертації згідно з вимогами та діючими правилами.	01.12.2020 - 07.12.2020	
9	Подання роботи для перевірки на нормоконтроль та плагіат	07.12.2020 – 15.12.2020	

Студент

(підпис)

Тарасенко Я. П.
(ініціали, прізвище)

Науковий керівник дисертації

(підпис)

Явіся В.С.
(ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка магістерської дисертації містить 95 сторінок, 12 ілюстрацій, 10 таблиць та 18 джерел інформації.

Актуальність. Через ряд свої особливостей БСМ набувають все більшої популярності, в тому числі і на об'єктах спеціального призначення. Проте, проектування БСМ для функціонування на об'єктах спеціального призначення вимагає більшої точності та є складнішим в порівнянні з проектуванням звичайних БСМ. Враховуючи особливості функціонування та наслідки неправильної роботи БСМ на об'єктах спеціального призначення варто зазначити, такі сенсорні мережі повинні мати високу надійність та відмовостійкість, низькі енергетичні витрати та високий рівень інформаційного захисту. Тому розробка нової методики побудови сенсорних мереж для функціонування на об'єктах спеціального призначення є актуальною.

Мета. Метою даної магістерської дисертації є дослідження особливостей експлуатації сенсорних мереж на об'єктах спеціального призначення та проведення аналізу існуючих методів побудови та підвищення ефективності таких мереж. Розробка нової методики побудови сенсорних мереж для моніторингу стану об'єктів спеціального призначення, який відповідає всім необхідним вимогам та створений з урахуванням всіх особливостей та проблем функціонування таких сенсорних мереж.

Основні задачі для досягнення вказаної мети роботи:

- Аналіз особливостей функціонування БСМ;
- Детальний аналіз існуючих концепцій побудови сенсорних мереж спеціального призначення;
- Розробка нової енергоефективної методики побудови сенсорних мереж для моніторингу станів об'єктів спеціального призначення з урахуванням надійності роботи та забезпечення надійного рівня інформаційного захисту;

- Розробка стартап проекту;

Об'єкт дослідження. Процес функціонування об'єктів спеціального призначення.

Предмет дослідження. БСМ моніторингу об'єктів спеціального призначення.

Наукова новизна. В результаті дослідження було розроблено більш енергоефективну та надійну архітектурну концепцію сенсорної мережі для моніторингу об'єктів спеціального призначення. Тобто ця концепція містить такі функції, як моніторинг та оптимізація споживання електроживлення, низька собівартість технічного обслуговування, достовірність та великий обсяг станів моніторингу, захищеність від стороннього втручання та високу інформаційну безпеку.

Ключові слова: безпроводова сенсорна система спеціального призначення, методика побудови БСМ спеціального призначення, відмовостійкість, енергоефективність, інформаційний захист.

ABSTRACT

The explanatory note of the master's dissertation contains 95 pages, 10 illustrations, 10 tables and 24 sources of information.

Topicality. Due to a number of features, WSNs are becoming increasingly popular, including in special purpose objects. However, the operation of WSN to operate on special facilities requires greater accuracy and is more complex than designing conventional WSN. Given the peculiarities of the functioning and consequences of improper operation of WSN at special facilities, it should be noted, such sensor networks must have high reliability and fault tolerance, low energy costs and a high level of information security. Therefore, the development of a new method of building sensor networks for operation at special facilities is relevant.

Goal. The purpose of this master's dissertation is to study the features of the operation of sensor networks at special facilities and to analyze existing methods of building and improving the efficiency of such networks. Development of a new method of construction of sensor networks for monitoring the condition of special purpose objects, which meets all the necessary requirements, created taking into account all the features and problems of operation of such sensor networks.

The main tasks to achieve this goal:

- Analysis of the features of the WSN;
- Detailed analysis of existing concepts for the construction of special purpose sensor networks;
- Development of a new energy-efficient method of building sensor networks for monitoring the condition of special purpose objects, taking into account the reliability of work and ensuring a reliable level of information protection;
- Development of a startup project;

Objects of research. The process of functioning of special purpose objects.

Subject of research. WSN monitoring of special purpose objects.

Scientific novelty. As a result of the research, a more energy-efficient and reliable architectural concept of the sensor network for monitoring special purpose objects was developed. That is, this concept includes functions such as monitoring and optimization of energy consumption, low maintenance costs, reliability and a large number of monitoring conditions, protection from external interference and high information security.

Keywords: wireless sensor system for special purposes, methods of building WSN for special purposes, fault tolerance, energy efficiency, information protection.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	11
ВСТУП	12
1. ПРИНЦИПИ РОБОТИ ТА ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БСМ	14
1.1 Структура сенсорного вузла	15
1.2 Структура транзитних вузлів.....	17
1.3 Структура базової станції.....	18
1.4 Основні обмеження під час використання БСМ.....	20
1.5 Проблеми та необхідність інформаційного захисту в БСМ.....	22
Висновки до розділу:	23
2. АНАЛІЗ ПРИНЦИПІВ ФУНКЦІОНУВАННЯ БСМ НА ОБ'ЄКТАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ	25
2.1 Аналіз методів збору інформації в безпроводових сенсорних мережах	26
2.1.1 Аналіз методу збору даних на основі розкладу.....	27
2.1.2 Аналіз методу збору даних на основі запиту.....	29
2.1.3 Аналіз методу збору даних на основі події.....	30
2.1.4 Аналіз адаптивного методу збору даних.....	31
2.2 Аналіз існуючих методів побудови інфраструктури безпроводової сенсорної мережі	32
2.3 Аналіз методів забезпечення достовірності інформації	36
2.3.1 Управління потужністю прийомопередавача	37
2.3.3 Автоматичний запит повторної передачі	38
2.4 Аналіз методів інформаційного захисту БСМ	40
2.4.1 Аналіз протоколів захищеної маршрутизації сенсорної мережі	41
2.4.2 Аналіз існуючих методів шифрування та методів керування ключами	44
2.4.3 Протоколи безпеки для сенсорних мереж.....	47

Висновки до розділу:	51
3. МЕТОДИКА ПОБУДОВИ СЕНСОРНОЇ МЕРЕЖІ МОНІТОРИНГУ СТАНУ ОБ'ЄКТІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ	54
3.1 Визначення цілей та основних параметрів запропонованої БСМ	54
3.2 Розробка структури сенсорної мережі та складу сенсорного вузла	56
3.3 Визначення методу збору даних.....	58
3.4 Вибір протоколу маршрутизації.....	61
3.5 Розробка системи інформаційного захисту.....	66
3.5.1. Інформаційний захист фізичного рівня	66
3.5.2 Інформаційний захист канального рівня	70
3.5.3 Інформаційний захист мережевого рівня	72
3.5.4 Інформаційний захист прикладного рівня	75
3.6 Методика побудови сенсорної мережі для моніторингу станів об'єктів спеціального призначення.....	78
Висновки до розділу:	81
4. РОЗРОБКА СТАРТАП ПРОЕКТУ	83
4.1 Опис розробленої методики.....	83
4.2 Технологічний аудит проекту.....	85
4.3 Аналіз ринкових можливостей запропонованого проекту	86
Висновки до розділу:	89
ВИСНОВОК.....	90
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	93

ПЕРЕЛІК СКОРОЧЕНЬ

БСМ – Безпроводова сенсорна мережа

АЦП – Аналогово – цифровий перетворювач

BER (Bit Error Rate) – інтенсивність бітових помилок

CRC (Cyclic Redundancy Check) – циклічний надлишковий код

FCS (Frame Check Sequence) – послідовність перевірки кадру

MAC (Message Authentication Codes) – кодове повідомлення автентифікації

RREP (Route Response) – відповідь маршруту

RREQ (Route Request) – запит маршруту

TESLA (Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol) - тимчасовий, ефективний, потоковий протокол автентифікації, стійкий до втрат

SNEP (Secure Network Encryption Protocol) – протокол безпечного мережевого шифрування

SPIN (Sensor Protocols for Information via Negotiation) – сенсорні протоколи для інформації через переговори

LEACH (Low-Energy Adaptive Clustering Hierarchy) – ієрархічний алгоритм адаптивної кластеризації з низьким рівнем використання енергії

ESPDA (Energy-Efficient Secure Pattern based Data Aggregation) - агрегація даних на основі енергоефективних захищених шаблонів

TDMA (Time Division Multiple Access) – доступ з розділенням у часі

FHSS (Frequency Hopping Spectrum Spreading) – розширення спектру методом стрибкоподібної зміни частоти

ГВЧ – генератор випадкових чисел

ACK (Acknowledgement) – повідомлення підтвердження

CBC (Cipher Block Chaining) - режим ланцюгування шифроблоків

GK (Global Key) – глобальний ключ

СК (Cluster Key) – ключ кластера

СК (Sensor Key) – ключ сенсорного вузла

ВСТУП

Останнім часом все більшої популярності набирають безпроводові сенсорні мережі. Завдяки ряду переваг і особливостей їх залучають для використання до все більшої кількості різних сфер з метою забезпечення надійного та якісного моніторингу. Проте для надійної роботи системи необхідно її чітко та правильно спроектувати ще на первинних етапах розробки. Проектування та побудова сенсорних мереж для моніторингу об'єктів є надзвичайно складним завданням. Постійний моніторинг параметрів об'єкту спостереження, який може змінюватися як у часі так і у просторі, майже завжди створює значні потоки інформації. Основним завданням сенсорної мережі є своєчасна та повна доставка цієї інформації до центрів керування. Ще однією складністю є те, що в багатьох системах моніторингу важко або взагалі неможливо визначити інфраструктуру сенсорної мережі, що приводить до складностей її побудови та обслуговування.

Проте проектування таких сенсорних мереж для їх використання на об'єктах спеціального призначення є на порядок складнішим ніж проектування звичайних БСМ. Перша складність обумовлена тим, що сенсорна мережа повинна своєчасно та безпомилково реагувати на зміну стану об'єкту моніторингу. Тобто при спостереженні за спеціальними об'єктами правильність та оперативність виявлення інформації є критично важливим питанням. Ще однією складністю є забезпечення надійного рівня інформаційної безпеки. Використовуючи сенсорну систему для моніторингу спеціальних об'єктів недооцінювання факторів її інформаційної безпеки може призвести до тяжких або навіть катастрофічних наслідків. Тому для мінімізації ризиків необхідно прийняти всі міри для ускладнення чи унеможливлення протиправних дій стосовно системи моніторингу. Проте чи не найбільшою складністю при побудові таких сенсорних мереж є обмеженість ресурсами сенсорного вузла. А саме обмеження в ресурсах

пам'яті, енергії, швидкостях передачі та якісних алгоритмах обробки великої кількості даних.

В першому розділі роботи описано особливості функціонування БСМ. Розглянуто структуру основних вузлів, які входять до складу БСМ, а саме: сенсорних вузлів, транзитних вузлів та базових станцій. Також в цьому розділі описані основні обмеження використання БСМ та необхідність забезпечення надійного рівня інформаційного захисту.

Другий розділ присвячено порівняльному аналізу існуючих методів та аспектів побудови сенсорних мереж для функціонування на об'єктах спеціального призначення. В цьому розділі проаналізовані основні методи збору інформації в БСМ, методи побудови інфраструктури таких сенсорних мереж, методи підвищення достовірності інформації та існуючі методи забезпечення інформаційного захисту в БСМ. Аналіз був проведений на основі енергоефективності, часу життя та надійності функціонування БСМ.

В третьому розділі було запропоновано нову методику побудови сенсорних мереж для моніторингу об'єктів спеціального призначення на прикладі атомної електростанції. Нова методика передбачає визначення основних цілей та параметрів проектованої БСМ, розробку структури мережі та складу сенсорного вузла, надійну модель збору інформації, чітку маршрутизацію та надійний рівень інформаційного захисту.

Четвертий розділ присвячений розробці стартап проекту для запропонованої методики побудови сенсорних мереж для функціонування на об'єктах спеціального призначення.

1. ПРИНЦИПИ РОБОТИ ТА ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БСМ

Беспроводові сенсорні мережі це автономні сенсорні мережі, які використовуються для моніторингу за певним середовищем. Це може бути моніторинг фізичних станів об'єкту або певних екологічних станів навколишнього середовища. В основі роботи БСМ лежить те, що сенсорний вузол збирає певну інформацію про об'єкт моніторингу, здійснює її первинну обробку та передає її до центру керування через проміжні вузли. Центр керування сенсорною мережею виконує функцію керування та збору всієї інформації та представлення її користувачу, тобто можна сказати, що центр керування слугує інтерфейсом між користувачем та всією мережею. Зазвичай БСМ складається із сотень сенсорних вузлів, які обмінюватися даними між собою за допомогою радіосигналів. Беспроводовий сенсорний вузол оснащений певними датчиками, обчислювальними пристроями, прийомопередавачами та силовими компонентами. Окремі вузли в бездротовій сенсорній мережі мають певні обмеження в ресурсах: вони мають обмежену швидкість обробки інформації, ємність зберігання та пропускну здатність зв'язку. Після розгортання сенсорних вузлів вони відповідають за самоорганізацію відповідної мережевої інфраструктури. Після чого вузли починають збирати необхідну інформацію. Бездротові сенсорні вузли також відповідають на запити, які надіслані з базової станції для виконання певних інструкцій або передачі зібраних параметрів моніторингу. Режим роботи сенсорних вузлів може бути як неперервним так і керованим на основі детектування події.

За останній час БСМ здобули широкого розповсюдження через ряд своїх переваг. До основних переваг використання БСМ можна віднести:

- невеликі габарити та низьку собівартість окремих сенсорних вузлів;
- висока масштабованість БСМ;
- швидкість та легкість розгортання сенсорної мережі;

- стійкість до змін топології мережі;
- відмовостійкість сенсорної системи, внаслідок наявності великої кількості запасних маршрутів;
- самовідновлення та самоорганізація мережі;
- здатність обробки отриманої інформації та винесення відповідних рішень на сенсорних вузлах;

Тому через ряд своїх особливостей БСМ набули широкого розповсюдження. Таке розповсюдження також було досягнуто за рахунок гнучкості безпроводових сенсорних мереж та їх здатності до вирішення певних проблем в різних сферах використання. До основних сфер використання БСМ можна віднести:

- моніторинг параметрів навколишнього середовища;
- моніторинг об'єктів спеціального призначення;
- системи виявлення пожеж;
- системи безпеки та охорони та інші;

Проте в усіх випадках при розробці будь-якої сенсорної мережі однією з основних цілей є підтримка загальної працездатності мережі якомога довше. Ключовим фактором при цьому є спосіб формування мережі. Фактично, топологія в основному визначається на основі середовища та особливостей об'єкту моніторингу. Складність конструкції БСМ залежить від конкретних вимог мережі, таких як кількість вузлів, енергоспоживання, термін служби датчиків, інформація, яку необхідно сприймати, місце розташування датчиків та навколишнє середовище.

1.1 Структура сенсорного вузла

В БСМ сенсорні вузли виконують функції збору інформації, її первинної обробки та передачі до центру керування. Сенсорні вузли мають в своєму складі такі основні елементи: блок відповідних сенсорних датчиків, блок обробки інформації, прийомопередавач та джерело живлення. Також відповідно до особливостей сенсорної мережі та об'єкту моніторингу можуть

встановлюватися додаткові блоки. Приклад структурної схеми сенсорного вузла представлений на рисунку 1.1.

Блок сенсорних датчиків, зазвичай, складається з двох елементів: сенсорні датчики та АЦП. Принцип роботи полягає в тому, що сенсорні датчики зчитують необхідні параметри та перетворюють їх в аналоговий сигнал, АЦП в свою чергу перетворює цей аналоговий сигнал в цифровий та передає до блоку обробки інформації. Блок обробки інформації обробляє отриманий аналоговий сигнал та визначає зміну стану об'єкту моніторингу чи детектує відповідну подію, порівнюючи отримане значення з пороговим. Після чого сигнал передається до прийомопередавача. Він являє собою пристрій для встановлення зв'язку між вузлами сенсорної мережі. Для забезпечення живлення всіх вказаних блоків використовується джерело живлення.

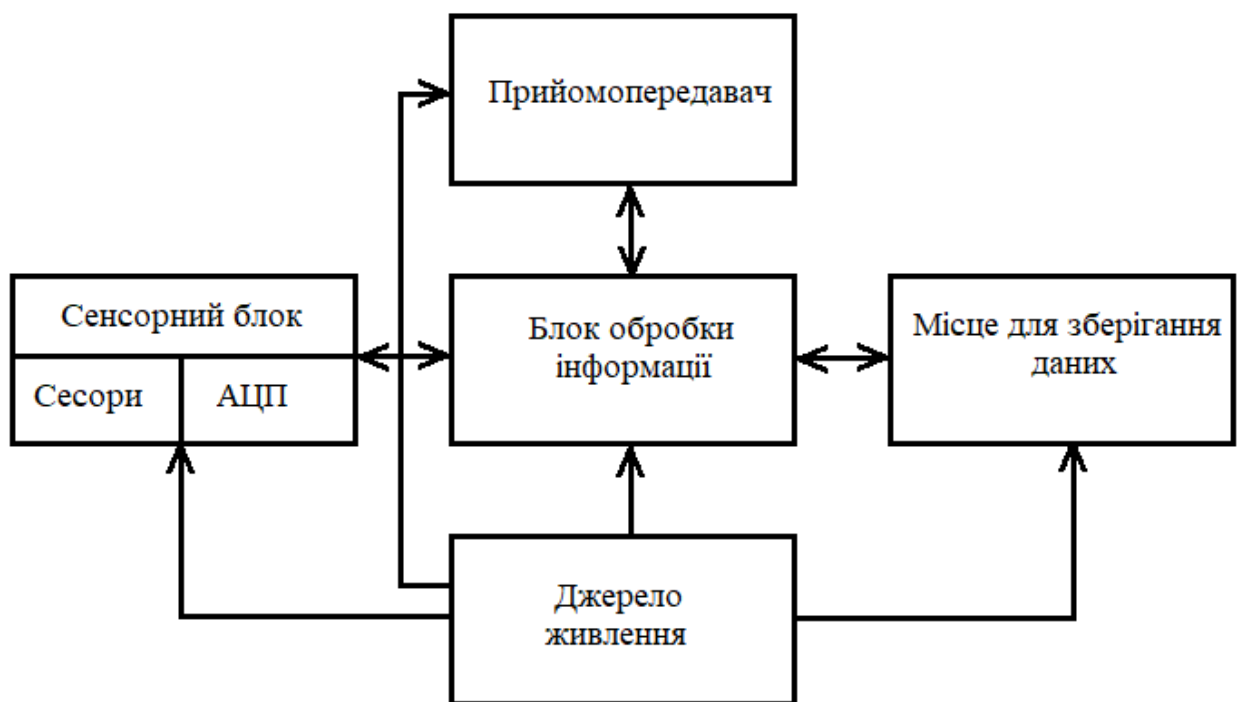


Рис.1.1. Структурна схема сенсорного вузла

Кожен сенсорний вузол повинен відповідати наступним вимогам:

- невисокий рівень енергоспоживання;
- невисока вартість;
- працювати в автономному режимі роботи;
- мати зв'язок з сусідніми вузлами та мати змогу працювати з великою кількістю інших вузлів, при невеликих відстанях між ними;
- можливість адаптації до зміни параметрів об'єкту моніторингу;

1.2 Структура транзитних вузлів

Транзитні вузли в БСМ можуть бути представлені маршрутизаторами або шлюзами. Такі вузли виконують функції збору інформації, отриманої від сенсорних вузлів та передачі її до базової станції. Також вони конфігурують загальні параметри мережі, додають нові вузли та можуть виконувати роль моніторингу загальних мережевих характеристик. Зазвичай транзитні вузли мають в своєму складі вузол з прийомопередавачем для збору інформації від сенсорних вузлів та пристрій для зв'язку з базовою станцією.

