

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Охорона (назва факультету)

Кафедра комп'ютерних систем та мереж

(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр

(назва освітнього ступеня)

на тему: Методи та алгоритми взаємодії безпроводних сенсорних мереж

Виконав: студент 6 курсу групи СІм-61
спеціальності

123 «Комп'ютерна інженерія»

(шифр і назва спеціальності (напряму підготовки))

Крайник О.В.

(підпис)

(прізвище та ініціали)

Керівник

Приймак М.В.

(підпис)

(прізвище та ініціали)

Нормоконтроль

Тиш Є.В.

(підпис)

(прізвище та ініціали)

Завідувач

кафедри

Осухівська Г.М.

(підпис)

(прізвище та ініціали)

Рецензент

Карпінський М.П.

(підпис)

(прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра комп'ютерних систем та мереж

(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

доц. Осухівська Г.М.

(підпис) (прізвище та ініціали)

«11» листопада 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня

магістр

(назва освітнього ступеня)

за спеціальністю

123 Комп'ютерна інженерія

студенту

Крайнику Олексію Володимировичу

(прізвище, ім'я, по батькові)

1. Тема роботи

Методи та алгоритми взаємодії безпроводних сенсорних мереж

Керівник роботи

Приймак Микола Володимирович., д.т.н., проф.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «29» листопада 2024 року № 4/7-1144

2. Термін подання студентом роботи 19.12.2024

3. Вихідні дані до роботи

наукові літературні джерела

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

1 Аналіз предметної області дослідження. 2 Теоретична частина.

3. Практична частина

4 Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Тема, мета, задачі, об'єкт, предмет, новизна дослідження. 2. Актуальність дослідження.

3. Порівняння вузлів різних виробників. 4. ZigBee Green Power

5. Основні протоколи Web of Things. 6. Порівняння потужностей та радіусу дії датчиків

7,8. Результати моделювання

9. Висновки. Результати проведеного дослідження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<i>Охорона праці</i>	<i>Осухівська Г.М., доцент</i>		
<i>Безпека в НС</i>			

7. Дата видачі завдання 11.11.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	<i>Аналіз існуючих методів та засобів розв'язання науково-технічних проблем, що відповідають тематиці кваліфікаційної роботи.</i>	<i>20.11.2024р. – 30.11.2024р.</i>	<i>Виконано</i>
2.	<i>Обґрунтування актуальності дослідження</i>	<i>05.12-08.12.24</i>	<i>Виконано</i>
3.	<i>Аналіз предмету дослідження та предметної області</i>	<i>09.12-11.12.24</i>	<i>Виконано</i>
4.	<i>Проведення дослідження методів та засобів аналітичного опрацювання даних</i>	<i>11.12-12.12.24</i>	<i>Виконано</i>
5.	<i>Оформлення розділу «Аналіз предметної області дослідження»</i>	<i>12.12-13.12.24</i>	<i>Виконано</i>
6.	<i>Оформлення розділу «Теоретична частина»</i>	<i>13.12-14.12.24</i>	<i>Виконано</i>
7.	<i>Оформлення розділу «Практична частина»</i>	<i>14.12-15.12.24</i>	<i>Виконано</i>
8.	<i>Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»</i>	<i>07.12-12.12.24</i>	<i>Виконано</i>
9.	<i>Нормоконтроль</i>	<i>11.12-14.12.24</i>	
10.	<i>Попередній захист роботи</i>	<i>20.12.24</i>	<i>Виконано</i>
11.	<i>Захист кваліфікаційної роботи</i>	<i>26.12.24</i>	

Студент

(підпис)

Крайник О.В.

(прізвище та ініціали)

Керівник роботи

(підпис)

Приймак М.В.

(прізвище та ініціали)

АНОТАЦІЯ

Крайник О.В. Методи та алгоритми взаємодії безпроводних сенсорних мереж робота на здобуття кваліфікаційного ступеня магістра: спец. 123 — комп'ютерна інженерія / наук.кер. М.В. Приймак. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2024. — 72 с.

Ключові слова: бездротова сенсорна мережа, інтернет речей, мот, zigbee

У цьому дослідженні розглянуто концепцію інтернету речей, технологічною основою якої у багатьох її застосуваннях і стали бездротові сенсорні мережі, береться до уваги насамперед принципова зміна кількісних характеристик мережі.

Бездротова сенсорна мережа виконуватиме функцію виявлення квадрокоптерів. Вибір середовища, що передає сигнал, повинен мати у супроводі надійні схеми модуляції і кодування, це безпосередньо залежить від характеристик передавального каналу.

Одержано порівняльну характеристику випадкового та детермінованого методів розміщення вузлів бездротової сенсорної мережі для гарантування покриття площі обслуговування. Експериментально доведено, що детермінований спосіб розміщення вузлів за умови досить точного розміщення вузлів забезпечує більшу ефективність. Запропонований алгоритм кластерної організації сенсорної мережі дозволяє значно зменшити енерговитрати мережі на роботу зі збору даних.

Використання даної бездротової сенсорної мережі планується на об'єктах, які не допускають на свою територію функціонування дронів.

ANNOTATION

Krainyk O. Methods and algorithms of wireless sensor network. Master's Graduation Thesis: speciality 123 — Computer engineering / supervisor M.V. Pryimak. Ternopil: Ternopil Ivan Puluj National Technical University, 2024. — 72 p.

Keywords: wireless sensor network, internet of things, iot, zigbee

This thesis considers the concept of the Internet of Things, the technological basis of which in many of its applications has become wireless sensor networks, taking into account primarily a fundamental change in the quantitative characteristics of the network.

The wireless sensor network will perform the function of detecting quadcopters. The choice of the medium transmitting the signal must be accompanied by reliable modulation and coding schemes, this directly depends on the characteristics of the transmission channel.

A comparative characteristic of the random and deterministic methods of placing nodes of a wireless sensor network to guarantee coverage of the service area has been obtained. It has been experimentally proven that the deterministic method of placing nodes, provided that the nodes are placed quite accurately, provides greater efficiency. The proposed algorithm for cluster organization of a sensor network allows significantly reducing the energy consumption of the network for data collection work.

The use of this wireless sensor network is planned at facilities that do not allow the operation of drones on their territory.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП.....	9
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ	11
1.1. БСМ та їх застосування	11
1.1.1. В галузі оборони та безпеки.....	14
1.1.2. В галузі охорони здоров'я.....	14
1.1.3. У побуті	15
1.1.4. В екології.....	16
1.2. Основні платформи і дослідження впливу факторів на роботу БСМ	16
1.3. Енергія БСМ	19
1.3.1. Технологія запозичення енергії	20
1.3.2. Запозичення від сонячного світла	22
1.3.3. Запозичення від вібрації	22
1.3.4. ZigBee Green Power	24
1.4. Висновки до розділу	25
РОЗДІЛ 2. ТЕОРЕТИЧНА ЧАСТИНА	26
2.1. Відмовостійкість, масштабованість та витрати на виробництво БСМ	26
2.2. Апаратна частина	27
Restful services 2.3. Топологія мережі	28
2.4. Концепція БСМ як частина Інтернету речей.....	29
2.4.1. Restful services.....	30
2.4.2. CoAP	32
2.4.3. AMQP	34
2.4.4. WebSocket.....	35
2.4.5. MQTT.....	36
2.5. Маршрутизація в БСМ.....	37
2.6. Вимоги до БСМ	39

2.7. Висновки до розділу	40
РОЗДІЛ 3. ПРАКТИЧНА ЧАСТИНА.	41
3.1. Інформація для виконання дослідження	41
3.2. Фактори, котрі створюють вплив на створення моделі БСМ	42
3.3. Алгоритм порівняння потужностей	43
3.3.1. Розрахунок радіусу дії БСМ для ZigBee	44
3.3.2. Розрахунок радіусу дії давачів.....	44
3.3.3. Програмна реалізація в Python.....	45
3.3.4. Особливості моделювання мережі в Matlab	46
3.4. Модель розрахунку споживання БСМ у режимі точка- багато точок	47
3.5. Висновки до розділу	56
РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	56
4.1. Охорона праці	56
4.2. Функціонування державної системи спостереження, збирання, обробки та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу	59
4.3. Висновки до розділу	61
ВИСНОВКИ.....	62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	64
ДОДАТОК А. Тези конференції	

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

AMQP (Advanced Message Queuing Protocol) – відкритий стандарт протоколу прикладного рівня для проміжного програмного забезпечення, орієнтованого на обробку повідомлень.

CoAP (Constrained Application Protocol) – протокол для взаємодії між пристроями Інтернету речей, які мають обмежені ресурси.

IoT (Internet of Things) – Інтернет речей.

HTML (Hypertext Markup Language) – стандартизована мова розмітки документів для перегляду вебсторінок у браузері.

M2M (machine-to-machine) – машино-машинна взаємодія, загальна назва технології, яка дозволяє просто, надійно та вигідно забезпечити передачу даних між різними пристроями.

MQTT (Message Queue Telemetry Transport) – спрощений мережевий протокол, що працює на TCP/IP.

REST (Representational State Transfer) – підхід до архітектури мережевих протоколів, які надають доступ до інформаційних ресурсів.

WoT (web of things) – набір стандартів Консорціуму Всесвітньої павутини (W3C) для взаємодії різних платформ Інтернету речей і доменів додатків.

XMPP (Extensible Messaging and Presence Protocol) – розширюваний протокол обміну повідомленнями та присутності

BSN (WSN –Wireless Sensor Network) – бездротова сенсорна мережа.

ОС – операційна система.

ВСТУП

Актуальність теми. Сьогодні дослідження Безпроводних Сенсорних Мереж (БСМ) розглядаються як один із найважливіших сучасних напрямів розвитку технологій XXI століття. Удосконалення бездротового зв'язку і цифрової електроніки дало змогу розробити дешеві, слабопотужні багатофункціональні БСМ на основі мотів (вузлів), вони досить маленького розміру та «спілкуються» безпосередньо один з одним, відрізняються низькою вартістю, швидкістю розгортання та ефективністю.

Основний задум БСМ – уникнути прямої участі людини в зборі інформації, як приклад, через неможливість людей бути присутніми в конкретному місці чи упродовж здійснення технологічного процесу, особливо коли необхідно збирати інформацію упродовж тривалого часу щодо явищ та процесів, а також одержувати інформацію, котра може бути як простою, так і складною. Технологія БСМ зараз, не дивлячись на певну недосконалість, актуальна і перспективна, привертає увагу вчених, комерційних організацій, промисловості, багато проектів перебувають у стадії розробки, розробляються нові мережеві технології, впроваджуються нові продукти та створюються нові послуги, тим самим одержуючи широке застосування у світі. Сотні мільйонів напівпровідникових сенсорів будуть багатофункціональними засобами автоматизації і впроваджуватимуться в усе, починаючи від брелока і закінчуючи дитячою коляскою. Такі давачі утворюватимуть єдину БСМ, котра виконуватиме первинну обробку даних, самовідновлюватиметься, взаємодіятиме одна з одною, виступатиме в ролі самоідентифікації, оснащуватиметься маленькими акумуляторами, які практично не споживатимуть електроенергії, і їх вистачатиме на весь термін роботи сенсорів.

Мета дослідження: розробка та дослідження алгоритмів, створення нової БСМ, яка згодом буде досліджуватися.

Завдання кваліфікаційної роботи:

- розробка алгоритмів обчислення;
- виявлення можливостей зменшення кількості мотів, із використанням

чутливіших давачів.

– дослідження порівняльних характеристик випадкового та детермінованого методів розміщення вузлів сенсорної мережі.

Об'єкт дослідження: Сучасні Безпроводні Сенсорні Мережі.

Предмет дослідження: БСМ, яка дозволяє відстежувати квадрокоптери та дрони при детермінованому та випадковому розміщенні вузлів на відкритій місцевості.

Методи дослідження: фундаментальні твердження комп'ютерної інженерії, методи - аналітичний, порівняльний, експериментальний.