Працюючи без маршрутизатора шлюз NIWSN Ethernet може з'єднувати 8 сенсорних вузлів. За рахунок використання у мережевій топології маршрутизаторів шлюз може з'єднувати 36 вузлів. На рисунку 1.2 показано маршрутизатор Phy Net Router з Монографія «Інформаційна безпека в середовищі безпроводових сенсорних мереж» 16 вбудованою двонаправленою антеною на 2,4 ГГц. Розміри такого маршрутизатора 4,4 x 2,3 x 9,3 см, вага 718 г. Для його живлення від стаціонарної електричної мережі передбачено використання зовнішнього адаптера на 100-240 В AC на 50/60 Гц, який на виході забезпечує номінальну постійну напругу на 5 В [3].



Рис.1.2. Маршрутизатор Phy Net Router [3]

Маршрутизатори виконують функції передачі пакетів інформації, забезпечують відповідну маршрутизацію, та створюють нові маршрути, які були втрачені внаслідок неправильної роботи сенсорної мережі або зловмисного втручання. Вони дозволяють будувати БСМ з високою розгалуженістю та масштабованістю та керувати ними. За рахунок використання великої кількості транзитних вузлів можна досягти високої кількості сенсорних вузлів, що підключені до мережі а також зменшити загальні енерговитрати та затримки при передачі, за рахунок удосконалення шляхів ретрансляції пакетів інформації між вузлами мережі.

1.3 Структура базової станції

Базові станції слугують для координації всієї сенсорної мережі. Вони відповідають за організацію зв'язку між ними та сенсорними вузлами або транзитними вузлами. За рахунок цього існує можливість розташування сенсорної мережі на великих територіях та здійснювати контроль над ними з єдиного центру управління. Базова станція посуті є своєрідним центром керування мережею. Вона конфігурує всю мережу, керує процесом додавання вузлів, встановлює політику безпеки та керує відповідними

мережевими ключами. Також базова станція забезпечує такі дії з інформацією, як: її обробка, зберігання, аналіз та представлення користувачу.

Зокрема Phy Net Server забезпечує трансляцію інтерфейсів ІВ у веб-сервіси з SOAP/Rest/XML інтерфейсами, веб-консоль користувача для налаштування ІВ, візуалізацію стану розгортання БСМ на дисплеї у вигляді карти користувача або зображення, відкриває, реєструє, переміщує, конфігурує вузли, вмикає/вимикає ІВ, відображає батареїний статус, програмує гетерогенні вузли, дозволяє налаштувати маршрутизатори, графічно відображати статистику, налаштувати інтервали звітності, пороги і попередження. До складу Phy Net Server (рис. 1.3) входить: процесор 1,6 ГГц, пам'ять 512 Мбайт, жорсткий диск 60 Гбайт, порти вводу/виводу RJ 45 10/1000 Ethernet, USB, Wi-Fi. Тобто для керування БСМ підприємства достатньо пристрою, який функціонально подібний до малого ПК, вміщується у корпус з розмірами 14,6x25x4,198 см. важить 1,36 кг. Роботу такої базової станції забезпечує зовнішній адаптер перемінної напруги 100-240 В. Робоча температура сервера від 0 до 40 0С [3].



Рис.1.3.Базова станція Phy Net Server [3]

1.4 Основні обмеження під час використання БСМ

Незважаючи на ряд свої переваг під час проектування та розгортання БСМ також виникає і ряд складнощів та обмежень. Перше і найбільше обмеження в БСМ це енергоресурси сенсорних вузлів. Тому під час проектування сенсорної мережі з самого початку постає проблема ефективного енерговикористання ресурсів на сенсорних вузлах. Щоб забезпечити максимальний термін функціонування мережі, вона повинна бути з самого початку спроектована з урахуванням ефективного керування енергетичними ресурсами.

Фактор енерговикористання сенсорних вузлів, визначає загальний термін функціонування сенсорної мережі. В цьому аспекті важливо чітко розуміти режими роботи сенсорного вузла та енерговикористання під час цих режимів. Як описано вище, сенсорний вузол складається з чотирьох блоків:

- Блок сенсорів. Складається з групи сенсорів та АЦП. Енерговикористання під час функціонування цього блоку можна знизити за рахунок використання сенсорів з невисокими потужностями та непостійної роботи сенсорного вузла, тобто зчитування параметрів середовища з певною періодичністю або на основі детектування певної події;
- Блок обробки інформації, зазвичай представлений мікропроцесором. Зазвичай цей блок працює в різних режимах для забезпечення керування сенсорним вузлом. Враховуючи той факт, що такі режими роботи зв'язані з рівнями енерговикористання, при проектуванні варто враховувати цей факт;
- Блок прийомопередавача. Прийомопередавачі можуть працювати в різних режимах. Тому одним з методів зменшення енерговикористання є керування потужностями передачі та, під час відсутності передачі, вимикати прийомопередавач, а не переводити в режим очікування;

- Блок живлення. Зазвичай представлений батареєю, яка виконує функцію живлення всіх елементів сенсорного вузла. Для зменшення загальних енерговитрат та підвищення строку служби джерела живлення можливо використовувати для живлення вузла меншу силу струму ніж номінальна сила струму джерела;

Тому варто зазначити, що для загального зменшення енерговикористання та підвищення часу функціонування на етапі проектування та розгортання мережі потрібно прийняти для цього якомога більше дій.

Ще одне обмеження це відмовостійкість. Варто зазначити, що часто сенсорні мережі розгортаються в небезпечних середовищах, що робить сенсорні вузли мережі більш вразливими. Сенсорні вузли можуть вийти з ладу через ряд певних проблем з мережею, зловмисного втручання або використання всього запасу енергії. Тому для підвищення відмовостійкості мережі існує необхідність забезпечення чіткої та правильної маршрутизації. Маршрутизація в сенсорної мережі повинна мати можливість знаходити сенсорні вузли, які припинили своє функціонування, якомога швидше і бути досить надійною, щоб забезпечити правильне функціонування мережі при наявності таких вузлів та їх великої кількості. Тобто, маршрутизація в БСМ повинна гарантувати наявність альтернативних шляхів для передачі інформації до потрібного отримувача. Проте варто зазначити, що різні особливості та середовища функціонування БСМ вимагають забезпечення різних рівнів відмовостійкості та накладають свої унікальні вимоги.

Іншим обмеженням є апаратні обмеження. В основному, кожен сенсорний вузол повинен мати сенсорний блок, блок обробки інформації, блок прийомопередачі і джерело живлення. Існує можливість того, що сенсорні вузли будуть мати кілька вбудованих датчиків або додаткових блоків, таких як система локалізації для забезпечення маршрутизації з урахуванням місця розташування. Однак з використанням додаткового функціоналу збільшується енергоспоживання і фізичний розмір вузла. Таким

чином, додаткова функціональність завжди повинна бути збалансована з урахуванням вартості і низького енергоспоживання.

Ще одним обмеженням є масштабованість. Сенсорні мережі можуть складатися з декількох вузлів або навіть кількох сотень таких вузлів. Відповідно, щільність БСМ також може бути різною. Для надійного та своєчасного збору даних, загальна щільність вузлів може бути такою, що окремий вузол може мати кілька сотень сусідів в межах своєї передачі. Тому, під час розгортання сенсорних мережах, необхідно використовувати протоколи, які забезпечують певний рівень масштабованості і мають можливість підтримувати високу продуктивність мережі.

1.5 Проблеми та необхідність інформаційного захисту в БСМ

Основна ціль на яку направлена інформаційна безпека в БСМ це забезпечення конфіденційності, цілісності, доступності, автентифікації та актуальності даних, якими оперує БСМ. Під конфіденційністю варто розуміти спосіб унеможливлення отримання інформації злоумисниками, тобто дані БСМ не повинні потрапити до неавторизованих осіб. Цілісність передбачає унеможливлення зміни чи підробки повідомлення злоумисником. Автентифікація забезпечує те, що обмін повідомленнями в мережі відбувається лише між оригінальними та зареєстрованими вузлами. Доступність забезпечує змогу своєчасного, повного та правильного отримання інформації користувачам, які належать до системи і мають для цього право. Під актуальністю даних варто розуміти те, що на приймальній стороні буде отримано лише актуальні і оновлені данні, тобто це гарантія того, що злоумисник не зможе відтворити застарілі дані. Актуальність даних особливо важлива у випадку коли в сенсорній мережі використовуються спільні ключі. При ненадійному рівні актуальності злоумисник може отримати старий ключ та на основі нього видати себе за оригінальний вузол.

В зв'язку з недавнім розвитком БСМ та особливими характеристиками не існує чіткої лінії захисту. На відміну від традиційних мереж з виділеними маршрутизаторами в БСМ кожен вузол може працювати як адміністратор, агрегатор та маршрутизатор. З однієї сторони це робить БСМ більш функціональним, але з іншої створює додаткові ускладнення. Через відсутність чітких ліній захисту всі спроби його проектування повинні відповідати основним напрямкам: запобігання, виявлення, усунення загроз. В основному під запобіганням слід розуміти можливість унеможливлення будь якого виду атаки, забезпечення правильності маршрутизації та встановлення безпечного зв'язку. Підхід виявлення розуміє здатність системи своєчасно виявляти та ідентифікувати загрози. Усунення загроз може бути використаним для анулювання будь-яких загроз чи пошкоджень системи і усунення недоліків захисту. Коли в мережу вводиться більше функцій безпеки, паралельно з підвищенням рівня безпеки, постійно зростає обчислення, комунікація та накладні витрати на керування. Отже, продуктивність мережі, з точки зору масштабованості, доступності сервісу, надійності та інших засобів безпеки стає важливим питанням у БСМ, яка обмежена ресурсами.

Висновки до розділу:

В розділі було розглянути особливості функціонування та принципи роботи БСМ. Слід зазначити, що через ряд свої переваг останнім часом БСМ набирають високої популярності. Це обумовлено тим, що маючи невисоку собівартість та габарити сенсорних вузлів, за допомогою них можна побудувати високомасштабовану сенсорну мережу, здатну самоорганізовуватись та підлаштовуватись відповідно до об'єкту моніторингу.

В розділі були розглянуті структури трьох основних вузлів сенсорної системи, а саме: сенсорного вузла, транзитного вузла та базової станції. Варто зазначити, що сенсорний вузол виконує функції збору та первинної

обробки інформації і складається з чотирьох основних елементів: блоку сенсорів, блоку обробки інформації, блоку прийомопередавача та джерела живлення. Транзитні вузли служать для ретрансляції інформації від сенсорних вузлів до базової станції. В основі їхньої структури можна виділити два основні елементи: вузол з прийомопередавачем для збору інформації від сенсорних вузлів та пристрій для зв'язку з базовою станцією. За координацію та управління всією мережею відповідають базові станції.

Також були проаналізовані основні проблеми та вимоги до застосування сенсорних мереж. До таких проблем варто віднести обмеження сенсорних вузлів в енергетичних ресурсах та їх апаратні обмеження, масштабованість та відмовостійкість всієї мережі в результаті яких виникає ряд додаткових ускладнень. Також варто зазначити, що без відповідного рівня інформаційної безпеки функціонування сенсорних мереж буде неправильним та майже неможливим. Тобто отримання інформації або доступу до сенсорної мережі в наслідок зловмисних дій, може потягти за собою тяжкі або навіть катастрофічні наслідки.

2. АНАЛІЗ ПРИНЦИПІВ ФУНКЦІОНУВАННЯ БСМ НА ОБ'ЄКТАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Проектування та побудова сенсорних мереж для моніторингу об'єктів є надзвичайно складним завданням. Постійний моніторинг параметрів об'єкту спостереження, який може змінюватися як у часі так і у просторі, що майже завжди створює значні потоки інформації. Основним завданням сенсорної мережі є своєчасна та повна доставка цієї інформації до центрів керування. Ще однією складністю є те, що в багатьох системах моніторингу важко або взагалі неможливо визначити інфраструктуру сенсорної мережі, що приводить до складностей її побудови та обслуговування.

Проте проектування таких сенсорних мереж для їх використання на об'єктах спеціального призначення є на порядок складнішим ніж проектування звичайних БСМ. Перша складність обумовлена тим, що сенсорна мережа повинна своєчасно та безпомилково реагувати на зміну стану об'єкту моніторингу. Тобто при спостереженні за спеціальними об'єктами правильність та оперативність виявлення інформації є критично важливим питанням, адже у протилежному випадку це може мати тяжкі або навіть катастрофічні наслідки. Для забезпечення цієї вимоги необхідно чітко визначити методи збору інформації сенсорною мережею. Тому перша частина цього розділу присвячена аналізу відомих методів збору інформації в БСМ.

Ще однією особливістю при проектуванні таких сенсорних мереж є чіткість та правильність вибору інфраструктури, що не завжди є можливим та методів підвищення достовірності інформації. І чи не найважливішим є питання забезпечення надійного рівня інформаційної безпеки. Використовуючи сенсорну систему для моніторингу спеціальних об'єктів недооцінювання факторів її інформаційної безпеки може призвести до тяжких або навіть катастрофічних наслідків. Тому для мінімізації ризиків необхідно прийняти всі міри для ускладнення чи унеможливлення

протиправних дій стосовно системи моніторингу. Проте основна складність при забезпеченні всіх вищевказаних вимог є обмеженість ресурсами сенсорного вузла. А саме обмеження в ресурсах пам'яті, енергії, швидкостях передачі та якісних алгоритмах обробки великої кількості даних.

2.1 Аналіз методів збору інформації в безпроводових сенсорних мережах

Враховуючи той фактор, що безпроводові сенсорні мережі можуть розташовуватися на великих відстанях чи у важкодоступних середовищах, алгоритми їх роботи та програмне забезпечення мають велике значення, вони мають забезпечувати надійність і відмовостійкість мережі, максимальний час роботи вузла, та часткове автоматичне конфігурування. Тому варто зазначити, що самим дефіцитним ресурсом є енергія, яка визначає час роботи всієї мережі.

Основною особливістю сенсорних мереж є можливість ретрансляції даних від одного вузла до іншого, це дозволяє при невеликих потужностях передавача передавати інформації на великі відстані. З іншого боку сенсорні вузли мають обмеження в обчислювальних потужностях, канали передачі жорстко обмежені в пропускній здатності та дальності і надійності зв'язку. В багатьох системах важко або зовсім не можливо передбачити інфраструктуру для побудови сенсорної мережі. Тому одною з основних тем для дослідження є збір, обробка та доставка інформації в сенсорних мережах. Розробка ефективного методу та алгоритму збору інформації для безпроводової сенсорної мережі дозволить зменшити час збору інформації її сенсорними вузлами та їх енергозатратність. Таким чином підвищаться ефективність та час роботи всієї сенсорної мережі. Проте, зараз, не існує універсального методу збору даних, який здатен в повній мірі застосовуватись за призначенням БСМ.

Далі приведено аналіз існуючих методів збору інформації:

- метод збору даних на основі розкладу;
- метод збору даних на основі запиту;
- метод збору даних на основі події;
- адаптивна метод збору даних;

Аналіз вказаних методів проведений на основі енергоспоживання(загального та в різних режимах роботи) та часу роботи вузла.

2.1.1 Аналіз методу збору даних на основі розкладу

Принцип роботи метод збору даних на основі розкладу полягає в тому, що безпроводовий сенсорний вузол надсилає повідомлення про поточний стан об'єкту моніторингу в поточний час за певним розкладом. Розклад відправки повідомлень залежить від специфіки та особливостей об'єкту моніторингу, тобто він зазначається на основі вимог про частоту оновлення даних про стан об'єкту моніторингу. За допомогою даного методу збору інформації дозволяє оптимізувати використання енергії сенсорним вузлом за рахунок чергування робочих режимів(збір, обробка, та відправлення даних) та режиму сну.

Загальне енергоспоживання вузла можна визначити за формулою:

$$E_B = (E_{\Pi} + E_{\Pi P} + E_M) \times T_A + (E_C + E_{IH}) \times T_C, \quad (2.1)$$

де E_{Π} – енергія, що використовується вузлом за період прийому;

$E_{\Pi P}$ – енергія, що використовується вузлом за період передачі;

E_M – енергія, яку споживає мікроконтролер;

E_C – енергія, яка використовується під час режиму сну;

E_{IH} – енергія, що використовується в інших режимах(режим видхлу чи переходу в стан сну та інші).

Час роботи вузла в такому режимі можна записати такою формулою:

$$T_B = \frac{E_B}{E_B} (T_A + T_C), \quad (2.2)$$

де E_B – енергоспоживання вузлах;

T_A – період робочого режиму;

T_C – період режиму сну;

E_B – заряд батареї.

Основну частину часу сенсорні вузли перебувають в пасивному режимі і переходять в робочий режим після закінчення часу збору даних про стан об'єкту моніторингу, або при отриманні повідомлення від сусідніх вузлів.

Передачу інформації при методі збору даних на основі розкладу можна представити як хвилі, що передаються від початкового вузла до центру керування мережею, рис 2.1 .

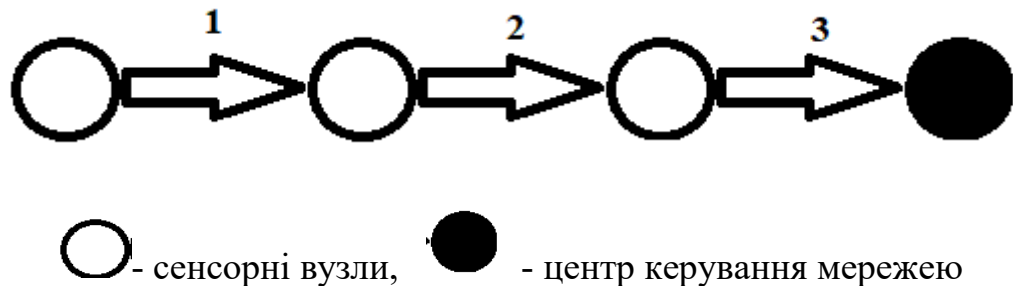


Рис.2.1. Приклад передачі інформації при моделі збору даних на основі розкладу

Для нормальної роботи сенсорної мережі та надійної ймовірності доставки повідомлення надважливим є необхідність синхронізації вузлів мережі, а саме синхронізації часу робочих режимів на всіх вузлах мережі.

Ймовірність успішної доставки повідомлення можна пов'язати з відхиленням пристрою синхронізації вузла такою формулою:

$$P = 1 - \frac{\Delta t}{T_A - T_C}, \quad (2.3)$$

де Δt – час розсинхронізування вузлів (час коли доставка повідомлення не можлива).

Для підвищення точності годинників вузлів необхідно здійснювати їх корекцію, спираючись на дані попередньої синхронізації. Як еталон можна

використовувати час на центрі керування мережею, який можливо синхронізувати з пристроєм точного часу.

Метод збору даних на основі розкладу ефективна під час її використання для постійного моніторингу параметрів досліджуваного об'єкту. Основною проблемою використання даного методу є складність синхронізації вузлів між собою та з центром керування, а також те, що повідомлення будуть надсилатися до центру керування в один час, що може призвести до додаткового навантаження на мережу. Для усунення вказаних проблем необхідно використовувати механізми синхронізації робочих режимів вузлів, що призведе до більш рівномірного навантаження на мережу.

2.1.2 Аналіз методу збору даних на основі запиту

Метод збору даних на основі запиту ґрунтується на взаємодії між вузлами безпроводової сенсорної мережі та центром управління. Алгоритми за якими працює даний метод багато в чому схожі з алгоритмами в традиційних системах управління базами даних. Принцип роботи методу полягає в тому, що центр керування мережею надсилає запит з вказаними параметрами, вузли мережі обробляють цей запит і у відповідь надсилають дані моніторингу. Тому сенсорний вузол можна розглядати як джерело даних, а всю мережу як розподілену базу даних.

Запит може відправлятися з певною періодичністю або внаслідок якоїсь події. Він може надсилатися як і всій мережі так і окремим її складовим. Одним з основних недоліків є складність формулювання запитів на мовах програмування високого рівня та неможливість казати у запиті просторово-часові вимоги до полів даних.

Час роботи безпроводової сенсорної мережі при використанні моделі збору даних на основі запиту залежить від типу запитів та їх частоти, механізмів агрегації даних та обчислювальної складності запитів.

Максимальну частоту запитів можна записати формулою:

$$F = \frac{E_B \times E}{T_3}, \quad (2.4)$$

де T_3 – час необхідний на виконання запиту(в годинах);

E – енергозатрати вузла на час T_3 .

Загальні енергозатрати вузла можна записати як суму всіх його енергозатрат в різних режимах роботи:

$$E = E_C + E_M + E_{\Pi} + E_{\Pi P} + E_{\Pi H}, \quad (2.5)$$

де E_{Π} – енергія, що використовується вузлом за період прийому;

$E_{\Pi P}$ – енергія, що використовується вузлом за період передачі;

E_M – енергія, яку споживає мікроконтролер;

E_C – енергія, яка використовується під час режиму сну;

$E_{\Pi H}$ – енергія, що використовується в інших режимах(режим видхлу чи переходу в стан сну та інші).

Застосування методу збору даних на основі запиту дозволяє частково отримати переваги описані в моделі збору на основі розкладу. До недоліків даного методу можна віднести необхідність розробки складного програмного забезпечення для обробки запиту, агрегації та вибору даних, а також збільшення вимог до обчислювальних потужностей вузлів.

2.1.3 Аналіз методу збору даних на основі події

В основі роботи методу збору даних на основі події лежить те, що перше повідомлення надсилає сенсорний вузол. Вузол відправляє повідомлення центру керування мережею, тільки в разі виявлення певної події. Тому за допомогою цього методі можна досягнути невеликих енергозатрат та довгого терміну роботи вузла.

Використання в даному алгоритмі механізмів локальної фільтрації даних дає можливість зменшити навантаження на мережу та можливість уникнути сигналізування від багатьох вузлів про одну і ту ж подію. Це вдається досягнути за рахунок визначення типу важливої події.

Загальний час роботи вузла можна записати формулою:

$$T = \frac{E_B}{E} (T_{A1} + T_{A2} + T_C), \quad (2.6)$$

де E – енергоспоживання вузла;

T_{A1} – період робочого режиму без події;

T_{A2} – період робочого режиму з подією;

T_C – період сну;

E_B – заряд батареї.

Загальне енергоспоживання вузла можна записати:

$$E = E_M \times T_{A1} + (E_M + E_{\text{пр}} + E_{\text{п}}) \times T_{A2} + (E_C + E_{\text{ін}}) \times T_C, \quad (2.7)$$

де $E_{\text{п}}$ – енергія, що використовується вузлом за період прийому;

$E_{\text{пр}}$ – енергія, що використовується вузлом за період передачі;

E_M – енергія, яку споживає мікроконтролер;

E_C – енергія, яка використовується під час режиму сну;

$E_{\text{ін}}$ – енергія, що використовується в інших режимах (режим відхлупу чи переходу в стан сну та інші).

Метод збору даних на основі події найбільш ефективна під час її використання для моніторингу об'єктів де необхідне швидке визначення важливих подій або стрімка зміна стану об'єкту моніторингу. Якщо чітко визначити подію не вдається, пропонується проводити детектування події певною групою чи всіма вузлами сенсорної мережі. До недоліків вказаного алгоритму можливо віднести складність або зовсім неможливість оперативного отримання інформації про загальний стан об'єкту моніторингу та обмежене застосування.

2.1.4 Аналіз адаптивного методу збору даних

Метод функціонування адаптивної моделі збору даних базується на ідеї самоорганізуючих сенсорних мереж. Основна ідея полягає в тому, що в системі відсутній який чіткий алгоритм роботи. Вузли мережі певним чином

самостійно організовуються в мережу, відповідно до сфери застосування безпроводової сенсорної мережі.

Для розподілу пропускної здатності мережі застосовують пріоритети вузлів вищого рівня і інтервали передачі інформації вузлам нижчого рівня. Визначення інтервалів передачі інформації можна записати формулою:

$$T = T_{\text{ПТ}} \frac{e_i(p_{\text{макс}}+1) - \sum_1^{e_i} p_i}{p_{\text{макс}} - p_i + 1} \beta_t, \quad (2.8)$$

де $T_{\text{ПТ}}$ – період передачі інформації, призначений для поточного вузла його вузлом вищого рівня;

$p_{\text{макс}}$ – максимальний пріоритет вузлів нижчого рівня;

p_i – пріоритет вузла нижчого рівня;

e_i – кількість вузлів нижчого рівня;

β_t – час можливої затримки передачі.

За допомогою застосування адаптивного методу збору інформації можна досягти підвищення рівня надійності і затримки доставки пакетів інформації з більш пріоритетних вузлів.

Загальний сенс використання адаптивних методів збору інформації полягає у відсутності чіткого розкладу, закладеного в принципи функціонування мережі. Вузли сенсорної мережі самостійно визначають, якому вузлу їм передавати інформацію та у який час це краще зробити.

До переваг даного методу можна віднести підтримку мобільності та високу надійність мережі. До недоліків варто віднести тривалий час збору даних та високі енергозатрати сенсорними вузлами.

2.2 Аналіз існуючих методів побудови інфраструктури безпроводової сенсорної мережі

На сьогоднішній день є два повністю протилежних підходи до побудови інфраструктури сенсорних мереж. Перший з них ґрунтується на повній відсутності чіткої фізичної інфраструктури мережі. Тобто сенсорна мережа з такою інфраструктурою не має певних пристроїв чи чітких

установок, які підтримують зв'язок між усіма вузлами мережі. Замість того підтримка взаємодії між вузлами забезпечується цими ж вузлами, але відповідно до рівня їх доступу. При такому методі взаємодія між вузлами необхідна для забезпечення чіткого та розподіленого використання ресурсів один одного.

Другий підхід базується на забезпеченні фізичної інфраструктури, яка буде забезпечувати всі необхідні дії для вузлів мережі, наприклад маршрутизацію. Сенсорна мережа, що побудована за даним принципом, повинна використовувати певні базові станції, які будуть забезпечувати чітку інфраструктуру системи для взаємодії між сенсорними вузлами.

На відміну від звичайного вузла сенсорної мережі, базова станція має більші обчислювальні потужності та діапазони для прийому і передачі інформації. Зазвичай кожен вузол має прямий зв'язок з базовою станцією і обмінюється повідомленнями виключно з нею.

Часто сенсорні мережі розгортаються випадковим чином, тобто без підтримки певної чіткої фізичної інфраструктури. При такому підході алгоритми та протоколи, що використовуються в БСМ будуть на порядок складніші та тяжчі в реалізації, оскільки сенсорні вузли повинні самоорганізовуватися та взаємодіяти між собою без певної чіткої архітектури мережі. На практиці, значна частина мереж є поєднанням цих двох підходів. Тобто обидві інфраструктури можуть успішно функціонувати паралельно в одній мережі.

При побудові сенсорної мережі розгортання інфраструктури є дорогим та часто не можливим процесом. З іншого боку відсутність чіткої інфраструктури тягне за собою більш складний процес забезпечення інформаційного захисту сенсорної мережі. Це обумовлено тим, що всі необхідні дії, які стосуються інформаційної безпеки повинні автономно здійснюватися вузлами мережі на основі їх взаємодії та прав доступу.

При побудові сенсорних мереж на основі вищевказаних підходів необхідно зважати на три основні типи обладнання: координатор, маршрутизатор та шлюз, сенсорний вузол.

На найвищому рівні знаходиться координатор, який виконує процеси формування топології мережі, забезпечення централізованого управління мережею та центру інформаційного захисту. Тобто координатор встановлює та забезпечує політику інформаційного захисту, створює та розподіляє ключі безпеки мережі та створює налаштування на етапі приєднання сенсорних вузлів до мережі. Проте крім виконання функцій управління координатор забезпечує процеси вторинної обробки інформації: архівування, передачу за межі мережі, повторний аналіз та представлення у певному вигляді.

На другому рівні знаходяться маршрутизатор та шлюз, їх ще називають транзитними вузлами. Функціями даного обладнання є агрегування інформації, налаштування мережевих параметрів та під'єднання вузлів мережі. Маршрутизатор та шлюз координує зв'язок між сенсорними вузлами та координатором мережі, а також в деяких випадках здатен виконувати функції координатора кластеру.

Маршрутизатор кластеру збирає дані з сенсорних вузлів певного кластеру і передає їх до координатора, шляхом ретранслявання іншим маршрутизаторам. У разі збоїв в роботі мережі чи виходу з ладу певного мережевого обладнання, робота сенсорної мережі не буде припинена за рахунок здатності самостійного до переконфігурування мережі транзитними вузлами.

На найнижчому рівні знаходиться сенсорний вузол. Він здатен збирати та виконувати первинну обробку інформації і передавати її до найближчого маршрутизатора. Проте варто враховувати той факт, що ресурси сенсорних досить обмежені вимогами вартості та розмірів. Одним із найбільших обмежень є обмеження в енергоспоживанні, через неможливість дозаряджання сенсорних вузлів.

Провівши аналіз основних типів обладнання підходи до методів побудови сенсорної мережі також можна розділити на дві групи:

- Мережі з кількома головними вузлами. При такій концепції, вузли сенсорної мережі не тільки збирають інформацію про стан об'єкту моніторингу, а й отримують її від інших вузлів мережі і передають та ретранслюють її далі;
- Мережі з одним головним вузлом. В цьому випадку сенсорний вузол передає зібрану інформацію безпосередньо до центру керування мережею, проте для цього передавач сенсорного вузла повинен мати достатню потужність;

До особливостей мережі з одним головним вузлом можна віднести те, що для принцип її роботи базується на зібранні сенсором інформації і передачі до базової станції. Для цього необхідне встановлення на сенсорних вузлах потужних прийомопередавачів, що в свою чергу потягне за собою значні енергозатрати на сенсорному вузлі. Також варто зазначити той факт, що у випадку відмови в роботі головного вузла вся сенсорна мережа не зможе коректно працювати або повністю припинить свою роботу. Тому до недоліків таких мереж можна віднести високу вартість та енергоспоживання сенсорного вузла, невелику масштабованість та низьку надійність.

Для сенсорних мереж з кількома головними вузлами варто зазначити те, що вони не використовують високі швидкості передачі, при цьому забезпечуючи незначні затримки в процесі передачі. Також вони мають не високу вартість та енергоспоживання сенсорного вузла.

Тобто, провівши порівняльний аналіз, ми можемо сказати, що сенсорні мережі з кількома головними вузлами є більш ефективними ніж мережі з одним головним вузлом. Їх перевагами є те, що сенсорні вузли збирають інформацію про стан об'єкту моніторингу, отримують її від своїх сусідів, та передають далі шляхом ретрансляції. Також до їх переваг варто віднести той факт, що вузли здатні адаптуватися відповідно до змін в мережі та створювати певні зв'язки між вузлами, відповідно до стану всієї мережі.

Тому під час розробки інфраструктури сенсорної мережі слід враховувати фактор мінімізації енергоспоживання. Це, в свою чергу, призводить до ускладнення обчислювальних та комунікаційних здатностей сенсорних вузлів.

2.3 Аналіз методів забезпечення достовірності інформації

Враховуючи обмеження в невеликих обчислювальних потужностях вузлів БСМ та їх автономне живлення, постає проблема забезпечення необхідного рівня надійності роботи БСМ. Також негативним фактором для забезпечення достовірності інформації в сенсорних мережах є спосіб її передачі шляхом ретрансляції від одного вузла до іншого. Тому для надійної роботи сенсорної мережі постає необхідність забезпечувати надійну та енергоефективну передачу даних на каналному рівні.

Основним методом підвищення достовірності даних та надійності передачі є використання схем контролю помилок. Ці схеми забезпечують надійний зв'язок в безпроводному каналі, де можуть виникнути помилки через перешкоди або завмирання. За рахунок цих помилок пошкоджується цілісність пакетів даних на каналному рівні. Також до збільшення помилок призводить невелика потужність передавача через автономне живлення вузла.

Отже для забезпечення надійного рівня достовірності необхідно застосовувати способи підвищення надійності на каналному та фізичному рівнях. Для забезпечення надійності на каналному рівні використовують схеми контролю помилок. До схем контролю помилок можна віднести:

- управління потужністю прийомопередавача;
- пряме виправлення помилок;
- автоматичний запит повторної передачі;

2.3.1 Управління потужністю прийомопередавача

Прийомопередавачі, якими обладнані сенсорні вузли, здатні передавати сигнал на чотирьох рівнях потужності, які встановлюються і змінюються відповідно від стану каналу для передачі даних. Під час збільшення потужності передачі прийомопередавача спостерігається покращення співвідношення сигнал-шум, що в свою чергу призводить до зменшення частоти помилок. Проте збільшення потужності передачі призводить до збільшення енергоспоживання вузла. Також варто зазначити, що застосування механізмів управління потужністю прийомопередавача потребує збільшення обчислювального ресурсу та об'єму пам'яті для мікроконтролера, а також ускладнює протоколи обміну даними.

2.3.2 Пряме виправлення помилок

Пряме виправлення помилок базується на використанні коректуючих кодів, які, за рахунок додання контрольних символів, забезпечують виправлення помилок.

На рисунку 2.2 зображено приклад прямого виправлення помилок. Розглянемо коректуючий код (n,k,t) , де n - загальна довжина коду, k - кількість інформаційних бітів, які можуть бути виправлені до t бітів без повторної передачі пакетів [6].



Рис.2.2. Приклад прямого виправлення помилок [6]

Проте варто зазначити, що використання коректуючих кодів призводить до збільшення енергозатрат вузла та зменшення корисної пропускної здатності.

Тому варто зазначити, що під час використання коректуючих кодів варто враховувати швидкість коду, яка створює надлишковість та визначає тяжкість алгоритмів кодування/декодування.

Використовуючи літературні джерела [5] можна побачити, що ймовірність помилок $BER > 10^{-4}$ при повторній передачі пакетів забезпечує більшу енергоефективність порівняно з використанням коректуючих кодів. Дана особливість спричинена тим, що при невеликій ймовірності помилок не завжди відбудеться повторна передача, а при використанні коректуючих кодів, надлишковість буде в кожному пакеті.

2.3.3 Автоматичний запит повторної передачі

Автоматичний запит повторної передачі використовується для контролю кількості помилок. В основі його роботи лежить принцип автоматичного запиту повторної передачі, який періодично робить службові запити щоб знайти пошкоджені або втрачені пакети. Цей метод додає до вже існуючого пакету ще один службовий заголовок, де вказує алгоритм процесу виявлення помилок, з якомога меншою обчислювальною складністю та вихідні дані вузла. Контроль цілісності пакетів даних у відповідності зі стандартом IEEE 802.15.4, здійснюється на основі циклічного надлишкового коду (Cyclic Redundancy Check, CRC). Перевірочна послідовність (Frame check sequence, FCS) складає 16 біт. Розраховується вона по заголовку MAC (MHR) та частини кадру (MAC payload) (рисунок 2.3) [7].

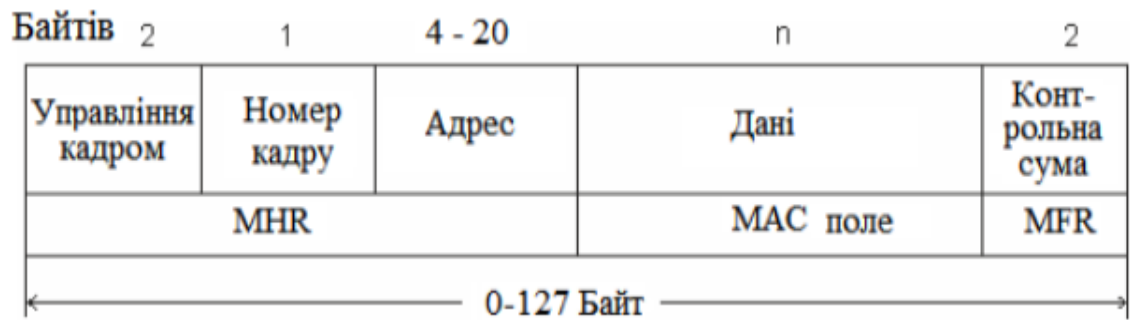


Рис.2.3. Структура фрейму даних стандарту IEEE 802.15.4 [7]

Застосування надлишкового циклічного коду дає змогу виявити присутність помилки в певних пакетах даних. Вузол, який приймає такі пакети буде діяти відповідно до наступної послідовності:

- 1) Обчислити контрольну суму прийнятих бітів кадру;
- 2) Порівняє обчислену суму з контрольною сумою отриманого пакета;
- 3) Відправить вузлу передавачу повідомлення з інформацією про цілісність пакета. У випадку виявлення помилки він відправить запит на повторну передачу пошкодженого або втраченого пакету;

Тобто вказаний метод базується на відправці позитивного підтвердження прийому, якщо пакет був прийнятий без помилок, або відправці негативного підтвердження, при виявленні пошкодженого або втраченого пакета. При передачі позитивного підтвердження, передавач встановлює визначений таймер для виявлення сигналу про надходження пакету. Якщо передавач передає повідомлення про пошкодження пакету, автоматично відправляється запит на повторну передачу вказаного пакету. Запит на повторну передачу можна поділити на 3 типи:

- 1) Повторити передачу N пакетів;
- 2) Повторити передачу вибраних пакетів;
- 3) Зупинити передачу та очікувати;

При запиті першого типу здійснюється повторна передача в кількості N пакетів. У випадку, коли пакет підтвердження не надійшов всі пакети повторно передаються. При запиті на повторну передачу другого типу,

передавач передає тільки вказані пакети, тобто ті на які не було отримано підтвердження. Третій тип запиту передбачає зупинення передачі до моменту отримання пакету про підтвердження і тільки після цього відправляє наступний пакет.