Наукова новизна отриманих результатів:

– отримав подальшого розвитку метод побудови БСМ при детермінованому розміщенні вузлів;

– запропоновано метод кластерної організації БСМ, котрий дає змогу значно зменшити витрати енергії мережі, котрі витрачаються на збір даних.

Практичне значення одержаних результатів. Можливе використання в охоронних системах безпеки, у захисті військових об'єктів та об'єктів державної ваги, котрі не допускають на свою територію проникнення дронів тощо.

Публікації. Окремі результати дослідження апробовано на XII науково-технічній конференції «Інформаційні моделі, системи та технології» як опубліковані тези:

1. Крайник Н.М. ZIGBEE GREEN POWER // *Інформаційні моделі, системи та технології*: Праці XII наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 18-19 грудня 2024 р.) С. 65.

2. Крайник Н.М. Вимоги до бездротових сенсорних мереж // *Інформаційні моделі, системи та технології*: Праці XII наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 18-19 грудня 2024 р.) С. 67.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів, висновків, списку використаної літератури та додатків. Обсяг роботи:

пояснювальна записка – 72 арк. формату А4, графічна частина – 9 аркушів формату А1.

РОЗДІЛ 1

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ

1.1. БСМ та їх застосування

БСМ будуються із мініатюрних обчислювально-комунікаційних пристроїв, котрі носять назву мотів (від англ. *motes* - порошинки), або сенсорів [1].

Мот - це невелика плата, розміром, зазвичай, трохи більше, ніж 1 кубічний дюйм. На ній розміщуються процесор, флеш-пам'ять оперативна, цифроаналогові та аналого-цифрові перетворювачі, приймач сигналу, джерело живлення та давачі. Працюють моти від невеликого акумулятора та використовують їх тільки для збирання, обробки первинної інформації та передачі сенсорних даних [2].

Давачі можуть бути різноманітними за рахунок підключення за допомогою цифрових та аналогових роз'ємів.

Набір використовуваних давачів залежить від функцій БСМ. Давачі температури, тиску, вологості, світла та вібрації використовуються частіше, тоді як магнітоелектричні, хімічні (наприклад, вимірювання вмісту CO, CO₂), звук та деякі інші використовуються рідше.

Сенсорні мережі, які засновані на співпраці великої кількості крихітних вузлів, які складаються з модулів збирання та опрацювання даних, передавача мають суттєві переваги перед набором традиційних давачів.

Звернемо увагу на дві головні особливості цих давачів:

- можливість давачів бути розташованими далеко від явища, що спостерігається. При такому підході потрібна множина давачів, які використовують складні прийоми, щоб ізолювати ціль від шуму;
- можливість розгортати кілька давачів, вони ж як і збирають дані, так і передають спостереження центральним вузлам, де ці дані збираються та опрацьовуються.

Сенсорна мережа містить значну кількість вузлів (інша назва - мотів), які щільно розташовані поблизу явища, що спостерігається. Положення шпindelів не

потрібно заздалегідь обчислювати. Це дозволяє їх випадково розміщувати у важкодоступних районах або застосовувати для полегшення операцій, котрі потребують швидкого реагування. Розглядаючи з іншого боку, мережеві протоколи та алгоритми, мотосистема повинна мати можливість самоорганізації [2].

Ще одна унікальна особливість сенсорних мереж – здатність окремих вузлів функціонувати разом. Оскільки мот оснащений процесором, замість передачі первинних даних вони можуть відразу обробляти дані, проводячи нескладні обчислення, а потім передавати, оброблені і тільки необхідні.

Що ж відрізняє БСМ від звичайних обчислювальних (провідних та бездротових) мереж [3]:

- повна відсутність електричних, комунікаційних кабелів тощо;
- можливість компактного розміщення або навіть впровадження мотів в об'єкти довкілля;
- надійність функціонування як окремих елементів, і, що важливіше, всієї системи загалом;
- відсутність необхідності у персоналі для монтажу та технічного обслуговування.

Можна стверджувати, що БСМ – це новий крок на шляху переходу в наступну епоху, у майбутньому БСМ стануть важливою складовою нашого життя, ймовірно навіть більше, аніж теперішні персональні комп'ютери. І для здійснення цих чи інших проектів, що потребують застосування БСМ, необхідні спеціальні методи.

Було розроблено багато протоколів та алгоритмів для традиційних бездротових однорангових мереж, проте всі вони не зовсім корисні для неповторних особливостей та умов БСМ.

Варто навести відмінності між сенсорною та звичайною одноранговою мережею:

- в сенсорній мережі кількість мотів може бути значно більшою, ніж у одноранговій мережі;
- щільне розташування вузлів;

- схильність вузлів до збоїв;
- може часто змінюватись топологія БСМ;
- вузли, переважно, застосовують широкомовні повідомлення, водночас більшість однорангових мереж базуються на точковому зв'язку;
- обмеження вузлів по потужності, пам'яті та обчислювальній потужності.

Багатоканальні комунікації можуть ефективно подолати деякі труднощі при передаванні сигналу на значні відстані в бездротовому з'єднанні. Одне із найбільш важливих обмежень для вузлів – повинно бути забезпечено мале енергоспоживання. Моти володіють обмеженими джерелами енергії [4].

Звичайні мережі сфокусовані на забезпеченні сигналу хорошої якості, а мережеві протоколи мотів мають орієнтуватися переважно на енергозбереження. Тоді мот повинен володіти механізмом, котрий дасть змогу користувачеві продовжити термін служби, шляхом пониження пропускної здатності чи збільшення затримки передавання інформації. Зараз багато дослідників беруть участь у розробці схем, які відповідають цим вимогам. Тим самим забезпечуючи широкий спектр застосування сенсорних мереж.

БСМ отримали великий розвиток і можуть використовуватися в багатьох областях [5]:

- у сфері оборони та забезпечення безпеки;
- здійснювати контроль довкілля;
- у промисловості;
- у охоронних системах;
- у сільському господарстві;
- в управлінні енергопостачанням;
- у контролі систем вентиляції, кондиціонування та освітлення;
- у пожежній сигналізації;
- у складському обліку;
- у стеженні за транспортуванням вантажів;
- в галузі охорони здоров'я, контроль фізіологічного стану людини

тощо;

– у контролі персоналу.

1.1.1. В галузі оборони та безпеки. БСМ за рахунок швидкого розгортання, самоорганізації та стійкості до відмови є невід'ємною частиною систем військового управління, зв'язку, розвідки, спостереження, орієнтації. Щільне розміщення одноразових та дешевих вузлів дозволяє під час військових дій при виході деяких з ладу не впливати на перебіг операції, як руйнування традиційних давачів. Тому з важливістю можна сказати, що застосування БСМ краще підходить для ведення військових дій, детектування ядерних, біологічних та хімічних атак, спостереження за зброєю та боєприпасами супротивника, спостереження за боєм, орієнтація на місцевості.

Керівникам та командирам можна постійно стежити за станом своїх вояків, станом та наявністю техніки і боєзапасу під час військових дій та давати своєчасну оцінку збитку від боїв. А прикріпивши давачі до кожної машини, обладнання та важливих боєприпасів, можна дізнатися про їх стан, ці дані всі збираються у ключових точках та передаються на верхні рівні командної ієрархії для поєднання із іншою інформацією.

Використанні БСМ щодо рекогносцировки у разі радіаційних інфекцій дозволить не піддавати людей впливу.

1.1.2. В галузі охорони здоров'я

Застосування таких мереж у охороні здоров'я також різноманітне, як приклад, допомога інвалідам, діагностування, збирання фізіологічних даних про людину, контроль пацієнтів та персоналу, моніторинг використання ліків у шпиталях.

Для прикладу, стан пацієнта може контролюватись лікарем віддалено, це зручно для пацієнта, і дає змогу лікарю зрозуміти їх стан та надати своєчасну допомогу.

Оброблені сенсорними мережами дані можуть застосовуватися у медичних

дослідженнях та містити інформацію упродовж довгочасного періоду. Інсталювані мережні вузли також можуть відстежувати переміщення людей похилого віку і, наприклад, запобігати падінню. Ці вузли компактні і дають змогу пацієнту більшу свободу пересування, водночас, дозволяючи лікарям заздалегідь виявляти симптоми захворювання. На додачу, вони допомагають гарантувати хворим більш комфортніше перебування. Для перевірки здатностей такої системи, на медичному факультеті Гренобль (Франція) було створено "здоровий розумний дім". Спостереження за лікарями та пацієнтами у лікарні: будь-який пацієнт володіє компактным та легким мережевим вузлом. Кожен мот має особисте специфічне завдання. Наприклад, слідкувати за частотою серцевих скорочень, а інший приймає показання артеріального тиску. Лікарі також можуть мати такий мот, що дасть змогу іншим працівникам віднайти їх у лікарні.

Комп'ютеризовані системи в лікарнях дозволять мінімізувати побічні ефекти помилкової доставки ліків. Можна прикріпити вузли до ліків, тоді можливість видачі неправильних ліків може бути зведена до мінімуму. У пацієнтів також можуть бути вузли, які визначають алергію на необхідні ліки.

1.1.3. У побуті. Застосування у будинках – це повна або часткова автоматизація будинку.

Про автоматизацію будинку можна сказати, що інтелектуальні вузли можуть бути вмонтовані в дитячі ліжечка для того, щоб чути дихання немовлят, стежити за станом здоров'я, побутовими приладами.

Використовуючи сенсорні мережі для керування електропостачанням, можна досягти економії в електроенергії. Тобто давачі відстежуватимуть ваше місцезнаходження і тим самим вимикатимуть та вмикатимуть світло.

Наведемо приклади застосування вузлів для побудови інтелектуального середовища. Моти можна вмонтувати у меблі та побутову техніку, для забезпечення їх взаємодії між собою та з сервером приміщення. Сервер кімнат також може взаємодіяти із іншими серверами приміщень, щоб слідкувати за сервісами, котрі вони здатні пропонувати, такі як друк, скан і відсилання факсів. Ці

сервери і сенсорні моти можуть бути вмонтовані в існуючі пристрої і формувати самоорганізуючі, саморегулюючі та адаптивні системи, котрі базуються на моделі теорії керування.

1.1.4. В екології. Найбільшого поширення БСМ набули у сфері моніторингу довкілля та живих істот. Доведено, що вони надають краще розуміння оточуючого середовища, можуть допомогти визначити тип, концентрацію метеорологічних чи геофізичних досліджень, хімічне, біологічне виявлення, розташування забруднюючих речовин, виявити повені, сторонні хімічні агенти у повітрі і воді.

Так як мот може бути стратегічно і щільно розгорнутий в лісі, то вони можуть передавати точне виявлення і походження пожежі ще до того моменту, коли вогонь стане неконтрольованим.

У сільському господарстві в режимі теперішнього часу можливий контроль забруднення повітря, стану ґрунту, ерозії, рівня пестицидів у воді залежно від змінних умов регулюється полив і кількість добрив, що вносяться.

В екології БСМ застосовуються для детектування переміщення комах, птахів та дрібних тварин.

Мільйони давачів можуть бути використані на постійній основі. Їх можна обладнати сонячними панелями, тому що вузли можуть залишатися без нагляду місяцями або роками. Моти будуть працювати разом, щоб виконувати розподілені завдання зондування та долати перешкоди, такі як дерева та каміння, котрі блокують провідні давачі. Відображення біологічного стану оточуючого середовища вимагає складних підходів до розпізнавання інформації в часі та просторі, але завдяки сучасним технологіям, досягненням у галузі збору інформації про об'єкти та явища та автоматизованого збору даних, все це дало змогу значно зменшити витрати на дослідження [16].

1.2. Основні платформи і дослідження впливу факторів на роботу БСМ

До головних платформ належать MicaZ, Intel Mote 2, TelosB (рис. 1.1).