Проте варто зазначити, що використання методу автоматичного запиту повторної передачі є неефективним з точки зору енергозатрат вузла. Так наприклад для передачі 1 біта інформації енергозатрати близькі до виконання 1000 операцій в звичайному процесорі сенсорного вузла. Тобто вказаний метод вносить додаткові втрати на передачу та погіршує пропускну здатність мережі.

2.4 Аналіз методів інформаційного захисту БСМ

Забезпечення надійного рівня інформаційного захисту є важливим для всіх сенсорних мереж. Проте проектуючи сенсорні мережі для моніторингу стану об'єктів спеціального призначення дане питання постає набагато гостріше і набуває ключового характеру. Використовуючи сенсорну систему для моніторингу спеціальних об'єктів недооцінювання факторів її інформаційної безпеки може призвести до тяжких або навіть катастрофічних наслідків. Тому для мінімізації ризиків необхідно прийняти всі міри для ускладнення чи унеможливлення протиправних дій стосовно системи моніторингу. На практиці для забезпечення надійного рівня інформаційної безпеки існує два основні напрямки. Перший це забезпечення захисту та правильності маршрутизації, а другий це забезпечення захисту даних які циркулюють в сенсорній мережі. Тому перший напрямок передбачає використання захищених протоколів маршрутизації, інший потребує використання схем шифрування та відповідних схем розподілу ключів. Проте варто зазначити, що забезпечення вказаних методів без використання додаткових протоколів безпеки матиме не високу ефективність. Тому найефективнішим буде використання комплексу захищеної маршрутизації, шифрування з відповідним розподілом ключів та певних протоколів безпеки.

Далі проведемо аналіз цих існуючих методів забезпечення інформаційної безпеки в БСМ.

2.4.1 Аналіз протоколів захищеної маршрутизації сенсорної мережі

Відомі протоколи маршрутизації в сенсорних мережах оптимізовані для використання при певних обмеженостях сенсорних вузлів та характеру мережі, проте вони частково або повністю не враховують питання інформаційного захисту системи. При розробці більшості стандартних протоколів маршрутизації використовувався принцип, що вузли сенсорної мережі будуть «дружелюбними», а забезпечити безпечне функціонування сенсорних мереж можна за рахунок використання чи модернізації відомих методів шифрування. Проте варто зазначити, що інформаційний захист мережових передач без використання захищеної маршрутизації не принесе цілковитого рівня інформаційної безпеки всієї сенсорної мережі. Тому для забезпечення надійності рівня безпеки слід використовувати дві відповідні точки: перша це захист передачі даних, інша це забезпечення безпеки маршрутизації. Далі ми проведемо аналіз відомих спеціальних протоколів маршрутизації, які спроектовані для забезпечення надійного рівня інформаційної безпеки.

Secure Efficient Ad hoc Distance vector routing protocol (SEAD)

Даний протокол базується на використанні векторної відстані маршрутизації. В основі роботи цього протоколу лежить застосування ефективних односторонніх хеш-функцій. Особливістю роботи SEAD є використання спеціальних порядкових номерів призначення, це дозволяє уникнути довготривалих циклів маршрутизації та забезпечує додатковий захист від відтворення зловмисником службових повідомлень оновлення маршрутизації.

При забезпеченні безпеки маршрутизації вказаний протокол частково ефективний, проте він створює великі накладні втрати, через збільшення

службових повідомлень про маршрутизацію та збільшення розміру самих службових повідомлень через додавання хеш-запису для автентифікації.

Ariadne

В основі роботи даного протоколу лежить використання симетричної криптографії. Цей протокол створює та автентифікує маршрутизацію використовуючи такі схеми:

- 1) спільний секрет між певною парою вузлів
- 2) спільні секрети між вузлами, що поєднуються в певні групи
- 3) «цифрові підписи» вузлів

За рахунок використання спільних ключів для певних пар вузла зникає необхідність точної синхронізації між вузлами, проте виникають більші втрати вузла для налаштування ключів автентифікації.

Authenticated routing for ad hoc networks (ARAN)

В основі роботи протоколу лежить використання криптографічних сертифікатів, що гарантують наскрізну автентифікацію. При використанні даного протоколу кожен вузол має сертифікат, який пов'язує його ідентифікатор з відкритим ключем. Використання криптографічних сертифікатів дає змогу запобігти більшості відомих атак на БСМ та виявляти нестійкі стани в мережі. Принцип роботи цього протоколу складається з процесу попередньої сертифікації та подальшого процесу створення екземпляру маршруту, який гарантує автентифікацію в процесі прийому. Виявлення маршруту в ARAN виконується за допомогою широкомовного повідомлення від вихідного вузла, на яке може відповісти тільки вузол призначення. Повідомлення маршрутизації є наскрізним і тому тільки авторизовані вузли можуть приймати участь в кожному транзитному сегменті сенсорної мережі між вихідним вузлом та вузлом призначення. Враховуючи той факт, що вказаний протокол витрачає більше часу та ресурсів на перевірку підписів, варто зазначити, що його енергоефективність

менша ніж в протоколів, які використовують хеш-ланцюги. Недоліком протоколу є великі об'єми пакетів маршрутизації, що призводить до збільшення загального навантаження маршрутизації та збільшення затримки в побудові маршруту.

Secure Ad hoc On-demand Distance Vector routing protocol (SAODV)

Цей протокол маршрутизації використовує хешоване повідомлення як алгоритм автентифікації. Принцип його роботи полягає в використанні підписів для автентифікації поля запиту маршруту (RREQ) і поля відповіді маршруту (RREP) та використанні хеш-ланцюжка для автентифікації кількості переходів в процесі маршрутизації. Відправник повідомлення обирає максимальне число транзитних сегментів мережі на основі приблизного очікуваного розміру мережі та генерує односторонній хеш-ланцюг, довжина якого складає максимальну кількість переходів плюс один. Цей односторонній хеш-ланцюг використовується в якості метричного автентифікатора. В ньому не передбачається використання криптографії, що забезпечує швидку перевірку повідомлень, автентифікацію проміжних вузлів та автентифікацію повідомлень. Цей протокол мінімізує затримки в часі та накладні витрати на управління службовими пакетами.

Secure Link-State Protocol (SLSP)

Даний протокол використовує технологію цифрового підпису вузла та односторонні хеш-ланцюги для забезпечення безпеки оновлення статусу каналу. SLSP може працювати при відсутності або мінімальній взаємодії з центром управління ключами. Він приймає інформацію про стан з'єднань через періодичний протокол місцезнаходження сусідів. Як складова протоколу місцезнаходження сусідів, кожен вузол здійснює широкомовну передачу повідомлення про зв'язок його IP та MAC. Цей протокол попереджує систему про неправильне використання таких зв'язок. Наприклад коли дві різних MAC-адреси використовують один IP або навпаки.

Повідомлення про оновлення статусу каналу підписуються цифровим підписом і розсилається обмеженій частині транзитних сегментів мережі. Щоб уникнути розсилки про оновлення певного каналу на транзитні вузли, які до нього не належать, кожне таке оновлення включає в себе чітку кількість визначених транзитних сегментів мережі. Як і в інших спеціальних протоколах маршрутизації, тут хеш-ланцюг використовується для автентифікації лічильника переходів маршрутизації, значення хеш-ланцюга автентифікується за рахунок включення цієї інформації в повідомлення про оновлення каналу. Тобто для ефективної роботи при відсутності централізованого керування ключами SLSP дозволяє кожному вузлу мережі розподіляти відкритий ключ між своїми сусідами. Так вузли періодично передають свій сертифікований відкритий ключ таким чином, що вузли призначення мають змогу перевірити наступні повідомлення про оновлення статусу каналу. Під час зміни топології сенсорної мережі її вузли отримують інформацію про ключі вузлів, які приєднуються до їхньої частини мережі, тобто стають їх сусідами. Таким чином досягається можливість відстеження граничної кількості ключів в кожному сегменті мережі.

2.4.2 Аналіз існуючих методів шифрування та методів керування ключами

Одним з ключових аспектів при забезпеченні інформаційної безпеки сенсорних мереж є правильність вибору методів шифрування та протоколів керування ключами. Під керуванням ключами варто розуміти встановлення певних ключів між вузлами сенсорної мережі для подальшого захищеного обміну інформацією між ними та додавання нових вузлів до всієї сенсорної мережі. Вибір правильного методу шифрування має життєвоважливе значення для сенсорних мереж. Це зумовлено тим, що основна частина аспектів інформаційної безпеки забезпечується методами шифрування. Проте при виборі відповідного шифрування варто враховувати обмеження сенсорних вузлів, розмір коду, час обробки та загальне енерговикористання.

На сьогодні відомо два основні методи шифрування: шифрування на основі відкритого ключа та шифрування на основі симетричного ключа.

Враховуючи розмір коду, розмір даних, час обробки та енерговикористання більш доцільним та ефективним буде використання в сенсорних мережах методу шифрування на основі симетричного ключа. Варто зазначити, що методи шифрування з відкритим ключем мають високу обчислювальну інтенсивність і зазвичай виконують тисячі або навіть мільйони команд множення для виконання однієї операції безпеки. Провівши певні дослідження можна вказати, що алгоритми з відкритим ключем затрачують від десятка секунд і майже до хвилини для виконання операцій шифрування та дешифрування в БСМ. З іншого боку алгоритми на основі шифрування з симетричним ключем або на основі хеш-функцій вимагають набагато менше обчислювальних потужностей та витрачають на багато менше час для виконання цих операцій. Для порівняння в таблиці 2.1 приведений середній час, необхідний для виконання операції шифрування.

Таблиця 2.1 Середній час необхідний для виконання операції шифрування різними методами шифрування

Алгоритм шифрування	Час в секундах
З відкритим ключем	
ECC secp160r1	0.81
ECC secp224r1	2.19
RSA-1024 public-key $e = 2^{16} + 1$	0.43
RSA-1024 private key w. CRT	10.99
RSA-2048 public-key $e = 2^{16} + 1$	1.94
RSA-2048 private-key w. CRT	83.26
З симетричним ключем	
Skipjack	0.00038
RC5	0.00026

Провівши порівняльний аналіз двох відомих методів шифрування варто зазначити, що вибір методу шифрування має основоположне значення для забезпечення інформаційної безпеки в сенсорних мережах. Проте вибір методу напряду залежить від обчислювальних потужностей та взаємозв'язків між вузлами мережі. Підводячи підсумки варто зазначити:

- Методи шифрування на основі відкритого вузла можуть мати практичне використання в сенсорних мережах, проте їх використання буде тяжким з точки зору обчислювальних та енергетичних затрат на вузлах сенсорної мережі;
- Методи шифрування на основі симетричного ключа переважають методи на основі відкритого ключа за рахунок меншого часу виконання операції шифрування і нижчими енергозатратами. Проте схеми розподілу симетричних ключів на даний момент не є досконалими і потребують подальшого розвитку;

Основною проблемою при симетричному розподілі ключів є правильний попередній розподіл. Тобто для встановлення зв'язку, всі вузли мережі мають знати необхідний симетричний ключ.

Часто в БСМ використовуються такі схеми розподілу симетричного ключа:

- Базовий розподіл;
- Випадковий розподіл ключів або так званий рандомний розподіл ключів;
- Створення парних ключів та попередній їх розподіл;
- Груповий розподіл ключів;
- Локальний розподіл ключів для деякої бази об'єднаних сенсорів;

Однак через те, що для нормального функціонування мережі кожен вузол повинен встановити зв'язок з своїми сусідніми вузлами та вузлами агрегації даних, виникає небезпека отримання доступу злоумисника до всієї мережі. Тобто, скомпрометувавши велику кількість вузлів, злоумисник може відновити весь пакет секретних ключів і розшифрувати дані.

2.4.3 Протоколи безпеки для сенсорних мереж

2.4.3.1 TESLA

TESLA (англ. Timed, Efficient, Streaming, Loss-tolerant Authentication

Protocol) та його розширення μ TESLA використовуються для забезпечення широкомовної автентифікації в сенсорних мережах. Для нормального функціонування цього протоколу базова станція та вузли мають бути синхронізовані по часу та кожен вузол повинен знати максимальну помилку синхронізації. Для забезпечення широкомовної автентифікації існує необхідність джерела асиметрії, тому приймачі можуть лише перевірити інформацію про автентифікацію та не можуть її згенерувати. В основі цього протоколу лежить те, що всі приймачі вільно синхронізовані по часу з відправниками з указанням верхньої межі помилки синхронізації. Основні етапи роботи можна описати наступним чином:

- Відправник створює часові інтервали однакової довжини та формує однонаправлений ланцюг значень для самоідентифікації, після чого присвоює кожному інтервалу певне значення ключа. Відправник також визначає час відкриття значень цього ланцюга, зазвичай це відбувається в декількох часових інтервалах;
- Відправник прикріплює message authentication codes (MAC) до кожного пакету, на основі вмісту цього пакету. Для кожного пакета визначається часовий інтервал і використовується відповідне значення з ланцюга в якості криптографічного ключа для визначення MAC. Після чого відправник відправляє пакет з останніми значеннями одностороннього ланцюга;
- Приймавши пакет, приймач знає графік розкриття ключів. Враховуючи той факт, що всі вузли вільно синхронізовані по часу, приймач може перевірити те чи ключ, на основі якого обчислювався MAC все ще секретний. Це досягається за рахунок визначення того чи міг відправник досягти часового інтервалу після якого цей ключ

розкриється. У випадку якщо ключ все ще секретний і не відкритий, отримувач буферизує пакет;

- Приймач перевіряє правильність розкритого ключа на основі самоавтентифікованих та раніше випущених ключів. Потім перевіряє правильність MAC буферизованих пакетів. Якщо MAC вірний, приймач приймає пакет;

Перевагою одностороннього ланцюга є те, що у випадку коли якісь його проміжні значення втрачаються їх повторно вирахувати на основі подальших значень. Тобто, навіть у тому випадку коли деякі розкриті ключі були втрачені, приймач може відновити послідовність цих ключів і перевірити правильність пакетів.

Підводячи підсумки, можна зазначити, що протокол TESLA та його розширення мають наступні переваги:

- Низькі енергозатрати на обчислення для генерації та перевірки інформації про автентифікацію;
- Низькі енерговитрати для забезпечення зв'язку;
- Своєчасна автентифікація для кожного окремого пакета через можливість буферизації повідомлень;
- Стійкість до втрати пакетів;
- Масштабованість на велику кількість приймачів;

2.4.3.2 SNEP

SNEP (Secure Network Encryption Protocol) використовують для забезпечення конфіденційності даних, двосторонньої автентифікації і актуальності даних для однорангового зв'язку (від вузла до базової станції). В основу цього протоколу покладено механізми двосторонньої автентифікації та забезпечення цілісності даних. Відповідно до механізму роботи цього протоколу зашифровані дані будуть мати наступний вигляд: $E = \{D\}_{(K_e, C)}$, а MAC $M = MAC(K_M, C|E)$, тоді повне повідомлення від вузла А до вузла В матиме вигляд:

$$A \rightarrow B: \{D\}_{(K_e, C)}, \text{MAC}(K_M, C | \{D\}_{(K_e, C)}), \quad (2.9) [8]$$

де D – дані;

K_e – ключ шифрування;

C – лічильник;

Проте через те що SNEP тільки примусово встановлює порядок відправки повідомлення у вузлі В, але не гарантує, що це повідомлення створене у відповідь на подію у вузлі А. Тому вузол А випадковим чином генерує N_A і разом із запитом відправляє його до вузла В. Після цього, вузол В відсилає до А відповідь наступним чином:

$$A \rightarrow B: N_A, R_A \quad (2.10) [8]$$

$$B \rightarrow A: \{R_B\}_{(K_e, C)}, \text{MAC}(K_M, N_A | C | \{R_B\}_{(K_e, C)}) \quad (2.11) [8]$$

В такому випадку, якщо перевірка показує, що MAC правильний це означає, що вузол В згенерував відповідь після запиту з вузла А.

До переваг використання цього протоколу можна віднести:

- Одне і те ж повідомлення кожен раз шифрується по різному, за рахунок того, що значення лічильника збільшується після кожного повідомлення. Це забезпечує семантичну безпеку;
- Невеликі енерговитрати досягаються за рахунок того, що значення лічильника зберігається і не потребує відправки в кожному повідомленні;
- Значення лічильника в MAC запобігає відтворенню минулих повідомлень;
- При правильній автентифікації MAC можна бути цілком впевненим, що повідомлення надійшло від легального відправника, чим і забезпечується автентифікація даних;

2.4.3.3 SPINS

SPINS представляє собою об'єднання двох протоколів SNEP та μTESLA. SNEP підтримує широкомовну передачу та наскрізний захист, а

μTESLA забезпечує автентифікацію широкомовної передачі. Основна відмінність від окремого використання цих протоколів полягає в тому, що під час їх об'єднання SNEP використовує спільний лічильник для відправника та отримувача, а μTESLA обмежує довжину MAC до 8 байт, а ключ відкривається всього один раз. За рахунок такого об'єднання досягається зниження енерговитрат для зв'язку та зменшення об'єму зберігання даних. За рахунок використання симетричної криптографії зменшуються енерговитрати обчислення. Для збереження ресурсів вузла μTESLA зберігає ланцюг ключів на базовій станції і виконує широкомовну передачу через неї ж.

SPINS передбачає, що розподіл всіх вузлів мережі відбувається на основі головного ключа K , який потім передається базовій станції. Всі інші ключі, такі як ключ шифрування K_E , ключ генерації випадкових чисел K_R та ключ для генерації MAC K_M , створюються на основі головного ключа за допомогою односторонньої функції. Цей протокол використовує метод шифрування RC 5 чим забезпечується надійний рівень конфіденційності. Процес передачі повідомлення від вузла A до вузла B виглядає наступним чином:

$$A \rightarrow B: \{D\}_{(K_E, C)}, MAC(K_M, C|D)_{K_E, C} \quad (2.12)$$

Після відправки та прийому кожного повідомлення на стороні приймача та передавача значення лічильника збільшується.

2.4.3.4 TinySec

TinySec протокол для захисту БСМ на каналному рівні. Базується на двох основних методах роботи: автентифікація та автентифіковане шифрування. Тобто можливе лише автентифікування або автентифікація та подальше кодування даних системи. В основі роботи протоколу лежить послідовність цифрових блоків і восьмибайтовий вектор для шифрування. Автентифікація даних здійснюється за рахунок обчислень та перевірки MAC. Довжину MAC, в основному, вибирають 4 байти. Тобто для того щоб

зламати цю систему зловмиснику необхідно провести спроби згенерувати ключ та відправити до якогось авторизованого вузла щонайменше 2^{32} раз. Відправлення такої кількості повідомлень призведе до блокування системою передавача цих повідомлень.

Висновки до розділу:

В першій частині розділу був проведений аналіз існуючих методів збору інформації для БСМ. За результатами даного аналізу можна зазначити, що під час вибору кожного з методів відбуваються певні обмеження в її застосуванні. Використання методу збору даних на основі запитів підходить для неперервного моніторингу параметрів об'єкту моніторингу. Метод збору даних на основі події ефективна для відстеження зміни стану об'єктів або важливих подій. Адаптивні методи збору даних дозволяють досягти сенсорними мережами високого рівня самоорганізації. Але варто зазначити, що не має чіткого метод збору даних яка б підходила для універсального використання для моніторингу стану об'єктів спеціального призначення. Тому для таких мереж доцільно використовувати не якийсь окремий метод збору інформації, а їх комплекс. Такий комплекс дозволить об'єднати декілька моделей збору інформації для конкретних БСМ, проте слід враховувати, що використання такого комплексу призведе до підвищення складності алгоритмів побудови мережі.

В другій частині були розглянуті та проаналізовані існуючі підходи до побудови інфраструктури БСМ. Дані підходи можна поділити на дві групи:

- Підхід на основі фізичної інфраструктури;
- Підхід на основі кількості головних вузлів;

Кожен з цих підходів розкидає певні складності чи особливості в процесі проектування безпроводової сенсорної мережі. Проте варто зазначити, що метод вибору інфраструктури сенсорних мереж є одним з найважливіших етапів в процесі її проектування. Тому під час розробки інфраструктури сенсорної мережі слід враховувати фактор мінімізації

енергоспоживання, проте необхідно знайти певний компроміс з ускладненням обчислювальних та комунікаційних здатностей сенсорних вузлів.

В третій частині були проаналізовані способи підвищення достовірності інформації в сенсорних мережах. Даний аналіз показав, що проблема забезпечення достовірності інформації в сенсорних мережах є досить актуально в наш час. Під час методів побудови сенсорної мережі, направлених на покращення достовірності інформації необхідно враховувати наступні параметри вузла: невеликі об'єми пам'яті, низьке електроживлення та відсутність інтелектуальної складової. Тобто використання вказаних методів покращення достовірності інформації може призвести до стрімкого зростання вартості та енергоспоживання вузла та збільшення фізичного впливу завад, що виникають в каналах зв'язку.

Також в цьому розділі були проаналізовані основні існуючі методи забезпечення інформаційної безпеки сенсорних мереж. До таких методів можна віднести використання захищеної маршрутизації, забезпечення відповідного методу шифрування та схем розподілу ключів та використання відомих протоколів безпеки сенсорних мереж. Варто зазначити, що використання вказаних методів окремо матиме набагато меншу ефективність ніж використання комплексів з цих методів

Проте основною проблемою при побудові сенсорних мереж для моніторингу об'єктів спеціального призначення є жорстко обмежені обчислювальні ресурси. Для економії енергії вузли майже завжди знаходяться у сплячому режимі і на зв'язок виходять тільки періодично. Крім того, сенсорні мережі розгортаються на великих територіях з кількістю вузлів порядку декілька сотень. Це означає, що під час розробки сенсорної мережі необхідно звернути особливу увагу на мінімізацію споживання енергії, що може бути забезпечено відповідними протоколами передачі даних.

Варто зазначити, що при побудові сенсорних мереж для їх використання на об'єктах спеціального призначення необхідно знайти певний компроміс між їх правильним та безвідмовним функціонуванням та жорстким обмеженням вузлів цієї мережі відповідними ресурсами.

3. МЕТОДИКА ПОБУДОВИ СЕНСОРНОЇ МЕРЕЖІ МОНІТОРИНГУ СТАНУ ОБ'ЄКТІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В цьому розділі запропоновано нову методику побудови сенсорної мережі для функціонування на атомній електростанції. Сьогодні атомна електроенергетика забезпечує основну частину електроенергії, яка необхідна людству. Через особливості роботи та безпеку в разі аварії такі системи потребують безперервного та надійного моніторингу їх стану та стану навколишнього середовища. Тобто існує гостра необхідність забезпечення чіткого контролю за станом таких станцій. Для цього контролю доцільно використовувати БСМ. Запропонована сенсорна система забезпечить надійний моніторинг за такими параметрами, як: радіаційний рівень на території АЕС та навколо неї; температура та радіаційне забруднення охолоджувальних рідин та басейнів та стан всередині енергоблоків.

3.1 Визначення цілей та основних параметрів запропонованої БСМ

Враховуючи той факт, що запропонована БСМ буде працювати на атомній електростанції її основні цілі та параметри будуть дещо специфічними. Варто зазначити, що проектування такої сенсорної мережі є на порядок складнішим ніж проектування звичайних БСМ та потребує надійного забезпечення основних цілей. До таких цілей функціонування БСМ на АЕС можна віднести:

- Своєчасний збір інформації та надійне і оперативне детектування подій;
- Чітка та відмовостійка маршрутизація;
- Забезпечення інформаційної безпеки;
- Енергоефективність;

Перша ціль обумовлена тим, що сенсорна мережа повинна своєчасно та безпомилково реагувати на зміну стану об'єкту моніторингу. Тобто при спостереженні за атомною електростанцією правильність та оперативність

виявлення інформації є критично важливим питанням, адже у протилежному випадку це може мати тяжкі або навіть катастрофічні наслідки. Наприклад для контролю та керування інтенсивністю протікання ядерних реакцій в енергоблоці використовуються графітові стержні, які вводяться в активну зону реактора. Тобто при виявленні підвищення допустимого рівня атомних реакцій в певному енергоблоці, туди вводяться графітові стержні, тим самим уповільнюючи інтенсивність протікання реакції. Тому сенсорні датчики повинні своєчасно та надійно реагувати на зміни параметрів всередині енергоблоку, оперативно детектуючи зміни температури, тиску, рівня радіації та інших відповідних показників. Для забезпечення цієї вимоги необхідно чітко визначити методи збору інформації сенсорною мережею.

Необхідність чіткої та відмовостійкої маршрутизації обумовлена тим, що сенсорна мережа повинна надійно та своєчасно обмінюватися повідомленнями між вузлами. Наприклад при детектуванні певної події, інформація про це повинна бути доставлена до центру керування, якомога швидше та не повинна бути втрачена, тобто існує необхідність визначення найкоротшого шляху між відправником та одержувачем при заданому рівні якості. Також до основних задач маршрутизації необхідно віднести можливість створення нових маршрутів при втраті вже існуючих.

І чи не найважливішим є питання забезпечення надійного рівня інформаційної безпеки. Використовуючи сенсорну систему на АЕС недооцінювання факторів її інформаційної безпеки може призвести до тяжких або навіть катастрофічних наслідків. Так наприклад отримавши доступ до сенсорної мережі зловмисник може навмисно змусити її неправильно функціонувати або отримати доступ до секретної інформації. Тому для мінімізації ризиків необхідно прийняти всі міри для ускладнення чи унеможливлення протиправних дій стосовно системи моніторингу. Також варто зазначити, що ефективний інформаційний захист АЕС варто розглядати як важливий комплекс заходів забезпечення не лише ядерної та

радіаційної безпеки, але і як основу екологічної, економічної та інших видів безпеки, стратегічно важливих для держави і суспільства [18].

Проте основна складність при забезпеченні всіх вищевказаних цілей є обмеженість ресурсами сенсорного вузла. А саме обмеження в ресурсах пам'яті, енергії, швидкостях передачі та якісних алгоритмах обробки великої кількості даних.

На основі проведеного аналізу основних цілей функціонування БСМ на АЕС можна визначити основні параметри сенсорної системи, які необхідно розробити. До таких параметрів варто віднести:

- Структура сенсорної мережі;
- Склад сенсорного вузла;
- Надійний і своєчасний збір інформації та оперативне і правильне детектування подій;
- Надійність маршрутизації;
- Високий рівень інформаційного захисту;

3.2 Розробка структури сенсорної мережі та складу сенсорного вузла

На сенсорній мережі для функціонування на АЕС запропоновано використовувати структуру мережі, яка передбачає три основних пристрої: кінцевий сенсорний вузол, маршрутизатор та центр керування. Центр керування виконує функції управління всією сенсорною мережею та обробки отриманої інформації про стан АЕС. Також центр керування, в разі виявлення якихось значущих подій, передає цю інформацію відповідним системам реагування, наприклад системі управління графітовими стержнями для врегулювання потужності реакцій в енергоблоці або навіть системі аварійної зупинки енергоблоку чи представляє цю інформацію оператору сенсорної мережі, який уже і приймає відповідні рішення.

Маршрутизатори виконують функції збору інформації, отриманої від сенсорних вузлів та передачі її до базової станції. Враховуючи той факт, що

сенсори можуть встановлюватися в місцях з неможливістю проходження електромагнітних хвиль, наприклад в екранованих енергоблоках маршрутизатори та частина вузлів можуть мати як проводований так і безпроводовий зв'язок.

Кінцевий сенсорний вузол слугує для моніторингу параметрів на АЕС та передачі цієї інформації до центру управління. Для надійного моніторингу та зменшення навантаження на всю сенсорну систему на АЕС пропонується використовувати три типи сенсорних вузлів:

1. Сенсорний вузол для моніторингу рівня радіації на території АЕС та територіях навколо неї. Вузли цього типу пропонується обладнати сенсорами рівня радіації.
2. Сенсорний вузол для моніторингу температури охолоджуючих рідин і басейнів та рівня радіації в них. Такі вузли необхідно обладнати сенсорами рівня радіації та температурними сенсорами.
3. Сенсорний вузол для безпосереднього моніторингу стану всередині енергоблоку. Такі вузли необхідно обладнати сенсорами рівня радіації, тиску та температури.

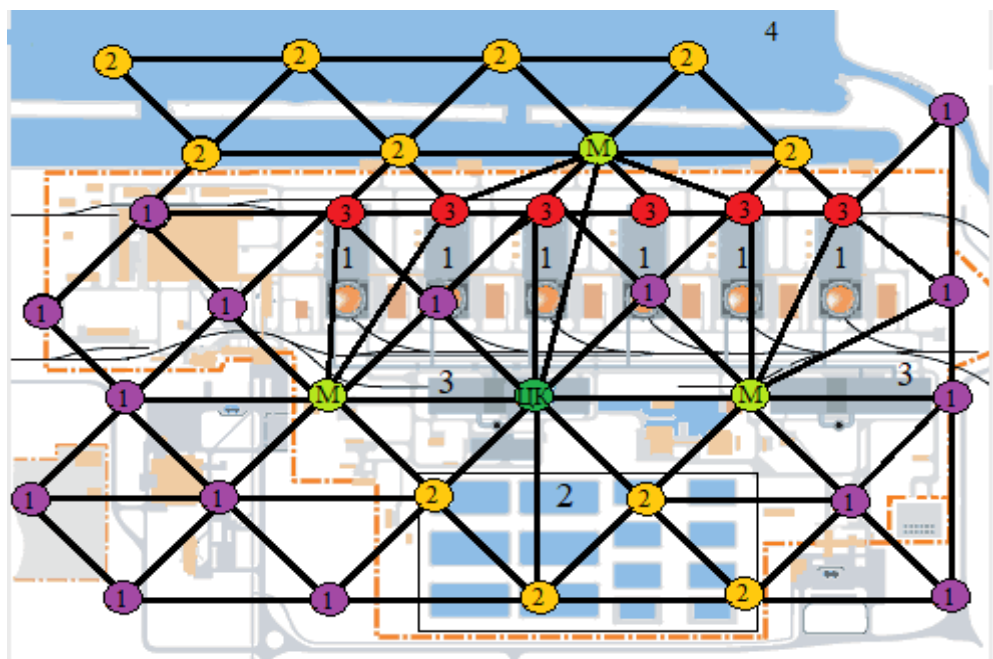


Рис. 3.1. Структура запропонованої сенсорної мережі на АЕС

На рисунку 3.1 приведено приклад структури БСМ для функціонування на АЕС. Умовні позначення:

- 1 – Енергоблоки;
- 2 – Охолоджувальні басейни;
- 3 – Технічні корпуси;
- 4 – Охолоджувальне водосховище;
-  - центр керування сенсорною мережею;
-  - маршрутизатор;
-  - сенсорний вузол першого типу;
-  - сенсорний вузол другого типу;
-  - сенсорний вузол третього типу;

На рисунку 3.2 представлено структурну схему сенсорного вузла.

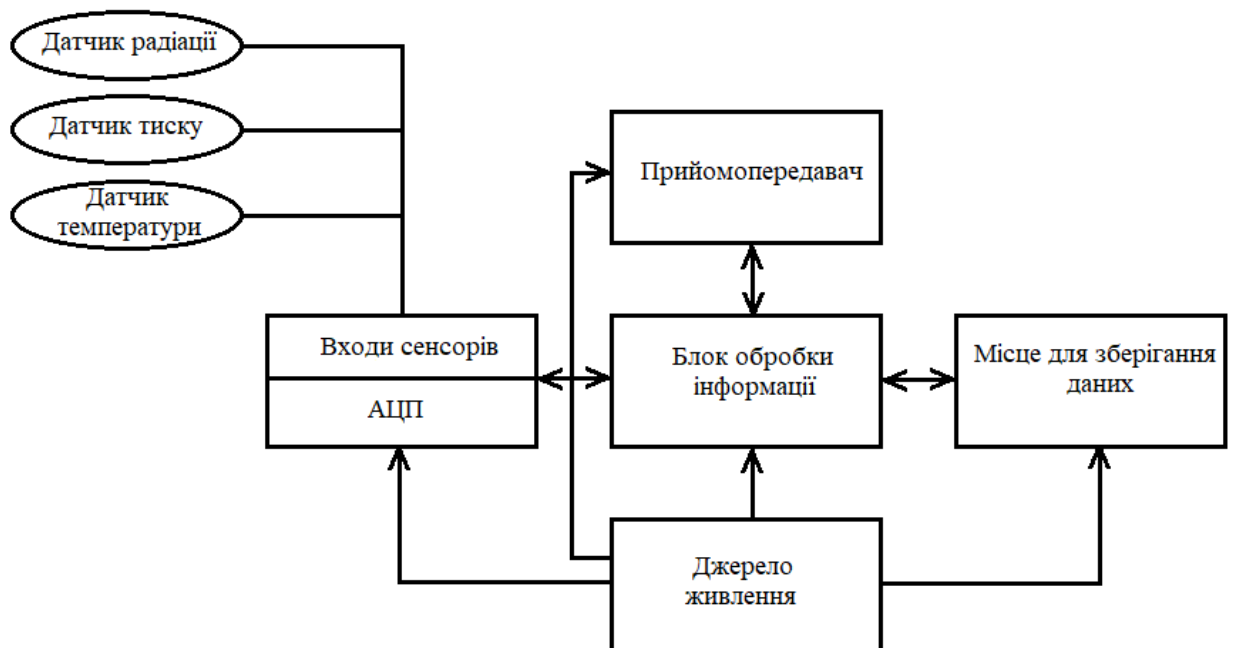


Рис.3.2. Структурна схема сенсорного вузла

3.3 Визначення методу збору даних

Метод збору даних в сенсорній мережі для моніторингу стану об'єктів спеціального призначення має важливе значення. Це обумовлено тим, що при спостереженні за спеціальними об'єктами правильність та оперативність

виявлення інформації є критично важливим питанням, адже у протилежному випадку це може мати тяжкі або навіть катастрофічні наслідки. Тому від правильності вибору методу збору даних залежить чіткість та оперативність виявлення зміни станів об'єкту моніторингу.

Приведений в попередньому розділі порівняльний аналіз відомих методів збору інформації показав, що універсальної моделі не існує, і кожен з проаналізованих методів накладає на мережу певні обмеження. Тому варто зазначити, що доцільно використовувати не якийсь окремий метод, а комплекс з кількох. Використання такого комплексу дозволить підвищити ефективність збору даних, а також зменшити споживання енергії та час відповіді вузла. Також за рахунок такого комплексу можна підвищити рівень достовірності інформації, яка надходить від сенсорних вузлів.

Варто зазначити, що для надійного моніторингу об'єктів спеціального призначення необхідно мати можливість не лише детектувати значущі події, а й мати можливість спостерігати за параметрами та показниками сенсорної мережі, тобто мати можливість в будь-який момент часу оцінити загальний стан об'єкту моніторингу. Враховуючи це фактор в таких системах доцільно використовувати комплексний метод збору даних на основі методів збору за розкладом та за подією. В основі роботи такого комплексного методу лежить те, що сенсорний вузол працює в режимі збору інформації за певним розкладом, при виявленні якоїсь події він відправляє повідомлення про детектування до головного вузла, після чого при відсутності якихось вимог переходить до збору інформації на основі розкладу.

Процес виявлення події є надзвичайно складним завданням і залежить від конкретної сенсорної мережі та об'єкту моніторингу на який вона направлена. Тобто варто зазначити, що не існує універсального підходу до виявлення події, який би чітко та безвідмовно функціонував на всіх сенсорних мережах спеціального призначення. Проте ми можемо створити приблизний його алгоритм, параметри якого будуть доопрацьовуватись чи

змінюватись відповідно до сенсорної системи, на якій він буде використовуватись.

Зазвичай детектування події відбувається на основі того, що виміряне значення перевищує встановлений поріг. Визначений поріг може встановлюватися для відповідного вузла вручну, ще на етапі розгортання мережі, або може бути встановлений на основі статистичних даних, зібраних вузлом. Наступним етапом після виявлення перевищення значенням порогу є класифікація цієї події, тобто визначення того чи справді відбулась якась подія чи відбулось якесь помилкове детектування. Під час такого визначення обробка даних лише одним вузлом може бути нечіткою або упередженою внаслідок зміни навколишнього середовища. Тому доцільним буде використовувати спільне виявлення події декількома сенсорними вузлами для підтвердження або не підтвердження виявлення події.

Спільне виявлення події виконується певною групою сенсорних вузлів, які для підвищення ефективності детектування події обмінюються цими даними між собою. Тобто окремо жоден вузол не приймає рішення, а воно виникає як результат колективного процесу обробки даних. Тобто сигнал про виявлення події надсилається в центр керування мережею лише після підтвердження цієї події від певної групи сенсорних вузлів. На цьому етапі постає питання чіткого розподілу мережі на певні групи, від яких і буде залежати правильність обраного рішення. Питання ефективного розподілу на групи можна вирішити за рахунок кластеризації мережі. За рахунок розподілу мережі на кластери можна уникнути того факту, що кожен активний вузол чи група вузлів буде надсилати до центру керування сигнали про виявлення однієї і тієї ж події, що в свою чергу призведе до навантаження на канали передачі і викличе додаткові енергетичні затрати. При спільному виявленні події на основі кластеру порядок виявлення події виглядає наступним чином. Сенсорний вузол, який виявив перевищення порогового значення надсилає повідомлення до голови кластера. Голова кластера після отримання цього повідомлення надсилає сигнали для зняття

відповідних показників сусідам вузла, який виявив подію. Після отримання результатів, головний вузол кластера робить висновок про детектування події і в разі її присутності відправляє інформацію базовій станції. За рахунок цього можна досягти підвищення точності виявлення події та зменшити кількість трафіку у всій сенсорній мережі.