а)



б)



в)

Рис. 1.1. Платформи БСМ (а) Мот MicaZ, б) Intel Mote 2, в) TelosB)

Основні чинники, які потрібні при розробці БСМ, для порівняння у різних моделях наведено у табл. 1.1.

Для БСМ із слабкими приймачами та передавачами був спеціально розроблений основний стандарт ІЕЕ 802. 15.4, а на програмне забезпечення стандартів не існує, але є сотні різноманітних протоколів опрацювання та передавання даних, крім того і системи керування мотами.

Найбільше поширена ОС є відкрита система під назвою TinyOs. Багато розробників часто створюють свою систему управління мовою Java. Програма керування сенсорними вузлами, що працює в ОС TinyOs, написана мовою nesC.

У 1990-х років технологія БСМ почала активно розвиватися, а з початком 2000-х років поступ мікроелектронних технологій дозволив виготовити дешевші елементи для складових мережі. Стандарт ZigBee [6], в основному, є основою БСМ від 2010-х років. З розвитком мікроелектроніки постають нові практичні і теоретичні задачі, пов'язані з використанням сенсорних мереж, росте кількість їх споживачів, багато сфер та царин діяльності (як то промисловість, транспорт, безпека) зацікавлені у впровадженні цих мереж. Крім того, ускладнюється технологічний процес, розвивається виробництво в окремих осіб ростуть запити у сегментах безпеки, необхідний контроль використання ресурсів та запасів.

Порівняння характеристик різних мотів

Назва	MicaZ	TelosB	Intel Mote 2
Мікропроцесор	Atmel ATmega128L	MSP430 F1611	PXA271 XScale
Частота	7.37 МГц	8 МГц	320/416/520 МГц
Флеш-пам'яті	128 Кб	48 Кб	32 Мбайта
ОЗП	ні	ні	32 Мбайта
Додатк. пам'ять для даних	4 Кб SRAM	10 Кб RAM	ні
UART's	2	1	ні
Шини	SPI, I2C	SPI	Mini-USB інтерфейс
Радіо	ChipCon CC2420	ChipCon CC2420	ChipCon CC2420
Зовнішня флеш-пам'ять	512 Кб	1024 Кб	ні
Додатковий конектор	51 -pin	16-pin	I-Mote2 конектор для зовнішніх пристроїв (31+21 pin)
Аналогових I/O	вісім 10 бітових	будований 12 біт ADC/DAC	ні
Цифрових I/O	21		ні
Програмованих LEDs	3	3	2
JTAG порт	так	так	ні
Живлення	дві батареї AA	дві батареї AA	три батареї AA

Гнучка архітектура, що забезпечує під'єднання аж до 65 000 вузлів, зниження витрат на встановлення, відрізняють такі мережі інтелектуальних давачів від інших засобів передавання даних, перш за все якщо мова про велику кількість під'єднаних модулів. Збільшення, зниження вартості, підвищення експлуатаційних параметрів БСМ дозволяють непомітно переходити від провідних рішень до систем збирання телеметричних даних, віддаленого діагностування і обмінювання інформацією.

Будь-який вузол БСМ здатен мати різноманітні давачі для систематичного стеження за навколишнім середовищем, а також мікрокомп'ютер і радіопередавач. Через те пристрій виконує вимірювання, самостійно властиво опрацьовує вихідні дані та може бути на зв'язку із зовнішньою інформаційною системою.

1.3. Енергія БСМ

Найбільш широко БСМ використовуються в галузі моніторингу, дослідження оточуючого середовища і живих істот, а також і для військової промисловості. Кожен вузол давача збирає дані і передає їх на шлюзи чи базові станції безпосередньо, або через інші вузли давача.

Сенсорні вузли, зазвичай, мають обмежені можливості живлення та відновлення. Бездротові сенсорні вузли споживають енергію передачі, опрацювання повідомлень і обчислень. Продовження терміну служби сенсорного вузла залежить від терміну функціонування звичайної батареї, котрі досить часто використовуються. Енергія, що споживається під час передачі повідомлень, може становити до 75% від наявного енергетичного ресурсу. При цьому мають бути вирішені завдання щодо надсилання повідомлень та їх маршрутизації. БСМ здатна включати тисячі вузлів, інша назва - сенсорне поле. Згідно зі специфікаціями протоколу ZigBee, до складу сенсорної мережі може входити аж до 64 000 вузлів. Вже зазначалося, що БСМ має обмежені ресурси: обмежене джерело живлення, малу пам'ять, низьку швидкість передачі і так далі. Вони у свою чергу на пряму впливають на створення протоколів та алгоритмів, котрі використовуються в БСМ. Ми вже розібралися, що розроблені алгоритми для БСМ мають продуктивно функціонувати на дуже обмежених апаратних можливостях. Водночас більшість часу сенсорні вузли перебувають в сплячому стані, що потребує застосування мережесхемних принципів, що самоорганізуються, для функціонування БСМ.

Поява численних досліджень на тему заряджання електронних пристроїв власне від джерел енергії, котрі є відновлювальними, зумовлена низкою факторів:

- широке застосування отримали БСМ, і це є найбільш значущим, на

думку експертів;

- зниження енергоспоживання мікроконтролерів.

1.3.1. Технологія запозичення енергії. У літературі існує спеціальний термін «збирання енергії», що використовується для позначення перетворення відновлюваної енергії із оточуючого середовища на електричну енергію.

Існують різні способи позначення цієї технології, наприклад, «збирання енергії», але в майбутньому замість терміну «запозичення енергії» використовуватиметься термін «збирання енергії».

Запозичення енергії є способом підвищення енергоефективності та надійності БСМ, через перетворення енергії оточуючого середовища у електричну енергію, котру можна застосувати для потреб мота цієї мережі. У такий спосіб пристрої з ймовірністю запозичення енергії із оточуючого середовища можуть замінити складні акумулятори там, де низьке споживання електроенергії, а це значить, що вони не лише генерують, а й економлять електроенергію.

Сучасні технології щодо запозичення енергії, що бурхливо розвиваються, і мікроконтролери, компоненти БСМ, можуть бути під'єднані до спеціалізованих модулів, які забирають енергію із навколишнього середовища (рис 1.2).

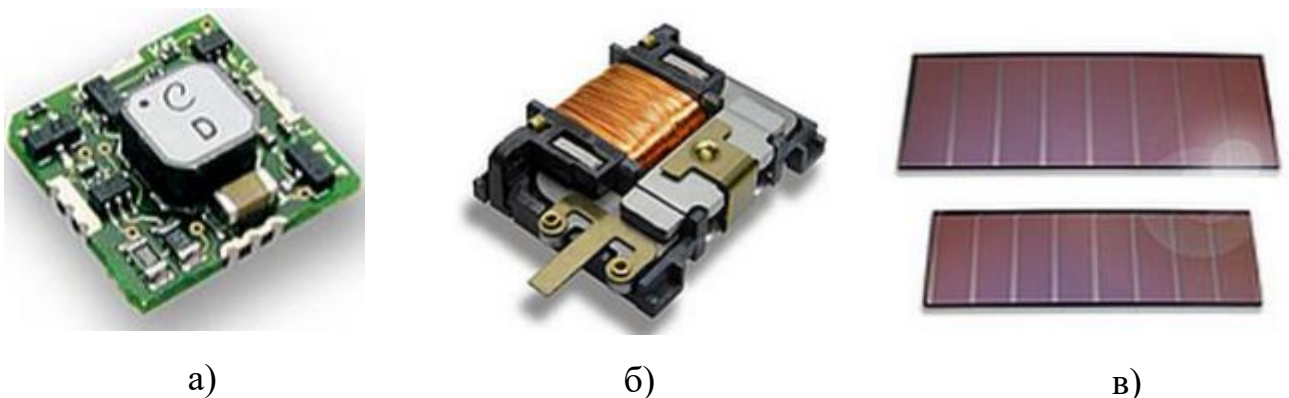


Рис. 1.2. Спеціалізовані модулі, котрі беруть енергію із навколишнього середовища (а - ECO 200 - Motion Energy Harvesting, б - ECT 310 Perpetuum - Thermo Energy Harvesting, в - ECS 300/ ECS 310 - Solar cells)

У разі значної кількості вузлів із енергоємними складовими, з'ясуємо яку

енергетичну вигоду дає використання альтернативних джерел енергії, і за якої кількості вузлів буде взята достатня енергія для простих операцій, а також буде покрита вартість придбаних модулів, що створюють енергію.

Основні методи запозичення енергії бахуються на перетворенні різного роду енергій (світлової, кінетичної, різниці температур середовища) та джерела тепла на електричну або «корисну» енергію.

Проведемо оцінку рівнів енергії мкВт/см і з допомогою табл. 1.2 дослідимо кожен із описаних раніше способів запозичення енергії.

Окрім стандартних методів, котрі є загальновизнаними, втілюється метод одержання електричної енергії із високочастотного випромінювання.

Таблиця 1.2

Методи запозичення енергії навколишнього середовища

Метод запозичення	Значення	Одиниця вимірювання
Вібрації/переміщення людини (в ГЦ діапазоні)	4	мкВт/см ²
Вібрації/переміщення промислових систем (в кГц діапазоні)	800	мкВт/см ²
Зміна температури людини	60	мкВт/см ²
Зміна температури промислових систем	1-10	мкВт/см ²
Світлове випромінювання зовнішнє	10000	мкВт/см ²
Світлове випромінювання у приміщенні	100	мкВт/см ²
GSM (900 МГц)	0,1	мкВт/см ²
WiFi (2,4 ГГц)	0,001	мкВт/см ²

Дослідженням наявності можливості підзарядки від навколишнього середовища та розробкою систем стандартів займаються багато великих компаній, наприклад, EпOcean вже випустила 3 покоління систем, що підтримують запозичення енергії.

1.3.2. Запозичення від сонячного світла. Кремнієва сонячна батарея використовується для запозичення енергії із сонячного світла. З її допомогою можна одержати напругу до 0,6 В, коефіцієнт корисної потужності буде 15-20%. Акумулятори також здатні бути виготовленими на органічних матеріалах та оптичних волокнах із застосуванням сенсibilізованих барвників.

Величина того струму, котрий генерується, перебуває в залежності від інтенсивності світла, що падає. Батарея служить від 1 аж до 5 років. Переваги його використання – низька ціна, прозорість та малий рівень освітленості.

Серед фірм та компаній, котрі беруть активну участь у розробці технологій для сонячних панелей, можна виділити: Konarka Technologies (США), Advanced Industrial Science and Technology, ASIT.

Silicon lab розробила надзвичайно малопотужний вузол БСМ, який запозичує та трансформує сонячну енергію, показуючи, що це рішення зручне для бездротових застосунків сенсорної мережі. Запозичення енергії оточуючого середовища в бездротовій мережі надзвичайно важливе, коли елементи живлення вузлів складно замінити або мають високу вартість. Вузол, котрий запозичує сонячну енергію, наприклад продукт Silicon lab, містить чіп серії MCUs Si10xx, який виконує керування та підтримує функції бездротового інтерфейсу на рівнях, що потребують низького електроспоживання. В той же час наявність додаткового вхідного джерела дає змогу одержувати енергію від інших альтернативних джерел (зокрема радіочастотне випромінювання, вібрації та ін.) на етапі керування енергією, коли сонячні батареї не є зарядженими чи доступ до них на даний момент неможливий.

1.3.3. Запозичення від вібрації У цій сфері на ринку досі відсутні повноцінні системи для збирання цієї енергії, різні компанії пропонують тільки неповні рішення, як приклад плати LTC3105 та LTC 3109.

Компанія Perpetuum на виставці Energy Harvesting & Storage Europ продемонструвала бездротовий давач вібраційного енергетичного комбайна (VEN). VEN не вимагає додаткового технічного обслуговування, практично

ідеальний для встановлення на деталі, що обертаються, такі як підшипники коліс потяга і виконує декілька функцій (як то заміри температури, передавання вимірних даних оператору, вироблення необхідної електрики від механічних коливань), окрім запозичення енергії даввач миттєво детектує критичне підвищення температури у підшипниках, тим самим запобігаючи масштабному ремонту.