3.4 Вибір протоколу маршрутизації

Під час проектування сенсорних мереж для функціонування на об'єктах спеціального призначення важливим є правильність вибору протоколу маршрутизації та його надійного захисту. Проте варто зазначити, що роль безпечної маршрутизації стане марною, якщо побудована на ній схема агрегації даних не передбачатиме свого інформаційного захисту. І навпаки, протокол безпечної агрегації даних потребує захищений базовий протокол маршрутизації в якості основи, щоб бути ефективним з точки зору інформаційного захисту. Враховуючи ці фактори можна запропонувати енергозберігаючий протокол на основі LEACH та ESPDA, який поєднує в собі безпечний протокол маршрутизації і безпечний протокол агрегації даних.

Варто зазначити, що надійний рівень функціонування та інформаційного захисту досягається саме за рахунок об'єднання та спільного використання цих двох протоколів. Так наприклад окреме використання LEACH стосується тільки енергоефективності маршрутизації. Хоча його рандомізована зміна головних вузлів кластеру по суті забезпечує захист вузлів агрегатора, він не бере до уваги аспект безпеки. Таким чином для захисту маршрутизації існує кілька додаткових схем, таких як SLEACH, SecLEACH, SC-LEACH, Armor LEACH і MS-LEACH. Основна ідея ESPDA полягає в тому, що замість прямої відправки фактичних даних в канал головного вузла, вузли датчиків спочатку відправляють свої коди шаблонів. Кодом шаблону є дані, що представляють виміряні дані, і генерується на основі секретного початкового числа шаблону, яке періодично поширюється

по каналу головного вузла. Потім головний вузол порівнює ці коди шаблонів, вибирає тільки унікальні і запитує фактичні дані у вузлів, які мають відповідні унікальні коди. У відповідь кожен обраний вузол потім відправляє зашифровані фактичні дані в канал, в той час як іншим може бути дана інструкція скинути дані. Головному вузлу не потрібно розшифровувати отримані зашифровані дані, тому що процес агрегування даних виконується до фактичної передачі даних. Це знижує накладні витрати і, таким чином, сприяє підвищенню енергоефективності. Енергоефективна агрегація даних на основі захищених шаблонів (ESPDА) працює з кластерними БСМ і підходить для протоколів безпечної маршрутизації на основі LEACH.

Принцип роботи об'єднання цих протоколів складається з двох фаз: фази налаштування кластеру та фази усталеного стану. Фаза налаштування - це етап, на якому завершується формування кластера. На початку цієї фази кожен вузол, який хоче стати головним вузлом кластеру в наступному раунді, транслює початкове повідомлення, що містить його ідентифікатор. Після отримання цих повідомлення, вузол, який хоче приєднатися до кластеру, відправляє назад повідомлення запиту на приєднання до відповідного каналу. Склавши список всіх вузлів які приєднуються, головний вузол кластеру відправляє запит до базової станції з проханням надати ключ кластера для свого кластера. У відповідь базова станція передає повідомлення, що містить ключ кластеру і ідентифікатор каналу, щоб вузли, що належать цьому каналу, могли прийняти це повідомлення. Після цього головний вузол транслює повідомлення в своєму власному кластері, яке включає в себе розклад TDMA, початкове число шаблону і перестановку відображення. У фазі сталого стану спочатку кожен вузол в кластері відповідно до свого часового інтервалу відправляє повідомлення з кодом шаблону в канал головного вузла. Це повідомлення містить ідентифікатори вузла-відправника та каналу, репрезентативні дані показань датчика і тимчасову мітку показань датчика. Зібравши всі коди шаблонів свого кластера, головний вузол порівнює ці коди шаблонів і вибирає унікальні.

Пізніше головний вузол передає в свій кластер повідомлення для вибраних вузлів, що містить список вузлів, які мають унікальні коди шаблонів. Потім вибрані вузли відправляють повідомлення з даними в канал. Ці повідомлення містять ідентифікатори вузла-відправника та каналу, а також фактичне показання датчика. Нарешті, головний вузол пересилає всі зібрані дані до базової станції у вигляді повідомлення даних. Щоб забезпечити актуальність даних, вводяться лічильники трьох типів. Це лічильники, які спільно використовуються вузлом і базовою станцією, лічильник, яким користуються два вузли в мережі, і лічильник кластера, яким користуються в певному кластері. Ці лічильники збільшуються кожен раз, коли відбувається успішна комунікація між двома залученими вузлами, будь то окремі вузли або їх група. При скиданні лічильника винятком є лічильник кластера, який створюється кожного разу, коли формується новий кластер, і знищується в кінці циклу.

Для забезпечення цілісності даних і автентифікації джерела для початкових повідомлень, використовується цифровий підпис. Цілісність даних повідомлення запиту на приєднання забезпечується через MAC. Використання парного сеансового ключа між головним вузлом і відправником дає можливість автентифікації джерела повідомлення. Отримання парного сеансового ключа із загального секретного ключа і одноразового номера початкового повідомлення захищає від атак повторного відтворення. Функція цілісності даних під час запиту кластерного ключа надається через MAC. Використання секретного ключа, спільно використовуваного між запитуючим головним вузлом та базовою станцією, забезпечує автентифікацію джерела, тоді як актуальність даних досягається за рахунок включення лічильника, який головний вузол спільно використовує з базовою станцією для обчислення загального секретного ключа. Цифровий підпис забезпечує цілісність даних і автентифікацію джерела для всього повідомлення. Конфіденційність даних забезпечується за рахунок шифрування. Оскільки базова станція шифрує ключ кластера для

кожного вузла, вказаного в відповіді на повідомлення запиту ключа кластеру, використовуючи кожен відповідний загальний секретний ключ, вона також гарантує, що ключ кластера виходить від авторизованої базової станції. Базова станція також включає лічильники, які вона використовує спільно з кожним вузлом для обчислення загального секретного ключа, щоб забезпечити актуальність даних. Цілісність даних і автентифікація джерела доступні для зв'язку між членами кластера і каналом, а також між каналом зв'язку і базовою станцією за допомогою ключової угоди на основі ідентичності. Цілісність даних забезпечується через MAC. Використання загального секретного ключа гарантує автентифікацію джерела повідомлення. Функції забезпечення конфіденційності даних доступні через шифрування. Для повідомлення даних, переданого в кластері, його актуальність даних забезпечується включенням лічильника, який кожен вузол використовує спільно з головним вузлом в обчисленні MAC, тоді як актуальність даних для повідомлень даних, відправлених головним вузлом до базової станції, забезпечується включенням їх спільного лічильника для обчислення секретного ключа сеансу.

Для порівняння приведемо короткий аналіз інформаційної безпеки при окремому використанні цих протоколів та протоколів маршрутизації на основі LEACH, направлених на покращення інформаційного захисту. Для протоколів на основі LEACH слід враховувати аспект безпеки повідомлення розкладу. Повідомлення розкладу містить розклад TDMA для вузлів в певному кластері, які по черзі повідомляють зібрані дані зі своїх датчиків. SLEACH і SecLEACH не полегшують процес автентифікації джерела. Вони дозволяють будь-якому зловмиснику порушити графік передачі даних в будь-якому кластері. MS-LEACH не може надати автентифіковані повідомлення запиту на приєднання, хоча у нього є механізм парних ключів, який може допомогти в досягненні цього. Проаналізувавши протокол агрегації ESPDA, варто зазначити, що він не забезпечує захисту від більшості можливих атак, окрім підслуховування. ESPDA не застосовує жодних

контрзаходів, які можуть забезпечити актуальність даних. Відсутність парного ключового забезпечення серед сенсорних вузлів призводить до того, що існує можливість атак підміни головного вузла кластера і фальсифікація повідомлень. Ці атаки можуть негативно вплинути на результат процесу агрегації даних, оскільки базова станція може отримувати помилкові звіти про стан мережі. Порівняльний аналіз приведено в таблиці 3.1.

Таблиця 3.1 Можливість захисту від атак маршрутизації та агрегації

Атака	MS- LEACH	SLEAC H	SecLEAC H	ESPD A	Об'єднанн я протоколі в
Порушення розкладу	+	-	-		+
Підміна оригінальності Вузла	-	-	-	-	+
Підміна ідентифікаторів вузла	+	+	+		+
Повторна відправка повідомлення	+	+	+	-	+
Підміна повідомлень	+	-	-	-	+
Прослуховування	+	-	-	+	+

Проведемо приблизний аналіз енерговикористання кожного протоколу по трьох етапах обробки даних: етап налаштування кластеру, етап встановленого стану та етап агрегації даних. Аналіз показує, що на етапі налаштування найменші енерговитрати мають протоколи на основі LEACH. Це обумовлено тим, що повідомлення про приєднання та повідомлення про автентифікацію головного вузла та групового ключа додає до загальних

повідомлень невелику кількість бітів. Енерговитрати об'єднання протоколів на цьому етапі вищі ніж в попередніх протоколів. Розмір повідомлення запиту на приєднання і відповіді повідомлення ключа кластера є основними складовими цих енерговитрат. Аналіз інших етапів обробки даних показує, що енерговитрати об'єднаних протоколів на порядок нижчі ніж в його аналогів, за рахунок того, що тут присутнє планування TDMA. Проте, беручи до уваги той факт, що етап налаштування кластеру відбувається на порядок рідше в порівнянні з етапом агрегації даних, об'єднання протоколів можна порівняти з іншими протоколами маршрутизації на основі LEACH, коли вони використовуються в об'єднанні з певною схемою агрегації даних.

3.5 Розробка системи інформаційного захисту

Враховуючи той факт, що сенсорна мережа буде застосовуватися на об'єктах спеціального призначення то створення надійного рівня її інформаційної безпеки є одним із ключових завдань. Так наприклад через те, що в якості каналу передачі використовується звичайний радіоканал, зломисник може використовувати створення радіо завад направлених на повалення або прослуховування цього каналу. Також зломисник може порушити маршрутизацію чи агрегування даних, що призведе до неправильної роботи сенсорної мережі, або отримання секретних даних сторонніми особами. Тобто в сенсорних мережах внаслідок зломисних дій можуть виникати критичні ситуації. Враховуючи це, варто зазначити, що існує гостра необхідність розробки моделі протидії атакам та методу їх виявлення. Проектовану модель захисту пропонується побудувати на основі моделі OSI, тобто методи захисту фізичного, канального, мережевого та прикладного рівнів.

3.5.1. Інформаційний захист фізичного рівня

Фізичний рівень відповідає за вибір частоти, генерацію несучої частоти, виявлення сигналів, модуляцію і шифрування даних. На ньому рівні

можна виділити два основні типи атак: створення завад та фізичне втручання. Перший тип атак полягає в тому, що зловмисник навмисне створює радіозавади на частотах функціонування сенсорної мережі. За рахунок цього він може порушити радіокомунікацію певної частини або й навіть всієї сенсорної мережі. Ефективною протидією цій атаці є швидка псевдовипадкова перебудова робочої частоти (FHSS – Frequency Hopping Spectrum Spreading). Через розташування БСМ у важкодоступних місцях чи при відсутності можливості постійного контролю фізичного стану сенсорного вузла виникає загроза фізичного втручання до цього вузла зловмисником. Він може отримати криптографічні ключі від захопленого вузла, втрутитись в його схеми роботи, змінити методи кодування або навіть замінити його своїм датчиком. Тому існує гостра необхідність забезпечення фізичної цілісності вузла. Для забезпечення безпеки на фізичному рівні необхідно використовувати два наступних методи: метод стрибкоподібної зміни частоти та метод фізичного захисту вузла.

3.5.1.1 Метод стрибкоподібної зміни частоти

Даний метод використовуються для розширення спектру за рахунок стрибкоподібної зміни частоти на основі системи залишкових класів. Суть полягає в тому, що число N записується у вигляді залишків a_n на основі базису $(p_1, p_2, \dots, p_n)$.

$$N = \{a_1, a_2, \dots, a_n\}$$

Після того як залишки вираховані, вони передаються на визначених частотах $f_1, \dots, f_n$. Приклад такої передачі представлений на рисунку 3.3.

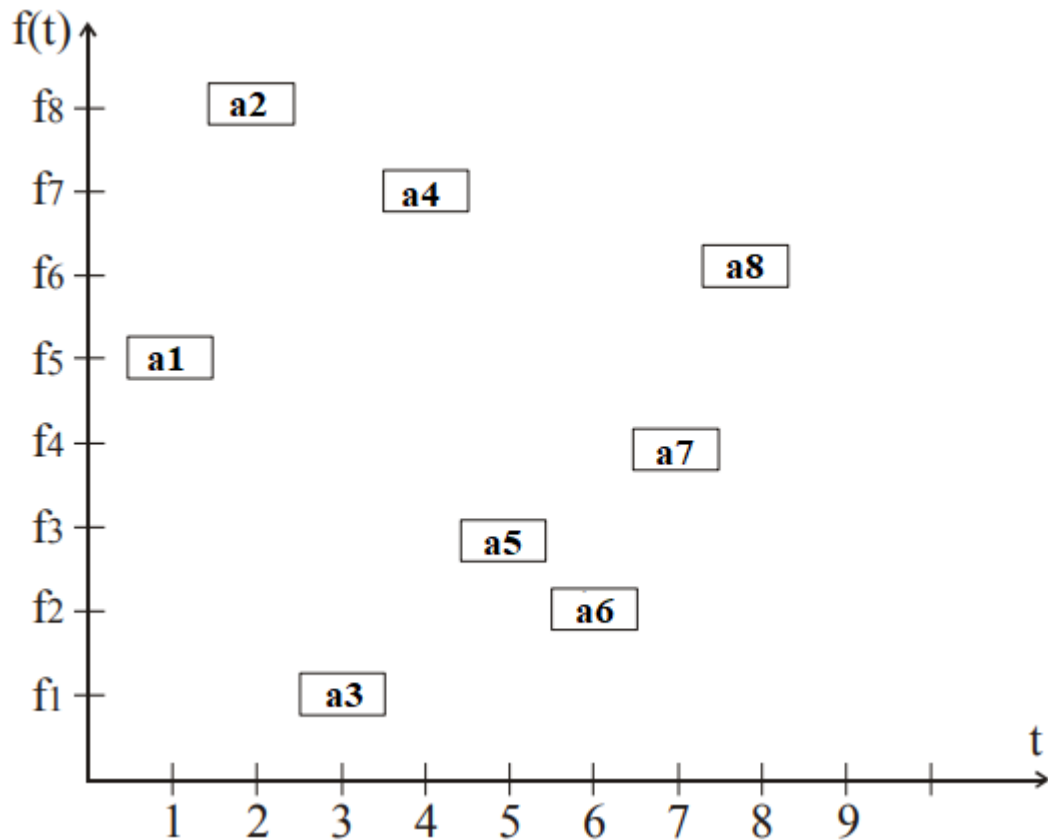


Рис.3.3. Приклад методу стрибкоподібної зміни частоти

Для використання цього методу необхідно забезпечити чітку синхронізацію між приймальною та передавальною сторонами. Забезпечення синхронізації необхідне для того, щоб під час прийомопередачі передавач та приймач змінювали відповідні частоти в чіткий необхідний момент часу. Порядок зміни частот відбувається на основі псевдовипадкової послідовності. Важливо зазначити, що передавач та приймач мають використовувати одну й ту саму послідовність для синхронної зміни частот.

Прийнявши послідовність залишків, приймач виконує зворотне перетворення. Тобто на основі послідовності отриманих залишків він вираховує двійковий код отриманого числа. Проте під час цього перетворення варто зважати на якість прийнятого сигналу. Для цього необхідно забезпечити можливість виявлення та корекції помилок. Тому на основі цього приймачу необхідно розширити основний базис $(p_1, p_2, \dots, p_n)$ до базису $(p_1, p_2, \dots, p_n, p_{n+1}, p_{n+2})$.

На рисунку 3.4 зображена структурна схема пристрою передачі та прийому, які працюють по методу стрибкоподібної зміни частоти.

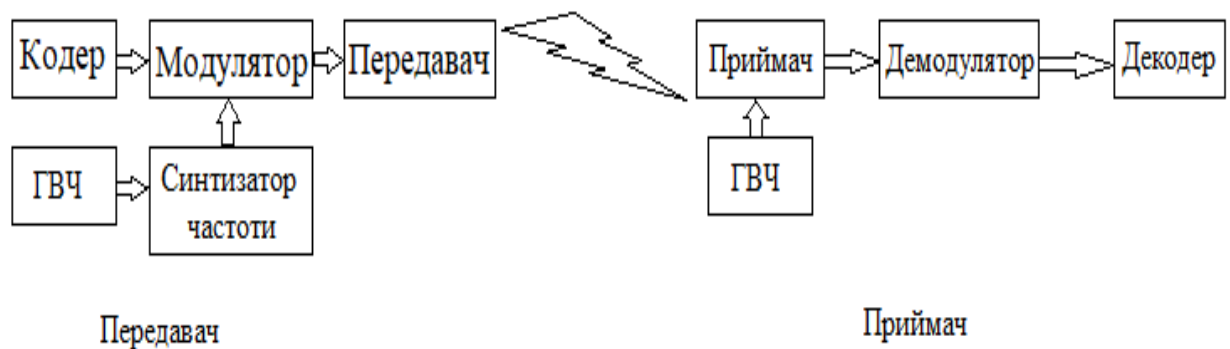


Рис.3.4. Структурна схема пристроїв передачі та прийому

Принцип цієї роботи полягає в тому, що дані надходять на вхід кодера, який перетворює їх на залишки на основі вказаного базиса та передає на вхід модулятора. Генератор випадкових чисел генерує псевдовипадкову послідовність чисел, яка надходить на синтезатор частоти. Синтезатор частоти генерує частоти на основі псевдовипадкової послідовності та передає їх в модулятор. Отримавши згенеровану послідовність залишків та послідовність частот, модулятор модулює сигнал та надсилає його на передавач. На приймальній стороні сигнал отриманий приймачем надходить на демодулятор. Демодулятор перетворює отриману послідовність залишків в двійковий код, виявляє та виправляє помилки.

Тобто основна суть полягає в тому, що по каналу зв'язку передаються залишки обчислені на основі певного базису і кожен з таких залишків передається на окремій частоті, згенерованій за псевдовипадковим законом. На відміну від варіанту коли передається ціле число в двійковій формі, використання вказаного методу дозволить захистити канал передачі від несанкціонованого доступу. Навіть у випадку коли зломисник за рахунок створення завад, створить перешкоди для передачі на певній частоті, це спричинить втрату тільки одного залишку із всієї послідовності. На

приймальній стороні за рахунок розширення базису, прийняту послідовність можна відновити та відповідно виправити. Тому варто зазначити, що запропонований метод підвищує рівень інформаційної безпеки фізичного рівня сенсорної мережі та дозволяє усунути можливість створення завад для передачі. Враховуючи той факт, що частоти передачі змінюються відповідно до псевдовипадкової послідовності, то створення зловмисником завади на одній із цих частот передачі приведе до втрати лише одного залишка, який можна відновити на приймальній стороні, опираючись на розширення базису.

3.5.1.2 Метод фізичного захисту вузла

Цей метод передбачає використання на сенсорних вузлах спеціалізованих захисних корпусів, які унеможливають доступ зловмисника до апаратної складової вузла. Це може бути використання корпусів з міцних та зламостійких сплавів або взагалі корпусів, які не передбачають доступ в середину вузла. Іншою частиною цього методу є самоусунення. Основна ідея полягає в тому, що датчик знищує сам себе, в тому числі знищує всі дані і ключі, коли він виявляє можливу атаку. Це особливо важливо в великомасштабованій БСМ, що має достатню кількість резервування інформації. В такому випадку втрата датчика набагато дешевша та безпечніша, ніж варіант коли датчик буде скомпрометований і працюватиме на користь зловмисника. Ключ до цього підходу - виявлення фізичної атаки. Просте рішення - періодично проводити перевірку сусідства та стану мережі.

3.5.2 Інформаційний захист каналного рівня

До функцій каналного рівня в БСМ можна віднести шифрування даних та виявлення і виправлення помилок. Атаки на цьому рівні направлені на створення колізій та вичерпання енергетичних ресурсів вузла. Колізії відбуваються коли два вузли намагаються передати повідомлення одночасно на одній і тій же частоті. В цьому випадку пакети стикаються та

відкидаються і внаслідок чого потребують повторної передачі. Зловмисник може викликати колізії в певних пакетах, таких як контрольні повідомлення АСК. Можливий результат такого зіткнення - це висока експоненціальна затримка. Зловмисник може просто порушити протокол зв'язку і безперервно передавати повідомлення, намагаючись створити зіткнення. Систематичні повторення таких зіткнень також можуть бути використані зловмисником для виснаження енергетичних ресурсів вузла. До методів інформаційного захисту цього рівня можна віднести такі дії: обмеження кількості запитів та повторних передач, методи виявлення колізій та використання менших кадрів пакету. Всі необхідні дії можна забезпечити за допомогою протоколу канального шифрування. Основним таким протоколом канального рівня в БСМ вважається TinySec. Проте ми пропонуємо використання модифікації вказаного протоколу під назвою SenSec.

SenSec - протокол безпеки канального рівня, аналогічний TinySec, але з дещо іншим типом пакета і більш гнучким механізмом введення ключів. На відміну від TinySec, SenSec працює тільки в одному режимі: автентифікація з використанням шифрування. SenSec використовує початковий вектор довжиною 8 байт та блоковий шифр на основі CBC для шифрування поля даних пакета. Фіксованою частиною восьмибайтового поля є адреса призначення, тип АМ і довжина поля. Ці поля займають 4 байти. Ще однією особливістю є те, що TinySec використовує лічильник, який збільшує як витрати на зберігання, так і витрати на обчислення. Щоб уникнути збільшення цих витрат, SenSec використовує режим випадкових чисел для генерації трьохбайтового випадкового числа і заповнює поле даних цим числом разом з одним байтом ідентифікатора групи.

SenSec використовує існуючий модуль блочного шифру, який використовує в своїй архітектурі в якості основного примітиву безпеки. Для простоти перше випадкове число генерується шифруванням заголовку першого пакета з 3-байтовим полем випадкового числа, встановленим в 0. Потім три найменш значущих байти шифрованого тексту використовуються

для заповнення поля випадкового числа в пакеті. Для наступних пакетів, поле випадкового 3-байтового числа визначається з 3 найменш значущих байтів MAC, який обчислюється та зберігається під час попереднього форматування пакета.

В той час як TinySec вимагає дві операції блочного шифрування для кожного блоку повідомлення в двухпрохідній схемі шифрування та автентифікації, SenSec використовує однопрохідну схему, яка називається XCBC. Таку схему можна вважати безпечною до тих пір, поки загальна кількість зашифрованих і автентифікованих пакетів з використанням одного і того ж ключа менша ніж 2^{32} . Також, аналогічно TinySec, SenSec використовує 32-бітові MAC для зменшення розміру пакета.

Режим XCBC за замовчуванням в SenSec виконує шифрування і автентифікацію для кожного пакету. Вибір XCBC як режим за замовчуванням призводить до того, що шифрування виконується без додаткових витрат, в той час як для шифрування в TinySec потрібні окремі операції в режимі CBC.

У БСМ обмін різними пакетами здійснюється між різними об'єктами мережі. Основними вимогами до інформаційної безпеки цих пакетів є забезпечення автентифікації та конфіденційності. Єдиний механізм ключа, такий як TinySec, не може задовольнити всі ці вимоги, тому SenSec використовує механізм багаторазового ключа для захисту всієї мережі від різних атак та підтримки ефективності функціонування сенсора. SenSec використовує три типи ключів, а саме глобальний ключ (GK), ключ кластера (СК) та ключ датчика (SK) для відображення розгортання сенсорних візлів. Всі ключі перед попередньо створюються та завантажуються перед розгортанням сенсорної мережі.

3.5.3 Інформаційний захист мережевого рівня

Основною функцією мережевого рівня є забезпечення правильної маршрутизації. Тобто цей рівень повинен забезпечувати чіткий обмін

повідомленнями між двома сенсорними вузлами мережі, між сенсорним вузлом та головним вузлом кластера, між головним кластерним вузлом та базовою станцією. Основні атаки на цей рівень направлені на вибірккову або повну втрату пакетів та на перенавантаження мережі, спричинене неправильною маршрутизацією. Ефективними методами боротьби проти цих атак є використання захищеної маршрутизації та безпечне керування ключами.

В пункті 3.4 цього розділу запропоновано та детально описано використання об'єднання протоколів на основі LEACH та ESPDA. Запропонований метод забезпечує правильність маршрутизації та агрегації даних при повному забезпеченні їх інформаційної безпеки та невеликих енергетичних затратах. Також цей протокол забезпечує захист керування ключами за рахунок використання цифрового підпису та неінтерактивної ключової угоди.

В запропонованому методі цифровий підпис використовується для автентифікації ширококомовних повідомлень. Процедура генерації такого підпису виконується в два етапи. Перший етап виконується в автономному режимі (до отримання інформації про повідомлення, яке необхідно підписати), другий етап виконується в режимі онлайн (після того, як стає відомо яке повідомлення необхідно підписати). Онлайн-фаза зазвичай дуже швидка і, отже, може ефективно виконуватися сенсорними вузлами.

До переваг використання такого цифрового підпису можна віднести:

- Використання одного цифрового підпису для всіх повідомлень вузла. Тобто вузлу необхідно один раз згенерувати свій цифровий підпис і далі вже додавати його до необхідних повідомлень. За рахунок цього можна досягти зменшення трафіку в каналі зв'язку, тому що сенсорному вузлу не потрібно кожен раз зв'язуватися з головним вузлом для оновлення інформації про цифровий підпис;
- Використання та генерація цифрового підпису не вимагає від вузла ніяких додаткових дій;

- Перевірка цього підпису іншими кластерними вузлами не потребує ніяких додаткових сертифікатів;

Для процесу керування ключами запропонований протокол передбачає використання неінтерактивної ключової угоди. Метод такого розподілу ключів базується на кластеризації мережі. Тобто розподіл необхідних ключів відбувається лише в межах певного кластеру. Принцип цього методу полягає в тому, що кожен вузол має свій унікальний ідентифікатор та секрет. При встановленні зв'язку між двома певними вузлами кластеру, вони використовують секрет третього вузла(зазвичай спільного сусіда) для виведення їхнього загального секрету. Цей спільний секрет, невідомий іншим вузлам, використовується для генерації криптографічного ключа для безпечного зв'язку між розглянутими вузлами. Через відсутність інтерактивності цей підхід цілком підходить для використання в сенсорних мережах з ресурсними обмеженнями. На рисунку 3.5 показано приклад встановлення ключової угоди між двома сенсорними вузлами, які використовують ідентифікатор третього для виведення спільного секрету в межах кластера. Вузол 10 та 4 хочуть обмінятися повідомленнями. Вузол 10 використовуючи свій секрет «J» та ідентифікатор вузла «5» виводить свій секрет, який має вигляд «5J». В свою чергу вузол 4 використовуючи свій секрет «D» та ідентифікатор вузла «5» виводить свій секрет, який має вигляд «5D». Обмінявшись секретами, вузли 10 та 4 виводять загальний секрет, який має вигляд «5JD», та відомий лише їм, тобто підходить для зв'язку лише між ними.

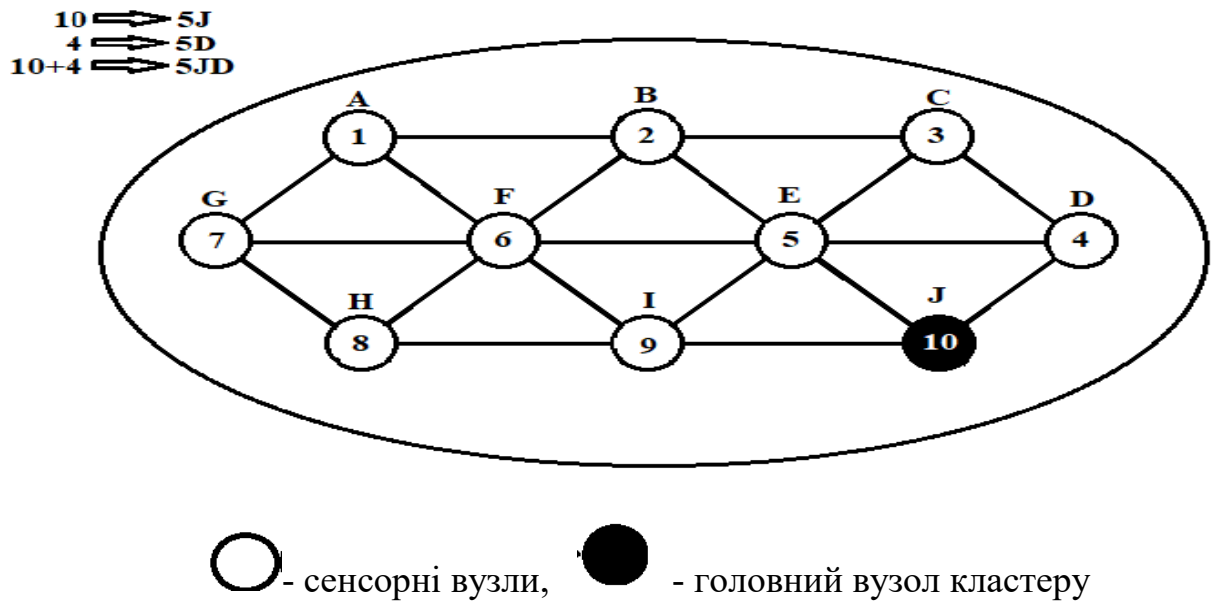


Рис.3.5. Приклад неінтерактивної ключової угоди в межах кластеру

3.5.4 Інформаційний захист прикладного рівня

Основною функцією прикладного рівня є збір всієї інформації та керування даним, тому на цьому рівні надзвичайно важливо впевнитися в достовірності цих даних. Основною атакою на цей рівень є спроби зломисників скомпрометувати або повалити роботу оригінальних вузлів. Це може призвести до того, що скомпрометований вузол отримає доступ до інформації, яка циркулює в сенсорній мережі та буде надсилати неправильну інформацію, яка може спричинити неправильну роботу всієї БСМ. Основними методами боротьби проти таких атак є забезпечення надійних схем агрегації та методів виявлення шкідливого вузла. В пункті 3.4 цього розділу запропоновано та детально описано використання об'єднання протоколів на основі LEACH та ESPDA. Запропонований метод забезпечує повну надійність та безпеку агрегації даних на цьому рівні. Виходячи з специфіки обраних протоколів маршрутизації та агрегації даних схему виявлення скомпрометованого вузла доцільно також будувати на цих протоколах, а саме на основі протоколу маршрутизації LEACH.

Принцип роботи протоколу маршрутизації LEACH складається з двох фаз: фази налаштування кластеру та фази усталеного стану. Враховуючи

правильність роботи мережі з урахуванням енергетичних обмежень вузла, варто зазначити, що оптимальна кількість кадрів на кожному етапі – 5. Тобто фаза усталеного стану містить 5 кадрів, а кількість слотів у кожному кадрі TDMA дорівнює кількості вузлів у кластері.

Тому запропонований метод виявлення скомпрометованого вузла буде працювати наступним чином:

1. Кожен вузол кластера надсилає свої дані у відповідному часовому інтервалі кожного кадру. На кожному етапі останній кадр використовується для передачі значення прямої довіри кластерного вузла до головного вузла кластера. Так наприклад значення прямої довіри вузла n визначає рівень довіри до всіх інших вузлів, які входять до його кластера. Значення прямої довіри можна описати інтервалом від 0 до 1. Тобто 0 означає відсутність довіри, а 1 передбачає повну довіру;
2. Кожен вузол використовує свій унікальний вектор довіри, який містить значення прямої довіри всіх вузлів в кластері. На початку роботи мережі всі зазначення прямої довіри мають значення 1 і кожен вузол повністю довіряє собі;
3. Головний вузол кластера забезпечує моніторинг стану кожного вузла кластера, вираховує їх значення прямої та непрямої довіри та на основі цього робить висновок про те чи певний вузол необхідно приєднати до кластера чи ізолювати його;
4. Головний вузол кластера виконує оновлення вектору довіри, який включає в себе поточні коефіцієнти оновлення довіри всіх вузлів, котрі входять до його кластера;

На кожному етапі кожен кластерний вузол надсилає свої значення прямої довіри до інших кластерних вузлів до головного вузла кластера. Головний вузол на основі цих даних обчислює середній рівень довіри, вагу та значення непрямої довіри для кожного вузла кластера.

Розрахунок оновлення коефіцієнта довіри виконується головним вузлом кластеру. Він агрегує зібрані дані, спостерігає за станом кожного вузла, реєструючи кількість переданих помилкових даних та обчислює відповідний коефіцієнт оновлення довіри. Коли головний вузол виявляє передачу помилкових даних від певного вузла, він зменшує коефіцієнт довіри до нього. Проте варто зазначити, що вузол, який передавав помилкові дані не обов'язково може бути скомпрометованим або поваленим. Помилкові передачі могли виникнути як наслідок несправності в каналі зв'язку, або за рахунок інших тимчасових системних факторів. Тому варто зазначити, що підозрілий вузол варто усунути при постійному зменшенні оновлених значень довіри на певних етапах.

Головний вузол порівнює пряму довіру кожного вузла кластеру із певним пороговим рівнем мінімальної довіри. Коли вказане значення нижче порогового рівня вузол вважається скомпрометованим або поваленим і ізолюється від мережі. Значення мінімального рівня довіри знаходиться в інтервалі від 0 до 1. Вибір цього порогового значення слід здійснювати виходячи з вимог певної сенсорної мережі, а саме з того аспекту наскільки швидко мають бути виявлені шкідливі вузли в сенсорній мережі. Проте варто зазначити, що висока швидкість виявлення таких вузлів не є цілковито ефективною. Це обумовлено тим, що під час винесення рішення на основі зміни мізерної кількості етапі може призвести до виключення нормального вузла, який передавав помилкові дані, наприклад, через тимчасові складності в каналі передачі. На рисунку 3.6 зображено алгоритм функціонування запропонованого методу.

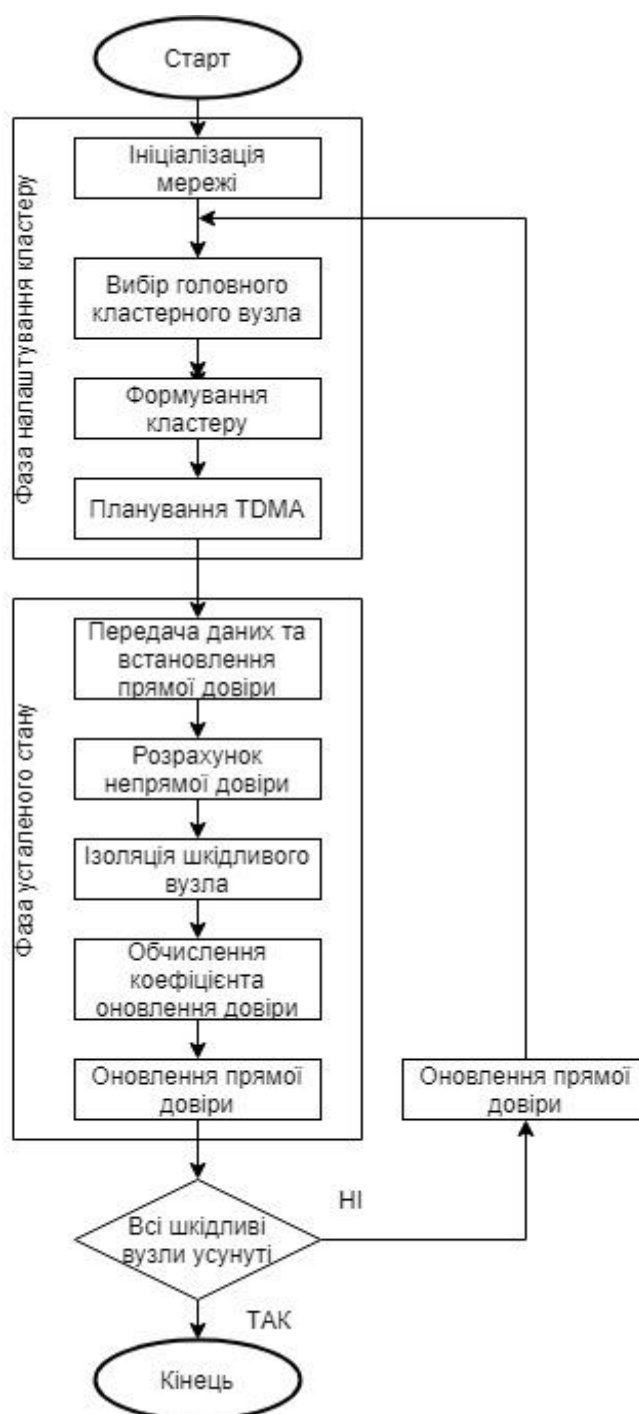


Рис.3.6. Алгоритм функціонування методу виявлення скомпрометованих чи повлених вузлів

3.6 Методика побудови сенсорної мережі для моніторингу станів об'єктів спеціального призначення

Для побудови сенсорної системи для функціонування на об'єктах спеціального призначення було розроблено нову ефективну методику.

Розроблена методика передбачає наступні етапи побудови такої БСМ:

1. Визначення основних цілей БСМ.
2. Визначення основних параметрів БСМ.
3. Аналіз існуючих технологій та параметрів для БСМ.
4. Розробка структури мережі та складу сенсорного вузла.
5. Визначення методу збору даних.
6. Вибір надійного протоколу маршрутизації та агрегації даних.
7. Розробка надійної системи інформаційного захисту мережі.
8. Визначення відповідності розробленої БСМ початковим умовам.
9. Визначення ефективності БСМ.