Cherry Energy Harvesting демонструє бездротовий комутатор, котрий генерує достатньо електроенергії для передачі сигналу включення чи короткого реле. Відстань, для передачі сигналу за рахунок енергії, що виробляється, залежить від робочої частоти. З метою передавання на 10 метрів застосовується частота 2,4 ГГц, передачі на 300 метрів - частота 868 МГц. Властиво, що потужність, котра генерується натисканням кнопки, може досягати аж до 0,5 МВт.

Додаткові можливості бездротового комутатора збору енергії включають роботу у складі БСМ (для цього комутатор має унікальний код, що виключає помилкове спрацьовування), функцію «повідомлення», що дозволяє використовувати кілька комутаторів для одного приймача або навпаки.

Компанія MicroGen System розробила та практично готова до масового виробництва перших модулів типу piezo-MEMS, які призначені для енергоживлення різних приладів. А коли їх ще й зафіксувати на якомусь джерелі постійної вібрації (стовп, стіна заводу, побутові прилади, рейки на дорогах тощо), то він постійно вироблятиме невеликий струм, якого може вистачити для живлення однієї якоїсь мікросхеми або світлодіода. Такий слабкий струм можна накопичувати і перетворювати за допомогою цих же мікросхем LTC3105 і LTC3109 в вищу напругу, тим самим повністю замінюючи акумулятори або іншого типу елементи живлення.

Wibrate є спеціальним консорціумом, який був створений для об'єднання зусиль розробників промислових систем, котрі функціонують на базі незалежного перетворювання енергії вібрації в електричну енергію. До таких систем належать бездротові промислові системи моніторингу і керування.

1.3.4. ZigBee Green Power. ZigBee, жвавий розробник стандартів і рішень для BSM, анонсував у 2009 році щодо свого рішення випустити стандарт Zigbee Green Power (GP), котрий призначався для пристроїв із власними альтернативними властиво джерелами живлення, заснованими на технології запозичення енергії. Грунтуючись на стандарті ZigBee GP, у 2014 році з'явився Посібник із застосування стандарту GP під час роботи з мікроконтролерами. Його особливості застосування:

- більш короткий формат кадрів GP і, відповідно, менший час передавання, аніж у разі кадрів ZigBee стандартного формату IEEE 802.15.4, це дає змогу заощаджувати енерговитрати на передавання;
- моти не обов'язково маюб бути повноцінними компонентами BSM, ймовірно, що вузли передаватимуть дані тільки за потреби (наприклад, якщо було натиснуто спеціальну кнопку).

Властиво кадр GP відноситься до проксі-вузла, котрий є частиною BSM та оснащений «тунелем», котрий перетворює кадр GP на стандартний формат кадру ZigBee з метою повторного передавання у BSM [8].

Власне кластер GP не вимагає наявності вихідного вузла, проте повинен перебувати у взаємодії як з проксі-вузлом, як з дренажем, для одержання кадрів GP, котрі інтерпретуються. Базовий механізм стандарту GP ZigBee наведений на рис. 1.3, для якого кадр 1 є кадром GP, а кадр 2 є туннелюваним кадром GP.

Переваги застосування ZigBee GP:

- підходить для тих вузлів, котрі розташовані з можливістю підтримки функціонування;
- можливість використання вузлів, основні джерела енергії при яких, батареї належним чином не є захищеними чи недоступними, а також використання ізолюваних вузлів або вузлів, розташованих небезпечно;
- застосування вузлами енергії властиво відновлюваних джерел;
- ймовірність усунення потреби в батареї у вузлах BSM, колективне підтримання працездатності, споживання та відновлення енергії;
- дешева, швидка та проста установка вихідних вузлів.

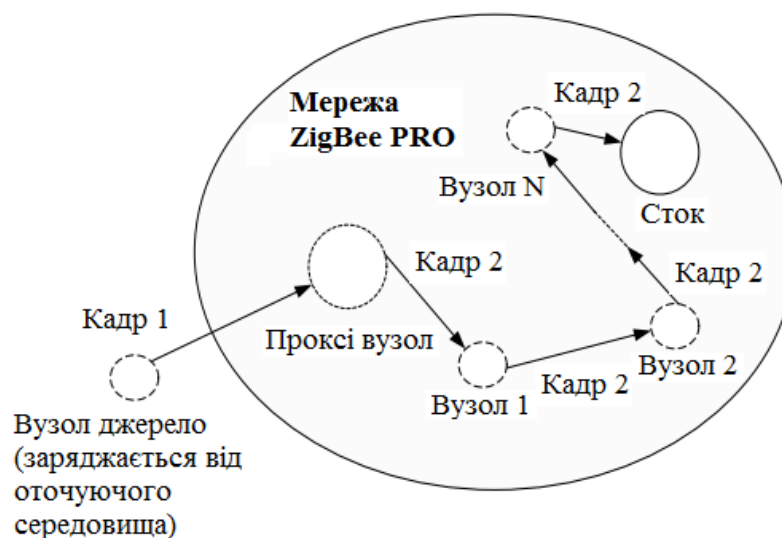


Рис. 1.3. Базовий алгоритм ZigBee GP

Звідси, можна стверджувати, що для оснащення БСМ можливістю запозичення енергії із оточуючого середовища існують не лише готові рішення (як приклад, Silicon Lab), але й стандарти для побудови модулів для запозичення живлення із оточуючого середовища.

Варто виділити Zigbee Alliance, котрий розробив спеціалізований стандарт Zigbee GP standard для доповнення стандартної мережі властиво відновлюваними джерелами енергії. Вже як сфери застосування даної технології, щоб підвищити енергетичний потенціал БСМ можна дослідити розроблення енергонезалежних модулів для БСМ.

1.4. Висновки до розділу

У першому розділі проаналізовано предметну область, зокрема описано поняття БСМ та сфери застосування (оборона та безпека, охорона здоров'я, побут, екологія).

Наведено основні платформи БСМ (MicaZ, Intel Mote 2, TelosB), проведено порівняння їх технічних характеристик. Проаналізовано особливості живлення та отримання енергії вузлами БСМ. Описано стандарт Zigbee GP.

РОЗДІЛ 2

ТЕОРЕТИЧНА ЧАСТИНА

2.1. Відмовостійкість, масштабованість та витрати на виробництво БСМ

Відмовостійкість - це можливість технічної системи підтримувати працездатність при виході чи відмові одного з вузлів. Відмова вузла не повинна впливати на роботу сенсорної мережі, інакше навіть невелика помилка може спричинити повну поломку.

Надійність $R_K(t)$ або стійкість до відмови моделюється з використанням розподілу Пуассона для визначення ймовірності відсутності відмови вузлів за період часу $(0; t)$. Відзначимо, що протоколи та алгоритми можуть бути орієнтовані на рівень відмови стійкості, необхідний для побудови сенсорних мереж. Якщо середовище, в якому розташовані вузли, менш сприйнятливим до перешкод, то протоколи можуть бути менш стійкими до відмови [21]. Наприклад, якщо вузли вбудовані в будинок для контролю рівня вологості та температури, то вимоги до стійкості до відмови можуть бути низькими, так як ці типи БСМ не можуть вийти з ладу і «шум» навколишнього середовища не впливає на їх роботу.

З іншого боку, якщо вузли використовуються на полі бою для спостереження, то стійкість до відмови повинна бути високою, так як спостереження критичні і вузли можуть бути знищені під час військових дій. У результаті рівень стійкості до відмови залежить від застосування сенсорних мереж, і моделі повинні розроблятися з урахуванням цього [21].

Масштабованість - це здатність системи впоратися зі збільшенням робочого навантаження, тим самим збільшувати свою продуктивність за рахунок додавання ресурсів. Кількість вузлів, розгорнутих вивчення явища, може бути близько сотень чи тисяч. Залежно від програми, це число може досягати екстремальних значень (мільйонів). Нові моделі мають бути здатні працювати з такою кількістю вузлів. Вони також повинні використовувати високу щільність сенсорних мереж, яка може змінюватись від кількох вузлів до кількох сотень на ділянці, яка може бути менше

10 м у діаметрі [21].

Оскільки сенсорні мережі складаються з великої кількості вузлів, вартість кожного вузла має бути такою, щоб виправдати загальну вартість мережі. Якщо вартість мережі вища, ніж при розгортанні традиційних давачів, це економічно не виправдано. У результаті вартість кожного вузла має бути невисокою. Тепер вартість вузла, що використовує передавач Bluetooth, є меншою за 10 \$. Вартість ж PicoNode – біля 1 \$. Отже, вартість мота повинна становити значно менше, ніж 1\$ задля економічного обґрунтування їх застосування. Ціна вузла Bluetooth, що вважається дешевим пристроєм, у 10 разів перевищує, в середньому, ціни на моти.

2.2. Апаратна частина

Сенсорний вузол чотири головні компоненти (рис. 2.1):

- блок введення даних;
- обчислювальний пристрій;
- блок живлення;
- передавач.

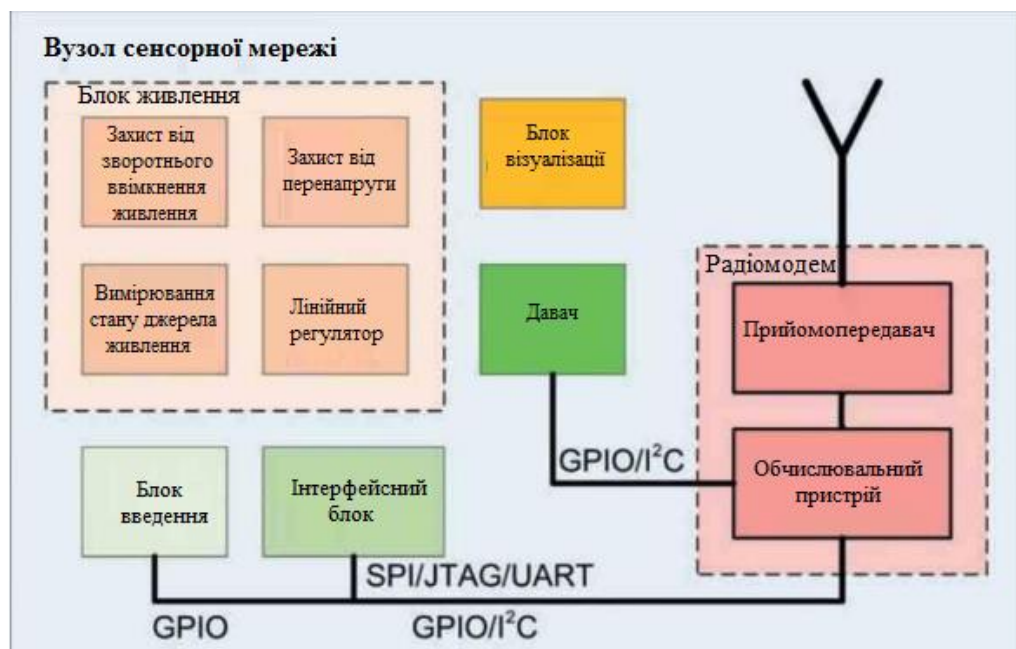


Рис. 2.1. Вузол БСМ

Більшість вузлів, які передають дані та збирають їх, повинні знати своє місцезнаходження з надзвичайною точністю. Для цього потрібен модуль позиціонування. Інколи є потреба у пристрої, який змінюватиме положення вузла при необхідності.

Весь комплект модулів здатен поміститися у «сірникову коробку». Розмір мота часом менший за кубічний сантиметр і досить легкий [22]. Крім розміру, існують деякі інші суворі обмеження для вузлів.

Для інтегрованої БСМ середній рівень заряду має бути меншим за 30, щоб забезпечити довгострокову роботу. Передавання даних вузла може виконуватися оптичним пристроєм (як активним, так і пасивним), міститися в інтелектуальному вузлі або радіочастотному передавачеві.

Детектування розміщення застосовується у різних протоколах маршрутизації БСМ (додаткові відомості див. у п. 2.1). Деякі вчені припускають, кожен вузол повинен мати модуль GPS котрий повинен функціонувати з точністю, яка близька 5 метрам [22].

2.3. Топологія мережі

Топологія – це схема з'єднання каналами зв'язку вузлів мережі між собою. Обслуговування мережі може бути складним завданням, оскільки складові частини можуть бути недоступними, а також вони досить схильні до збоїв.

Площа сенсорної мережі може містити сотні і тисячі вузлів. Вузли можуть бути розміщені зі щільністю більшою, аніж 20 на 1 м³. Таке розміщення значної кількості вузлів вимагає старанного мережевого сервісу [21].

Розгорнути вузли можна в масовому діапазоні або встановити їх окремо. Моти можуть бути розгорнуті таким чином:

- кожен вузол поміщається окремо людиною чи роботом;
- розповсюдження з літака;
- викинуто з катапульт (наприклад, транспортного засобу тощо);
- шляхом розміщення в ракеті чи снаряді;

- розміщення на заводі-виробнику.

Проте моти можна розгортати і статично. Проте відмова вузла часто відбувається через розряд батареї або її руйнування.

2.4. Концепція БСМ як частина Інтернету речей

В даний час існує можливість оснащення БСМ доступом до Інтернету. Доступ в інтернет можна використовувати як резервний канал. Якщо основний недоступний, таким чином можна підвищити надійність мережі.

Останні досягнення в області БСМ та використання протоколу IP у пристроях з обмеженими ресурсами радикально змінили структуру Інтернету [2].

Трильйони розумних пристроїв незабаром буде підключено до Інтернету, що дозволить нам говорити про формування концепції IoT [3].

Інженерна Рада Internet Engineering Task Force (IETF) стандартизувала новий протокол IPv6 по малопотужних бездротових персональних мережах (6lowpan) . Цей новий стандарт дозволяє використовувати IPv6 у мережах з низьким енергоспоживанням та втратами (LLNs), які, у свою чергу, ґрунтуються на стандарті IEEE 802.15.4.

На додаток до 6lowpan робоча група IETF розробила новий протокол маршрутизації для мереж з низьким енергоспоживанням та втратами (RPL) .

Однією з головних переваг IP на базі мережі LLNs є зміна стандартної архітектури веб-сервісів без необхідності використання шлюзів, оскільки смарт-об'єкти будуть інтегровані не тільки з Інтернетом, але і Інтернетом. Ця інтеграція визначається як WoT, котрий є невід'ємною частиною Інтернету речей та надає можливість контролювати та керувати розумними речами за допомогою сторінок. Концепція WoT надає прикладний рівень створення додатків Інтернету речей. Метою технології WoT є створення мережі для вузлів з низьким енергоспоживанням та втратами на основі передових протоколів прикладного рівня.

Перевага нової технології – програми для інтелектуальних об'єктів можуть

бути побудовані на архітектурі REST. Архітектура REST дозволяє програмам покладатися на набір існуючих служб, котрих можна запросити клієнтами залежно від їхніх поточних потреб.

Основна робоча група IETF провела роботу із стандартизації для впровадження веб-сервісів у мережах інтелектуальних об'єктів. Основна група розробила заснований на REST протокол для веб-передачі обмеженої програми Protocol (CoAP).

Протоколи WoT. Протокол XMPP був стандартизований у IETF більше десяти років тому і добре зарекомендував себе, внаслідок чого він досі широко використовується в Інтернеті. Проте, будучи давно усталеним протоколом, XMPP має низку природних недоліків реалізації нових додатків. З цієї причини Google припинила випуск стандарту XMPP минулого року. Однак нещодавно XMPP знову отримав підтримку від інженерної спільноти як протокол для пристроїв IoT. XMPP базується на протоколі транспортного рівня TCP та надає обмін повідомленнями (як за асинхронним, так і синхронним алгоритмом). Він підтримує швидкий обмін повідомленнями і забезпечує низьку затримку (латентність) з часом XMPP також підтримує взаємодію з криптографічними протоколами, такими як TLS / SSL. Однак він не здатний забезпечити необхідну якість обслуговування, що робить його використання недоцільним для M2M-комунікацій. XMPP підтримує архітектуру обміну повідомленнями видавець / підписник, яка більше підходить для IP - адрес, ніж принцип обміну повідомленнями "запит/відповідь".

Однак через те, що протокол XMPP заснований на спеціалізованій мові розмітки XML, існує ряд недоліків, пов'язаних з додатковими витратами на передачу даних, які вимагають розбору XML -тегів, що підвищує вимоги до обчислювальних можливостей і, як наслідок, збільшує енергоспоживання пристроїв.

2.4.1. Restful services REST – це насправді не протокол, а архітектурний стиль. Він був уперше представлений Роєм Томасом Філдіном у 2000 році і досі широко використовується. Він може використовувати різні протоколи передачі даних, наприклад, при використанні HTTP методи HTTP GET, POST, PUT та

DELETE використовуються для надання ресурсів для орієнтованої системи обмінювання повідомленнями, коли всі процеси мають проходити тільки при допомозі синхронних вказівок HTTP даного типу.

"Запит-відповідь". Команда використовує заголовок HTTP, вбудований у повідомлення Асерт, щоб вказати формат даних, що містяться. Формат даних може бути XML або JSON і перебуває у залежності від http- сервера і його конфігураційних параметрів. Все перераховане вище може бути реалізовано в смартфонах і планшетних додатках, оскільки для цього потрібна тільки бібліотека розробників http, яка доступна для всіх ОС (рис. 2.2).

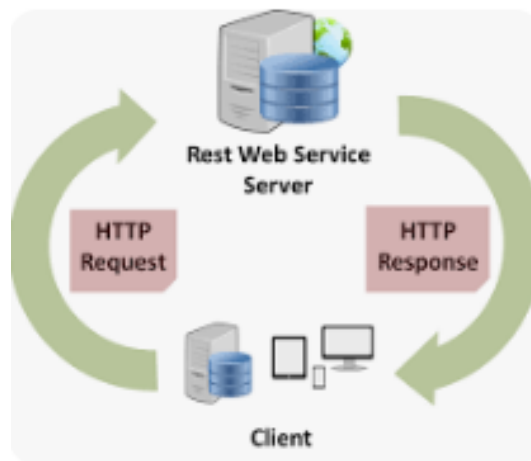


Рис. 2.2. Restful services

Функціональність протоколу HTTP також може бути використана для автентифікації та типу вмісту розмови. Служби Restful використовують різні протоколи прикладного рівня, такі як HTTP та HTTPS.

Проте малоймовірно, що протоколи, які використовують концепцію Restful, стануть домінуючими протоколами комунікацій. Враховуючи сучасні тенденції розвитку мобільних додатків, пов'язані з додатковими витратами на пропускну здатність каналу зв'язку, накладається архітектурою «запит/відповідь» та впливає на швидкість розряду батареї. Ця архітектура також заповнює смугу пропускання безперервно опитуваннями, які не оновлюють стан пристрою. Цю проблему можна вирішити застосуванням протоколів прикладного рівня, що базуються на архітектурі «публікація/підписка», такі як MQTT, XMPP або CoAP.

2.4.2. CoAP. Створений для обладнання із малим споживанням енергії і великими втратами. В його основі лежить протокол HTTP, тому він сумісний із ним.

CoAP призначений для застосування в дуже простих електронних пристроях і дозволяє їм взаємодіяти в інтерактивному режимі через Інтернет. Детальний опис є у стандарті RFC за номером 7252.

Протокол CoAP працює поверх протоколу транспортного рівня UDP. Як і HTTP, він використовує методи GET, POST, PUT, DELETE при клієнтській серверній взаємодії (рис. 2.3). Так як CoAP працює поверх UDP, була потрібна розробка механізмів, які дозволили досягти необхідного рівня надійності. повідомлення CoAP використовуються для контролю якості доставки.

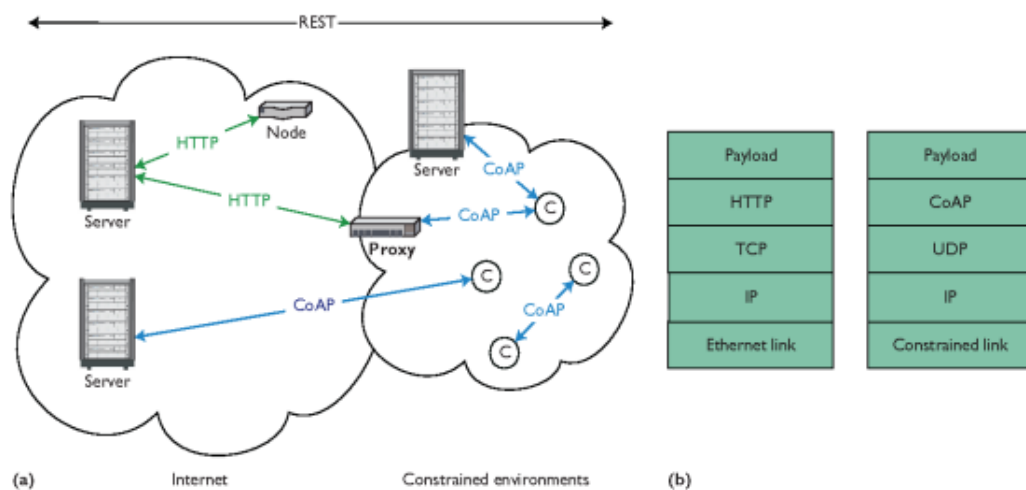


Рис. 2.3. Протокол CoAP

На основі цього поля можна виділити чотири різновиди повідомлень:

- Confirmable – повідомлення, які вимагають підтвердження доставки (ACK). Підтримує як синхронний, і асинхронний режим роботи;
- Non-Confirmable – повідомлення, які не вимагають підтвердження доставки;
- Acknowledgment - повідомлення, яке надсилається у відповідь на повідомлення типу Confirmable;

– Reset - повідомлення, яке надсилається, якщо повідомлення, що приймає, пошкоджено.

Також для протоколу CoAP існує механізм Stop-and-Wait, який затримує надсилання повідомлень і відправляє повторно повідомлення типу Confirmable у разі їх невдалої доставки. І також у CoAP є поле, що містить унікальний ідентифікатор повідомлення розміром 16 біт, за допомогою якого можна виявити дублікат.

Протокол CoAP, разом із методом HTTP Mapping дозволяє, CoAP -клієнту з допомогою проксі-сервера підключатися до HTTP -серверу. За аналогією HTTP -сервер має можливість підключення та передачі даних до CoAP -клієнту.

Для забезпечення безпеки протокол CoAP використовує криптографічний протокол DTLS поверх UDP. Він забезпечує коректну передачу даних, автентифікацію пристрою на сервері та встановлення криптографічно захищеного каналу зв'язку.

Реалізація протоколу CoAP у симуляторі Cooja

Для реалізації протоколу автори використовували інструменти розробки, які постачаються з ОС Contiki [7, 9]. Ця ОС підтримує сучасні протоколи зв'язку для мереж із низьким енергоспоживанням та втратами: 6LoWPAN, RPL, CoAP. Моделювання проводилося за допомогою інструменту COOJA. Для побудови мережі з урахуванням CoAP використовувалася реалізація протоколу ОС Contiki.

На рис. 2.4 показано сенсорне поле, яке є квадратом 100 на 100 метрів і містить 22 вузли, розміщених випадковим чином.