Рис.3.7. Алгоритм методики побудови БСМ для АЕС

Висновки до розділу:

Даний розділ присвячений розробці методики проектування сенсорних мереж для моніторингу станів об'єктів спеціального призначення на прикладі атомної електростанції. Розроблена методика відповідає висунутим вимогам до роботи сенсорних систем на об'єктах спеціального призначення та до обмеженостей вузла в енергетичних ресурсах.

В першій частині розділу були визначені та обґрунтовані основні цілі та параметри БСМ для функціонування на АЕС. Розроблено структуру мережі та склад сенсорного вузла. Також був визначений метод збору інформації в сенсорній мережі. Основний процес виявлення події можна описати двома етапами: отримання відповідних параметрів сенсорним вузлом та уточнення наявності події. Запропонований метод базується на об'єднанні двох відомих методів збору інформації, а саме на методі збору за розкладом та за подією. Використання такого комплексу дозволить отримувати інформацію про загальний стан об'єкту моніторингу та своєчасно виявляти відповідні події в ньому. Процес детектування події базується на спільному виявленні події за допомогою кластеру. За рахунок цього можна досягти того фактору, що обробка та передача інформації буде обмежена лише в межах одного кластера і сигнал про детектування події надійде до центра керування лише від голови кластера, що зменшить кількість необхідних передач в мережі про одну і ту ж подію. Також за допомогою виявлення події в межах кластеру підвищується точність виявлення події, це відбувається за рахунок того, що фактичне детектування події базується на спільному її виявленні кількома вузлами.

В другій частині розділу запропоновано як протокол маршрутизації використовувати об'єднання протоколів на основі протоколу маршрутизації LEACH та протоколу агрегації ESPDA. Використання такого об'єднання протоколів дасть змогу забезпечити надійну маршрутизацію та агрегацію даних та надійний інформаційний захист цих процесів. Порівняльний аналіз запропонованого протоколу та його аналогів показав той факт, що їх

енерговитрати знаходяться приблизно на одному рівні. Проте рівень інформаційного захисту запропонованого протоколу на порядок вищий і він здатен ефективно протидіяти відомим атакам на маршрутизацію та агрегацію даних в сенсорних мережах. Варто підкреслити важливість одночасного розгляду безпечної маршрутизації і безпечного агрегування даних при розробці протоколу для сенсорних мереж з метою підвищення енергозберігання але інформаційної безпеки сенсорних вузлів та всієї мережі в цілому.

Третя частина розділу присвячена розробці надійного рівня інформаційного захисту. Запропонована модель захисту побудована на основі моделі OSI та передбачає захист фізичного, канального, мережевого та прикладного рівні. Для захисту фізичного рівня описано використання методу стрибкоподібної перебудови частоти та методи фізичного захисту вузла. Це дасть змогу захистити сенсорну мережу від спроб несанкціонованого фізичного доступу до вузла та створення завад для радіоканалів передачі. Захист канального рівня передбачає використання протоколу безпеки канального рівня SensSec. Цей протокол дозволить ефективно протидіяти атакам направленим на створення колізій та вичерпання енергетичних ресурсів вузла. Щоб забезпечити чіткість та безпеку маршрутизації на мережевому рівні пропонується використовувати об'єднання протоколів LEACH та ESPDA. Для керування ключами пропонується використання методу неінтерактивного ключового розподілу. Захист прикладного рівня направлений на усунення атак компрометації або повалення вузла. Це досягається за рахунок запропонованої схеми виявлення шкідливих вузлів.

В результаті була розроблена нова методика побудови сенсорних мереж для функціонування на об'єктах спеціального призначення, яка відповідає всім необхідним умовам та поставленим цілям функціонування БСМ на таких об'єктах.

4. РОЗРОБКА СТАРТАП ПРОЕКТУ

В даному розділі приведено розробку стартап проекту для запропонованої методики побудови сенсорної мережі моніторингу стану об'єктів спеціального призначення.

4.1 Опис розробленої методики

Розроблена методика передбачає новий метод побудови сенсорних мереж на об'єктах спеціального призначення з урахуванням всіх необхідних вимог та особливостей функціонування БСМ та енергетичних обмежень сенсорних вузлів. Розроблена сенсорна мережа слугує для постійного моніторингу об'єктів спеціального призначення та своєчасного виявлення відповідних змін стану об'єкту моніторингу.

Таблиця 4.1 Основний зміст проекту

Опис проекту	Напрямки використання	Вигоди для користувачів
Запропонована нова енергоефективна методика побудови сенсорних мереж для своєчасного та надійного виявлення зміни станів об'єктів спеціального призначення	1.Військова сфера 2.Об'єкти спеціального призначення 3.Системи протипожежної безпеки 4.Системи виявлення вторгнення	Запропонована методика дозволяє своєчасно детектувати події чи зміни станів на об'єктах моніторингу з високою точністю та невисокими енергетичними витратами, при надійному рівні інформаційної безпеки

Основна відмінність запропонованої методики у порівнянні з аналогами полягає в підвищенні рівня інформаційної безпеки та зменшенні енергетичних витрат. В таблиці 4.2 приведено порівняння запропонованої методики з її аналогами.

Таблиця 4.2 Визначення основних характеристик проекту

№ п/ п	Техніко- економічні характерис тики	Потенційні концепції		Сильна сторона	Нейтральн а сторона	Слабка сторона
		Запропоно вана методика	Аналог и			
1	Надійний моніторинг об'єктів спеціальног о призначенн я	Забезпечує	Частко во забезп ечує	Зменшення загальних енерговитра т вузлами сенсорної мережі	Загальна вартість не може бути попереднь о визначена	Майже відсутня можливіст ь визначити чітку топологію мережі
2	Підвищенн я рівня інформацій ного захисту сенсорної мережі	Забезпечує	Частко во забезп ечує	Унеможлив лення зловмисног о втручання в мережу та отримання секретної інформації сторонніми особами	Необхідніс ть чіткого проектува ння та глибоких знань принципів функціону вання	Збільшенн я об'ємів інформації та розмірів пакетів даних

4.2 Технологічний аудит проекту

Технологічну реалізацію та використання технологій в запропонованій методиці приведено в таблиці 4.3

Таблиця 4.3 Технологічна реалізація запропонованого проекту

№ п/п	Основна ідея	Використання технологій	Доступність	Наявність
1	Побудова сенсорної мережі для моніторингу стану на об'єктах спеціального призначення	Спеціалізовані апаратно-програмні системи	Доступні	Частину необхідно розробити
2		Апаратно-програмні системи загального призначення	Доступні	Наявні
3		Розробка апаратно-програмних комплексів	Доступні	Необхідно розробити

Тобто варто зазначити, що побудова сенсорної мережі для моніторингу на об'єктах спеціального призначення буде реалізована з використанням загальноновживаних та спеціалізованих апаратно-програмних комплексів та частковою власною їх розробкою.

4.3 Аналіз ринкових можливостей запропонованого проекту

Характеристика потенційних ринкових можливостей запропонованого проекту приведена в таблиці 4.4.

Таблиця 4.4 Характеристика потенційних ринкових можливостей

№ п/п	Ринкові показники	Характеристика
1	Кількість основних гравців, од.	4
2	Загальний обсяг продажу	?
3	Тенденції ринку	Зростають
4	Наявність обмежень для входу	Залучення власників об'єктів спеціального призначення
5	Специфічні вимоги до стандартизування та сертифікування	Присутні
6	Середня норма рентабельності в галузі	?

Таблиця 4.5 Характеристика можливих клієнтів

№ п/п	Потреба, що формує ринок	Можливі клієнти	Відмінності поведінки клієнтів	Вимоги можливих клієнтів
1	Надійний моніторинг об'єктів спеціального призначення при надійному рівні інформаційної безпеки	Адміністрація об'єктів спеціального призначення та спеціалізованих державних структур, військові та силові структури	Клієнти можуть самостійно змінювати чи визначати аспекти функціонування сенсорної мережі	Забезпечення надійного моніторингу об'єкту при високому рівні інформаційного захисту та невисоких енергетичних витратах

Основні загрози для реалізації запропонованого проекту приведені в таблиці 4.6.

Таблиця 4.6 Основні загрози для запропонованого проекту

№ п/п	Фактор	Опис загрози	Необхідні дії для усунення загрози
1	Не високий інтерес клієнтів	Якщо провести невдалий маркетинг, існує проблема залучення потенційних клієнтів	Проведення чіткого маркетингу та залучення додаткових послуг
2	Зростання спроб несанкціонован ого отримання інформації	За останній час стрімко збільшується кількість зловмисників, які намагаються несанкціонованим чином отримати інформацію, якою оперує сенсорна мережа чи взагалі повалити її роботу	Постійний аналіз відомих атак на сенсорну мережу та розробка нових методів інформаційного захисту чи вдосконалення вже існуючих

Основні можливості для реалізації запропонованого проекту приведені в таблиці 4.7

Таблиця 4.7 Основні можливості запропонованої методики

№ п/п	Фактор	Зміст можливості	Необхідні дії
1	Використання запропонованої методики на основі уже існуючих	Збільшення кількості використання запропонованих систем клієнтами	Якісне покращення розробки
2	Передові позиції на ринку	Зростання попиту	Якісне покращення розробки

Також існує необхідність проведення аналізу впливу конкурентного середовища для розробки запропонованого стартап проекту. Необхідний аналіз приведений у таблиці 4.8.

Таблиця 4.8 Аналіз ринкової конкуренції

№ п/п	Аспекти конкурентного середовища	Опис аспекту	Дії, для забезпечення конкурентоспроможності
1	Конкуренція	Наявність аналогічних розробок	Підвищення надійності моніторингу та зменшення енергетичних затрат вузлами БСМ
2	Локалізація	Відсутність єдиного постачальника послуг	Індивідуальний підхід до розробки кожної можливої клієнтської системи
3	Внутрішньогалузева ознака	Відсутня	Відсутня

Продовження таблиці 4.8

№ п/п	Аспекти конкурентного середовища	Опис аспекту	Дії, для забезпечення конкурентоспроможності
4	Конкуренція за видами товарів	Конкуренція відбувається між товарами одного виду	Робота над зростанням авторитету марки товару та компанії
5	Ціновий	Наявність спеціалізованих програмно-апаратних комплексів, які мають високу ціну	Скорочення загальних витрат за рахунок використання загальнодоступних комплексів де це можливо
6	Марочна інтенсивність	Стандартизація запропонованої марки товару	Просування та високий маркетинг марки товару

Висновки до розділу:

В даному розділі приведена розробка стартап проекту для нової методики побудови сенсорної мережі моніторингу стану об'єктів спеціального призначення.

Аналіз показує, що існує висока можливість виходу на ринок збуту запропонованої методики побудови. Це зумовлено тим, що наразі на ринку збуту майже повністю відсутні компанії, які займаються розробкою та продажом спеціалізованих сенсорних мереж, які б задовольняли всі висунуті до них вимоги.

Висока конкурентоспроможність запропонованої системи досягається за рахунок зменшення загальних енергетичних витрат та підвищення рівня інформаційного захисту в порівнянні з аналогами. Тому варто зазначити, що подальша імплементація проекту є доцільною.

ВИСНОВОК

Магістерська дисертація присвячена розробці нової методики побудови сенсорних мереж для моніторингу на об'єктах спеціального призначення. Варто зазначити, що із розширенням сфер застосування таких БСМ до них відповідно збільшуються і вимоги. До основних вимог застосування БСМ на об'єктах спеціального призначення варто віднести надійну та безвідмовну роботу при надійному рівні інформаційного захисту. Вимоги до безвідмовної роботи зумовлені тим, що при використанні сенсорних мереж на об'єктах спеціального призначення існує гостра необхідність чіткого та своєчасного детектування змін станів чи значущих подій на об'єкті моніторингу. Вимоги до інформаційної безпеки виникають на основі того, що існує необхідність унеможливлення отримання інформації, якою оперує БСМ, або втручання в її роботу сторонніми особами. Варто зазначити, що без забезпечення вказаних аспектів роботи, функціонування БСМ буде неправильним або майже неможливим, а навмисне нехтування цими вимогами може призвести до тяжких або навіть катастрофічних наслідків. Проте під час впровадження нових методик чи систем в такі сенсорні мережі постає питання ефективного використання вузлами енергетичних ресурсів, які і без того жорстко обмежені. Тому для розробки надійної методики побудови сенсорної системи для функціонування на об'єктах спеціального призначення необхідно знайти певний компроміс між надійністю, відмовостійкістю, захищеністю та енергоефективністю такої сенсорної мережі.

В роботі були проаналізовані основні особливості функціонування БСМ та існуючі методи і аспекти побудови сенсорних мереж. Аналіз існуючих методів збору інформації для БСМ показав, що доцільніше використовувати не якийсь метод окремо, а певний комплекс з кількох таких методів. Також були проаналізовані існуючі підходи до побудови інфраструктури БСМ, способи підвищення достовірності інформації в сенсорних мережах, маршрутизація та існуючі методи інформаційного

захисту. Порівняльний аналіз існуючих методів та аспектів побудови БСМ був проведений на основі енергоефективності, часу життя, відмовостійкості та інформаційного захисту сенсорної мережі.

На основі детального аналізу відомих методів побудови сенсорних мереж було розроблено методику побудови сенсорних мереж для функціонування на об'єктах спеціального призначення на прикладі атомної електростанції. За цією методикою, першим кроком для створення вказаної сенсорної мережі є правильне визначення основних її цілей та, на основі цього, відповідних параметрів БСМ. Після того, як відповідні параметри визначені, потрібно провести детальний аналіз існуючих технологій та параметрів для побудови БСМ, та на основі цього визначити найбільш підходящі та ефективні технології. Після визначення цих технологій потрібно перейти до безпосереднього проектування програмно-апаратного комплексу БСМ.

Розроблена методика передбачає використання комплексного методу збору інформації в сенсорній мережі. Цей комплекс базується на об'єднанні двох відомих методів збору інформації, а саме на методі збору за розкладом та за подією. Використання такого комплексу дозволить отримувати інформацію про загальний стан об'єкту моніторингу та своєчасно виявляти відповідні події в ньому. Для забезпечення надійної маршрутизації запропоновано використання об'єднання протоколів на основі протоколу маршрутизації LEACH та протоколу агрегації ESPDA. Використання такого об'єднання протоколів дасть змогу забезпечити надійну маршрутизацію та агрегацію даних при надійному рівні інформаційної безпеки цих процесів. Також розроблено модель інформаційного захисту, яка побудована на основі моделі OSI та передбачає захист фізичного, каналного, мережевого та прикладного рівнів. Запропонована методика побудови сенсорних мереж моніторингу об'єктів спеціального призначення розроблений з урахуванням всіх необхідних вимог щодо функціонування сенсорної мережі на об'єктах спеціального призначення та з урахування обмежень вузлів в енергетичних

ресурсах. Також варто зазначити, що розроблений метод інформаційного захисту дозволяє ефективно протидіяти відомим атакам на сенсорну мережу.

Для запропонованої методики побудови сенсорної мережі був розроблений стартап проект, який показав, що подальша імплементація проекту буде доцільною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Matin M.A., Islam M.M. Overview of Wireless Sensor Network/ Mohammad Abdul Matin. *Wireless Sensor Networks – Technology and Protocols*. 2012.
2. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – Київ: Наукова думка, 2017. – 730 с
3. Інформаційна безпека в середовищі безпроводових сенсорних мереж/ Александер М.Б. та ін. Тернопіль, 2016. 160 с.
4. Галкін П. В. Аналіз моделей та оптимізації збору інформації в безпроводових сенсорних мережах. *Восточно-Европейский журнал передовых технологий ISSN 1729-3774*. 2014. № 71. С. 24-30.
5. Eriksson O. Error Control in Wireless Sensor Networks: A Process Control Perspective. 2011. 30 P.
6. Яцків В. В. Теоретичні основи створення і структурна організація компонентів безпроводних сенсорних мереж підвищеної ефективності : дис. д-ра. техн. наук : 05.13.05. Тернопіль, 2016. 327 с.
7. Довженко Н. М. Методика забезпечення достовірності інформації на основі двомірного кодування в сенсорній мережі : дис. канд. техн. наук : 05.13.06. Київ, 2017. 160 с.
8. Adrian Perrig , Robert Szewczyk , J.D. Tygar , Victor Wen SPINS: Security Protocols for Sensor Networks. *Wireless Networks*. 2002. Issue 8. P. 521-534.
9. A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation / Triana Mugia Rahayu, Sang-Gon Lee, Hoon-Jae Lee. *Sensors*. 2015. № 15
10. Somsri Jarupadung. Event Processing in Wireless Sensor Networks. Surrey, 2014. 73 P.
11. Поширення радіохвиль в зоні покриття безпроводових мереж зв'язку. Теоретичні основи та приклади розв'язання задач [Електронний

ресурс] : навчальний посібник для студентів спеціальності 172 «Телекомунікації та радіотехніка» / КПІ ім. Ігоря Сікорського ; уклад. С. О. Кравчук, Л. О. Афанасьєва, Д. А. Міночкін, І. М. Кравчук. – Електронні текстові дані (1 файл: 2,4 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 107 с.

12. Ioannis Krontiris, Tassos Dimitriou, Hamed Soroush, Mastooreh salajghen. WSN Link-layer Security Frameworks. Javier Lopez, Jianying Zhou. Cryptology and Information Security Series. Volume 1. 2008. P. 142-163.

13. Досягнення в телекомунікаціях 2019 / за наук. ред. М.Ю.Ільченка, С.О.Кравчука: монографія. - Київ: Інститут обдарованої дитини НАПН України, 2019.- 336 с.

14. Лисенко О.І. , Чумаченко С. М. , Валуйський С.В. , Тесленко О. М. Технології екологічного моніторингу в зоні спостереження об'єктів підвищеної небезпеки. *Науковий вісник УкрНДІПБ*. 2014. № 1.

15. Шахнович И.А. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – 288 с.

16. Ільченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. – К.: НВП «Видавництво «Наукова думка» НАН України», 2008. 328с.

17. Yong Wang, Garhan Attebury, Byrav Ramamurthy. A Survey of Security Issues In Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*. Volume: 8, Issue: 2, Second Quarter 2006. P. 2 – 23.

18. Погосов О.Ю., Дерев'янка О.В. Фізичний захист АЕС та інформаційна безпека як необхідні умови зниження ризиків ядерних і радіаційних аварій. *Ядерна та радіаційна безпека*. 2017. № 3. С. 50-55.

19. C.Siva Ram Murthy, B.S.Manoj. Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, 2004, 880p.

20. В. Столінгс. Беспроводные линии связи и сети. Київ, 2003. 617 с.

21. Алексєєва І.В., Пашинський Д. М., Класифікація та порівняння протоколів маршрутизації в бездротових сенсорних мережах. *Вісник АМУ серія «Техніка»*. 2014. №2.

22. Yih-Chun Hu, Adrian Perrig. A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security & Privacy*. Volume: 2, Issue: 3. May-June 2004. P. 28-39.
- 