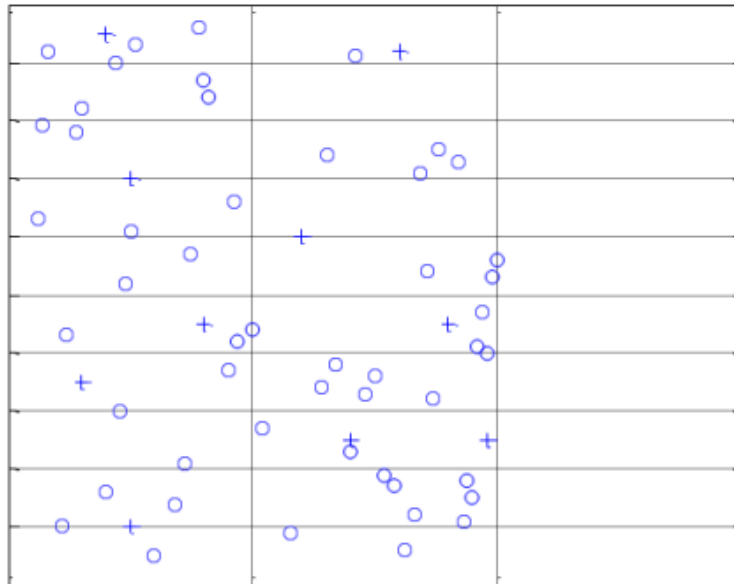


Рис. 2.4. Сенсорне поле

2.4.3. AMQP. Цей протокол може використовувати різні протоколи транспортного рівня, але він призначений для протоколів із гарантованою доставкою даних, таких як TCP (рис. 2.5).

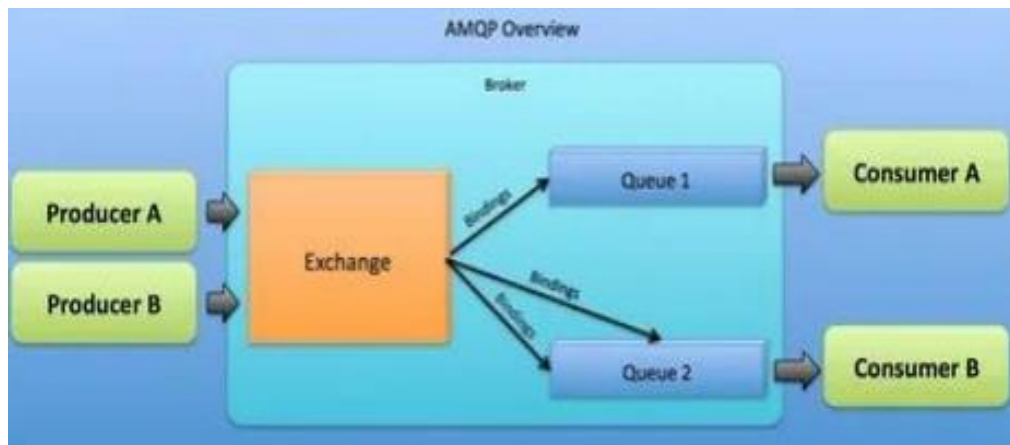


Рис. 2.5. Протокол AMQP

Протокол AMQP забезпечує асинхронну передачу даних на основі моделі видавець/передплатник. Його головною перевагою є функція зберігання та пересилання даних, що забезпечує надійність навіть після збоїв у роботі мережі. Надійність забезпечують такі властивості протоколу:

- "принаймні один раз" означає, що протокол гарантує правильну доставку

повідомлення, і якщо це не вдається, він повторно надсилає повідомлення. "Принаймні один раз" означає, що повідомлення, безумовно, буде доставлено один раз, а можливо, і більше;

- "рівно один раз" означає, що повідомлення буде доставлено тільки один разів.

Останнім часом дослідження показали, що AMQP має низьку ймовірність успішної доставки повідомлень при низькій пропускній здатності, але ця ймовірність зростає зі збільшенням пропускної здатності. Інше дослідження показує, що в порівнянні з вищезгаданим REST, AMQP може надсилати більше повідомлень за секунду. Крім того, було встановлено, що AMQP серед 2000 користувачів, розподілених на п'ять континентів, може обробляти 300 мільйонів повідомлень на день.

2.4.4. WebSocket. Протокол WebSocket був розроблений в рамках ініціативи HTML створення каналів зв'язку по протоколу TCP. У WebSocket клієнт ініціалізує з'єднання із сервером, щоб встановити сеанс WebSocket. Сама установка з'єднання аналогічна до установки з'єднання в протоколі HTTP, і веб-сервери можуть обробляти сеанс WebSocket, використовуючи той же порт, що і HTTP -з'єднання. Фактично, під час сеансу HTTP заголовки видаляються, і клієнти та сервери можуть обмінюватись повідомленнями в асинхронному режимі повної зупинки - інтегроване з'єднання. Сеанс зв'язку може бути перерваний на запит з боку сервера або клієнта (рис. 2.6).

WebSocket використовується для зниження навантаження на канали зв'язку в мережі загального користування, забезпечуючи повнодуплексний зв'язок в режимі реального часу. Існує також прото-протокол WebSocket, званий WebSocket sub-Protocol (WAMP), який призначений для підтримки моделі видавця/передплатника у WebSocket.

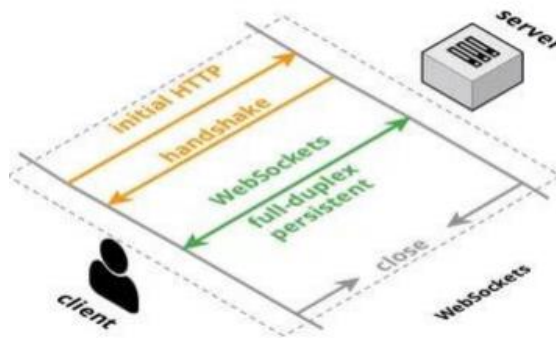


Рис. 2.6. Протокол WebSocket

Система обміну повідомленнями WebSocket працює поверх протоколу TCP і сама по собі не реалізує жодних механізмів безпеки. За потреби безпечні з'єднання можуть бути реалізовані через WebSocket із використанням криптографічних протоколів TLS/SSL. Під час сеансу повідомлення веб-сокету мають розмір 2 байти.

Дослідження показали, що при завантаженні посилання протокол HTTP повторно надсилає заголовок HTTP, що збільшує затримку. WebSocket, за оцінками, забезпечує зниження затримки від трьох до одного, порівняно з напівдуплексним режимом опитування HTTP. Протокол WebSocket не призначений для пристроїв з обмеженими обчислювальними можливостями, на відміну від перерахованих вище протоколів, що базуються на клієнт-серверній архітектурі. Цей протокол не дуже добре адаптований до рішень концепції, але він розрахований на роботу в режимі реального часу, є захищеним протоколом і мінімізує вимоги до каналу зв'язку, а при використанні протоколу WAMP дозволяє організувати ефективні сценарії обміну інформацією для ІВ.

Таким чином, WebSocket може конкурувати з будь-яким іншим протоколом, що працює поверх протоколу TCP.

2.4.5. MQTT. Створений компанією IBM для спрощення роботи M2M. Це асинхронний протокол, побудований поверх протоколу транспортного рівня TCP. Як сервер MQTT використовується так званий брокер (рис. 2.7).

Кожен клієнт, підключений до MQTT -брокера, при оновленні брокера отримує нові дані від каналу на брокері, на який він підписаний. MQTT розроблений для пристроїв з низьким енергоспоживанням та високими втратами (LLN).

Типи повідомлень MQTT:

- Fireandforget - повідомлення надсилається один раз і не потрібно підтвердження;
- Deliveredatleastonce- повторно надіслані повідомлення вимагають підтвердження;
- Deliveredexactlyonce - механізм чотириступінчастого рукостискання клієнт-брокера.

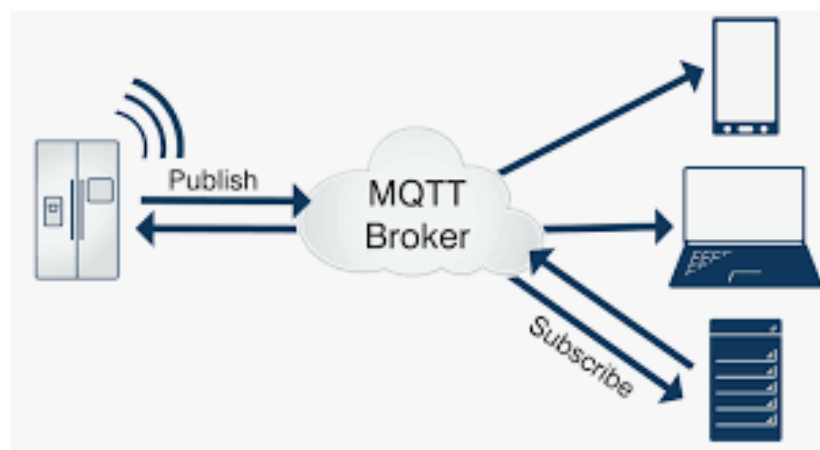


Рис. 2.7. Протокол MQTT

MQTT, як і протокол HTTP, для забезпечення безпечної передачі даних використовує методи автентифікації TLS/SSL.

2.5. Маршрутизація в БСМ

Існує три типи маршрутизації: проста, фіксована та адаптивна. Їх відмінність – коли треба враховувати зміни топології мережі та навантаження під час вирішення завдання вибору маршруту.

Звичайна маршрутизація, за якої вибір маршруту не враховує зміни топології

мережі та стану навантаження. Він забезпечує спрямовану передачу даних. В результаті він забезпечує низьку ефективність, але простоту у втіленні маршрутного алгоритму і гарантуванні стабільного функціонування мережі якщо вийдуть з ладу її окремі елементи. Проста маршрутизація поділяється на випадкову і лавинну. Відмінними рисами випадкової маршрутизації є те, що вибирається один випадково визначений вільний шлях для передавання пакета з вузла зв'язку, таким чином пакет «блукає» мережею, і врешті-решт з якоюсь ймовірністю він досягає пункту призначення. Не забезпечує ні ефективної пропускну здатності мережі, а ні оптимального часу доставлення пакета.

Лавинна ж маршрутизація використовує передавання пакета від вузла у різних напрямках, окрім власне того, звідки цей пакет прийшов до цього сайту. Існує явище «множення» пакета, у якому різко погіршується використання пропускну здатність мережі, що з великим навантаженням на вузли.

Ми повинні відзначити копії пакета та знищити дублікати, котрі йдуть через нього повторно на кожному вузлі, щоб зменшити навантаження. Головна перевага цього методу полягає в тому, що він гарантує оптимальний час доставки посилки одержувачу, так як принаймні один з них гарантує такий термін з усіх можливих напрямків, що посилка відправляється. Цей метод може бути використаний у незавантажених мережах, якщо вимоги до мінімізації часу та надійності доставлення пакетів даних є достатньо високими.

При фіксованій маршрутизації для будь-якого вузла призначення, шлях передавання буде вибиратися з таблиці маршрутів (каталог), що встановлює мінімально короткий шлях. Каталоги мстяться у центрі керування мережею. Каталоги знову складаються і за потреби модифікуються. Нездатність адаптуватися до змін навантаження веде до затримок передавання мережних пакетів. Існують одноколіїні та багатодоріжкові версії фіксованої маршрутизації. Перший заснований на одному пакетному шляху між двома абонентами, це зв'язано із відсутністю стійкості до збоїв та навантажень, а другий - на кількох можливих шляхах між двома абонентами, властиво з яких і робиться вибір найкращого шляху. Такий тип маршрутизації використовується у мережах зі слабо мінливою

топологією та стійкими потоками пакетів.

2.6. Вимоги до БСМ

Автономія. Ліквідація якогось вузла не має нести вплив на її функціонування. Так як мережа не має мати центрального вузла, який-небудь користувач здатен здійснювати функції віддаленої маршрутизації.

Енергетична ефективність. Протоколи маршрутизації мають максимально ефективно використовувати енергію.

Масштабованість. БСМ складаються із сотень мотив, саме тому протоколи маршрутизації повинні функціонувати з таким їх числом.

Стабільність. Давачі здатні раптово перестати працювати через поломку батареї живлення або із якихось зовнішніх причин. Маршрутизаційні протоколи мають опрацьовувати цю ймовірність так, щоб якщо струм у мотах пропаде, можна було використовувати альтернативний маршрут.

Неоднорідність приладів. Хоча більшість додатків БСМ залежить від однорідності вузлів, використання різних типів давачів може забезпечити значний привілей.

Мобільність. За певних подій моти здатні переміщуватися під час роботи.

Особливості та обмеження БСМ створюють спеціальні умови до маршрутизаційних протоколів.

Базується на параметрах. Для цих алгоритмів вузол надсилає запити до певних ділянок мережі та очікує відповіді від давачів, розташованих у цій частині. Вибір параметрів перебуває у залежності залежить від визначеної програми. Головна особливість такої схеми – зміст меседжу даних піддається аналізу під час кожного етапу маршрутизації.

Енергетична ефективність. У цих алгоритмах можна вибрати шляхи, котрі, як сподівається, найбільше сприятимуть зберіганню енергії в мережі. З цією метою маршрут містить вузли із вищими енергетичними ресурсами.

Агрегування даних. Відносно близькі вузли можуть робити аналогічні дані,

котрі здатні поєднуватися з деякою прийнятною втратою точності.

Застосування давачів істотно залежить від зв'язку між мотами, так як це потрібно для втілення визначених алгоритмів або процедур. На ділі є три головні типи алгоритмів маршрутизації для БСМ – централізовані, розподілені і локальні:

Алгоритми, що використовуються, є важливим фактором, який необхідно враховувати при вибиранні маршрутизаційного алгоритму. Коли застосовуються локальні алгоритми, тоді основною буде значна комунікаційна зв'язуваність вузлів, які знаходяться поруч. Для централізованих алгоритмів консолідація повідомлень буде значним привілеєм. Розподілені ж алгоритми мають надавати вірне з'єднання між двома мережевими мотами. Для локальних алгоритмів варто зважати на те, що застосування побічних механізмів позиціонування (як варіант GPS) здатне досить збільшити вартість такої мережі.

Класифікація за методом розрахунку шляхів:

- проактивні протоколи - всі шляхи розраховуються заздалегідь, як вони знадобляться;
- реактивні протоколи - шляхи розраховуються на вимогу;
- гібридні протоколи – це поєднання двох підходів.

2.7. Висновки до розділу

В цьому розділі описано характеристики відмовостійкості, масштабованості та витрат на виготовлення БСМ. Проаналізована апаратна частина та топологія мережі.

Також досліджено концепцію БСМ як частини Інтернету речей, докладно проаналізовані сервіси і протоколи Restful services, CoAP, AMQP, WebSocket, MQTT.

Описані особливості маршрутизації в БСМ, наведено вимоги до БСМ.

РОЗДІЛ 3

ПРАКТИЧНА ЧАСТИНА

3.1. Інформація для виконання дослідження

Сама структура систем моніторингу має такий вигляд. На нижньому рівні розташовуються давачі; кожен давач під'єднюється до моту. З мотом дротовими з'єднаннями пов'язано відразу кілька давачів або давач розташований на платі мота - це залежить від функцій, які виконують давачі. Ми розташовуватимемо давачі безпосередньо на контрольованій поверхні.

Моти будуть використовуватися тільки для збору та первинного перетворення сенсорних даних, вони відразу пересилають інформацію один одному, а в кінці, спеціальному пристрою - шлюзу (базовій станції, координатору), що має провідне з'єднання з сервером, де ці дані будуть оброблятися.

У мережі може бути кілька шлюзів, а також може бути, що кожен мот може стати шлюзом залежно від певних умов, що підвищує її надійність та швидкодію.

Управління режимами збору інформації та основна обробка одержуваних сенсорних даних здійснюється додатками мережі.

Найефективніша тут конфігурація типу «зірка» У цьому випадку моти будуть передавати інформацію виділеним мотам-маршрутизаторам, які взаємодіють із базовою станцією. Такий підхід підвищить безпеку мережі, а також підвищить ймовірність працездатності каналу, оскільки не буде зайвих пристроїв, до яких можуть підключитися зловмисники.

Зазвичай маршрутизатори сенсорами не оснащуються, але в принципі ніщо не забороняє їх оснастити. Таким чином, виходить, що мережа складається з багатьох кластерів, утворених маршрутизатором і сенсорними вузлами, в яких маршрутизатор запитує сенсорні дані. Маршрутизатори ретранслюють дані один одному, і зрештою ці дані передаються на шлюз. Надійність такої системи дуже висока: відмова великої кількості як двигунів, так і маршрутизаторів ніяк не вплине на роботу системи.

У даному дослідженні буде розглянуто метод боротьби з квадрокоптерами за допомогою БСМ та проведено аналіз факторів, що впливають на цю мережу. БСМ буде виконувати функцію виявлення квадрокоптера, будуть проаналізовані фактори, що впливають на відстань виявлення дронів, на дальність дії мотивів БСМ.

Бездротова мережа буде оснащуватися давачами, що вловлюють радіомагнітне випромінювання в діапазонах RC433 - 433 МГц і RC868 - 868-916 МГц, що випромінюється квадрокоптерами. Знаючи розташування давачів та обробляючи інформацію з них програмно можна визначити перетин квадрокоптером периметра та напрямок руху квадрокоптера.

На області, що охороняється, по чотирьох сторонах будуть розташовуватися давачі, що фіксують потужність випромінювання сигналу, в якому працюють квадрокоптери. Квадрокоптер літає біля периметра, що охороняється, але не перетинає його, давачі фіксують випромінювання. Коли квадрокоптер перетинає периметр, давачі фіксують потужність випромінювання його сигналу, вона буде максимальною, після перетину почне зменшуватися, а потужність сигналу на іншій стороні периметра і по центру, давачів буде збільшуватися. Порівнюючи потужності сигналу на різних давачах, можна визначити, чи квадрокоптер перетинав периметр чи ні, і приблизний його рух.

Дана БСМ використовуватиметься зовні, тому всі її вузли мають бути захищені від кліматичних факторів, протокол роботи ZigBee, режим роботи mesh, точка-точка, точка – багато точок або зірка в залежності від умов. Як варіант в якості мота можна використовувати Arduino, Teensy, Netduino та ін. Для економії моти даної БСМ можна оснащувати додатковими давачами, наприклад контролю периметра, клімату і т.д.

3.2. Фактори, котрі створюють вплив на створення моделі БСМ

Через особливості даної БСМ до факторів, які впливатимуть на її роботу можна віднести стійкість до відмов, можливість масштабування, витрати на виготовлення, топологію мережі, певні обмеження апаратної складової, модель

передавання даних та використання енергії [21], а також алгоритми обробки інформації. Дані фактори розглядаються та описуються багатьма дослідниками, але в жодному дослідженні повністю вони не враховані. Вони також мають вплив на розроблення БСМ, так як є дороговказом для створення протоколу чи алгоритмів функціонування мереж. Також, ці чинники можуть бути застосовані для співставлення різних пропонованих моделей [21].

3.3. Алгоритм порівняння потужностей

Р-потужність випромінювання в Дб уловлюється давачами БСМ від дронів.

Якщо в області давачів немає джерел випромінювання, вони перебувають у сплячому режимі. При виявленні радіовипромінювання давачі БСМ вмикаються. Після ввімкнення давачі постійно фіксують потужність випромінювання та запам'ятовують максимальну потужність випромінювання.

Маємо дев'ять давачів, здатних вловлювати електромагнітне випромінювання. Вісім треба розставити по периметру, а дев'ятий зробити центральним, як на рис. 3.1.



Рис. 3.1. Периметр області, яка охороняється

Це максимальне рішення, область охорони повністю перекривається, алгоритм дозволяє визначити перетин периметра, якщо дронів більше одного, а також дозволяє максимально точно визначити вектори руху.

3.3.1. Розрахунок радіусу дії БСМ для ZigBee. Для розрахунку потужності сигналу на вході радіоприймача можна використати формулу (3.1) [3]:

$$P_{\text{вхід}} = P_{\text{вих}} + 20\lg(\lambda) - 20\lg(4\pi) - 20\lg(r) \quad (3.1)$$

де $P_{\text{вих}}$ - потужність сигналу на виході передачі, від $P_{\text{вих}} = 1$ дБм; $P_{\text{вхід}}$ - потужність сигналу відповідно на вході приймача (приймається ≥ 95 дБм); λ - довжина хвилі радіосигналу (визначено 0,125 для діапазону 2,4 ГГц); r - дистанція між приймачем та передавачем.

Виконаємо розрахунок радіусу дії БСМ для ZigBee за (3.2), для наведених вище параметрів значення r буде рівним 627,94 м.

3.3.2. Розрахунок радіусу дії давачів. Потужність передавача квадрокоптерів фірми DJI 20 дБм, частота роботи 2400 ГГц. Потужність передавачів ентузіастів може змінюватись від 10 дБм до 29 дБм. Чутливість давача від 90 до 105 дБм.

Звідси за знайдемо на якій відстані давачі зможуть виявити електромагнітне випромінювання. Тут $P_{\text{вих}} = 10$ до 29 дБм. $P_{\text{вхід}}$ має бути від 90 до 105 дБм.

На рис. 3.2 наведено графік для визначення залежності радіуса дії давача від чутливості і потужності.

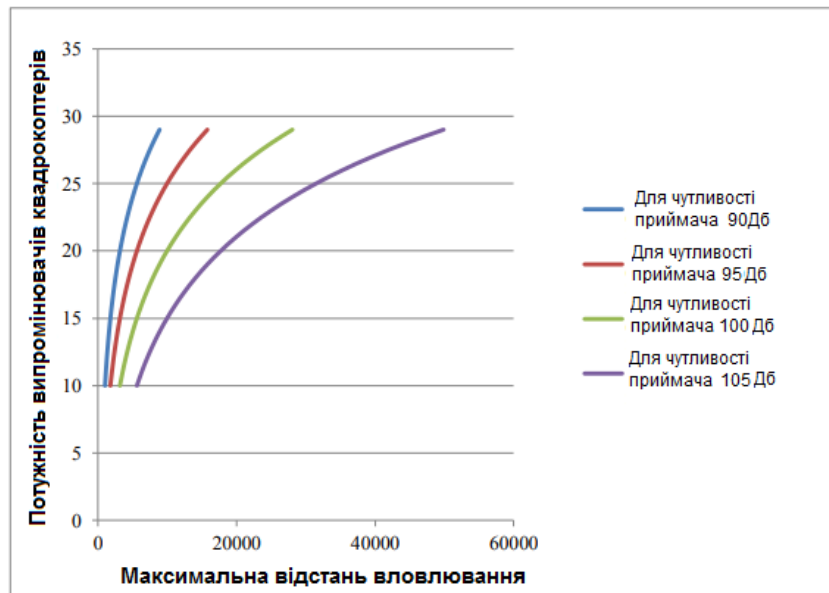


Рис. 3.2. Графік залежності радіусу дії давачів від чутливості приймача давачів та потужності передавача квадрокоптера

3.3.3. Програмна реалізація в Python. Python є високорівневою універсальною мовою програмування, котра спрямована на збільшення ефективності праці програмістів та читабельності коду. Синтаксис Python мінімальний. Існує досить багато різних прикладних бібліотек мови, які містять значне число потрібних функцій.

Показовим втіленням Python є компілятор CPython, котрий містить засоби підтримки тих платформ, котрі застосовуються найактивніше [11]. Існує безкоштовна ліцензія Python Software Foundation, яка дає змогу застосовувати його цілковито у будь-яких застосунках, у тому числі й пропрієтарних [12].

Фрагмент програмного коду наведено на рис. 3.3.

```

f = open("Data.txt" '7r', encoding = 'utf-8') «Відкриває текстовий
документ з даними отриманими від датчиків БСМ»
lst1 = list(f.readline(1))
lst2 = list(f.readline(2))
lst3 = list(f.readline(3))
lst4 = list(f.readline(4))
lst5 = list(f.readline(5))
lst6 = list(f.readline(6))
lst7 = list(f.readline(7))
lst8 = list(f.readline(8))
lst_centre = [0, 1, 3, 5, 7]
«Зчитує дані з рядків для кожного давача»
for i in range(len(lst1)):
....

```

Рис. 3.3. Фрагмент коду алгоритму

3.3.4. Особливості моделювання мережі в Matlab. При аналізі функціонування багатостадійних обслуговуючих комплексів БСМ одним із ключових завдань є оцінка за допомогою моделювання. Взаємна залежність між вузлами роботи, а також їх стохастичний характер їх тривалості не дозволяє гарантувати необхідну точність при отриманні відповідних оцінок шуканої випадкової величини. Імітація процесу обслуговування дозволяє спростити розуміння законів розподілу різних величин та зібрати докладні відомості, оцінити їх числові характеристики, розрахувати ризики затримки обслуговування та вирішити низку інших необхідних завдань.

Дослідження специфіки розв'язуваної задачі дозволило висунути низку вимог до системи, призначеної для моделювання багатостадійного обслуговування. З урахуванням специфіки функціонування досліджуваних комплексів, а також на підставі вимог, що пред'являються до системи, було розроблено її структуру та визначено призначення основних підсистем. Таким чином, розроблена система імітаційного моделювання, призначена для моделювання процесу функціонування багатостадійних обслуговуючих комплексів та забезпечує можливість збирання та аналізу статистичних даних про випадкову величину, що описує тривалість проекту.

Агентне моделювання добре підходить для концепції моделювання БСМ.

Оскільки мережні вузли розподілені по всій площі, активно співдіють із оточуючим середовищем та вузлами по сусідству. Відомо, що поведінка і параметри одного із вузлів БСМ чинять вплив на продуктивність усієї мережі. У підході дискретних подій увага приділяється конкретному процесу, що вже розглядається.

Можливості програми Matlab охоплюють практично всі галузі математики. Matlab як мова програмування використовується безпосередньо під час роботи з програмою. В даний час Matlab дуже популярний

Привабливість середовища на вирішення цих завдань полягає у забезпеченні інструментами та редактором для візуальної симуляції. Саме наявність спеціалізованих інструментів є основною причиною вибору Matlab як інструменту для моделювання обчислень у бездротовій сенсорній мережі.

Можливість обробки великих масивів даних дозволить оцінити розроблений метод на велику кількість вузлів.

При моделюванні БСМ у середовищі Matlab вузли з'єднуються між собою не напряму, а завдяки модуль бездротового каналу та служать свідченням передавання повідомлень від одного модуля до іншого. На додачу вони зв'язані із тими фізичними процесами, котрими вони керують. Кожен фізичний процес передбачає свій модуль.

Моти перебувають у взаємодії з фізичним процесом просторово і часово (надсилаючи повідомлення відповідному модулю) для отримання показів давачів. Там можливо декілька фізичних процесів, котрі визначають кілька давачів.

3.4. Модель розрахунку споживання БСМ у режимі точка- багато точок

Тут представлено порівняння способів інсталяції сенсорних вузлів покриття заданої області при використанні різних способів: випадкового розміщення і детермінованого розміщення. Розглянуто методи підвищення енергоефективності сенсорних вузлів для виявлення квадрокоптера.

Розглянуто два аспекти функціонування БСМ: по-перше, забезпечення покриття території, для чого використовується алгоритм випадкової інсталяції

сенсорних вузлів та подальша оцінка якості покриття заданої області. По-друге, підвищення енергоефективності мережі, навіщо використано метод підвищення енергоефективності сенсорних вузлів.

Як відомо, існує два основних способи інсталяції вузлів у БСМ: випадкове розміщення та детерміноване розміщення [3]. Випадкове розміщення, зазвичай, використовуються для великомасштабних БСМ не тільки тому, що це вимагає менших витрат, але також і тому, що в ряді випадків такий спосіб може бути єдиною можливим.

Однак, випадкове розміщення сенсорних вузлів може призвести до появи неконтрольованих зон; тому, у більшості випадків, випадкове розміщення не буде ефективно для досягнення максимального покриття [4].

Розглянемо можливість покриття при випадковому розміщенні сенсорних вузлів на заданій території. Буде використано двійкову модель, яка розглянута та наведена у додатку Б. У цій моделі кожен сенсорний вузол має однаковий і постійний радіус дії сенсора. Область обслуговування накриємо сіткою ліній $n \times m$, з розміром кожної комірки сітки рівної 1. Двійкова модель передбачає, що частка покриття області в межах обслуговування апроксимується часткою покритих вузлів сітки. Покриття всієї області пропорційне числу покритих вузлів решітки (рис. 3.4). Для опису покриття вузлів сітки $G(x, y)$ введемо двійкову функцію, значення якої дорівнює 1 якщо вузол потрапляє в зону покриття сенсора/

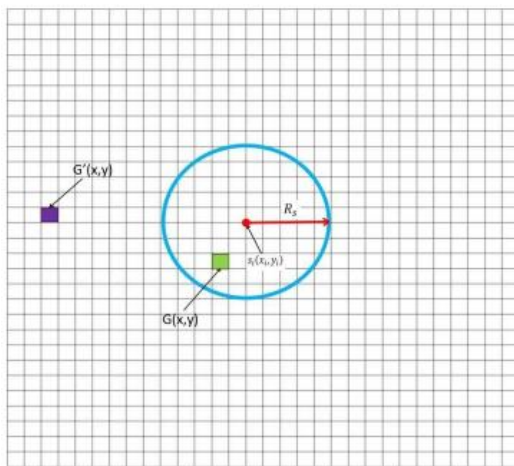


Рис. 3.4. Покриття вузлів сітки сенсорним вузлом

Розглянемо моделі БСМ з розстановкою випадковим і детермінованим способом. У першій моделі сенсорні вузли розподілені рівновіддалено від центру та один від одного на площині розміром 250м*250м. Число вузлів у мережі становить дев'ять, і базова станція знаходиться на межі сенсорного поля з координатами (150, 150) м (рис. 3.5).

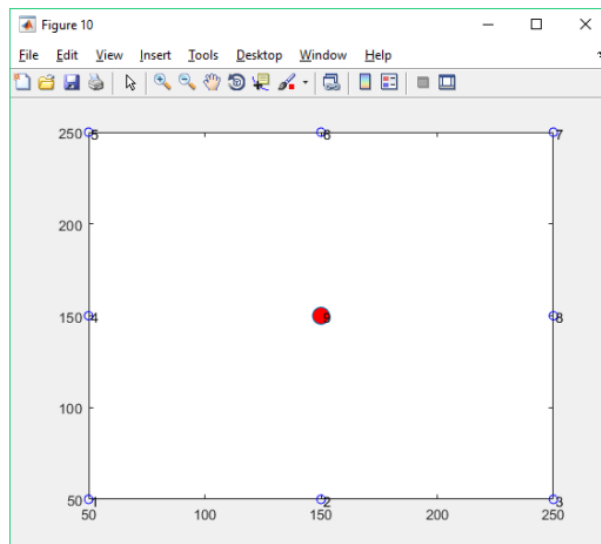


Рис. 3.5. Перша модель БСМ

Головний вузол має постійне джерело енергії. Інші вузли живляться від крони 9В із запасеною енергією в 8,5 Дж. Час життя моделі 2000 циклів.

Таблиця 3.1

Стан давачів для моделі 1

Номер вузла	Координати вузла по x	Координати вузла по y	Відстань від головного	Залишок енергії на 2000 циклів
1	50	50	141,42	4,79
2	150	50	100	7,37
3	250	50	141,42	4,79
4	50	150	100	7,37
5	50	250	141,42	4,78
6	150	250	100	7,37
7	250	250	141,42	4,79
8	250	150	100	7,37
Головний вузол	150	150	[]	[]

Судячи з табл. 3.1, отриманої в Matlab, для цієї моделі утворюються дві групи. Одна група з відстанню від центру 141 м і залишком енергії 4,79 Дж. Друга група з відстанню 100 м і залишком енергії 7,37 Дж.

На рис. 3.6 наведено графік зміни енергії.

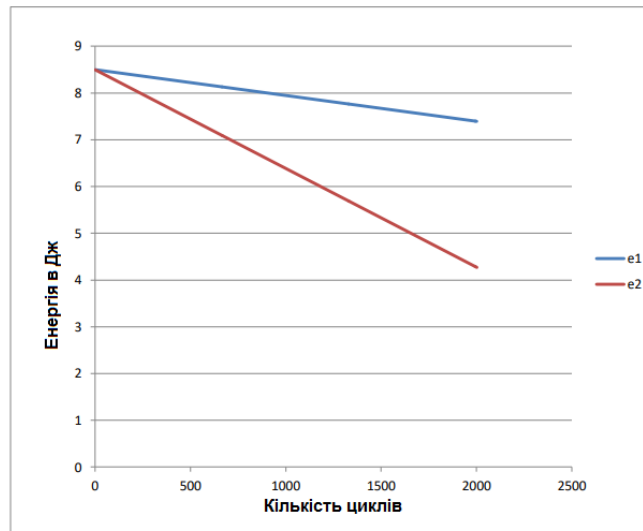


Рис. 3.6. Зміна енергії за 2000 циклів для двох груп давачів

У другій моделі сенсорні вузли розподілені випадково, віддалено від центру та один від одного на площині розміром 250м*250м. Число вузлів у мережі становить дев'ять і базова станція знаходиться на межі сенсорного поля з координатами (150, 150) м (рис. 3.7). Головний вузол має постійне джерело енергії. Інші вузли живляться від крони 9В із запасеною енергією в 8,5 Дж. Час життя моделі 2000 циклів.

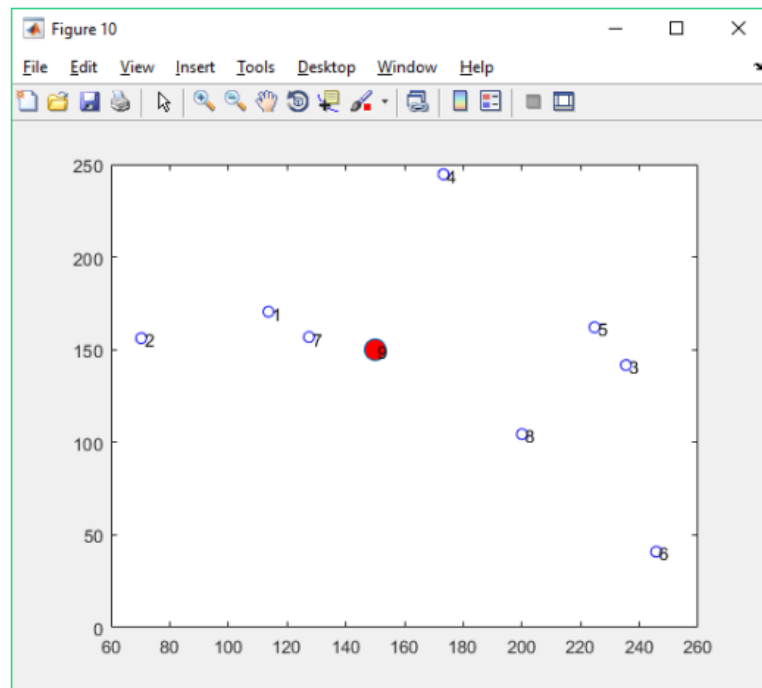


Рис. 3.7. Друга модель БСМ

У другій моделі немає певних груп, тому що великий розкид. Він нам не підходить через не повне охоплення області, що охороняється. За табл. 3.2 видно, що чим більша відстань, то менше енергії.

Таблиця 3.2

Стан давачів для моделі 2

Номер вузла	Координати вузла x	Координати вузла по y	Відстань від головного	Залишок енергії на 2000 циклів
1	113,66	170,52	41,73	8,27
2	70,315	156,22	79,92	7,97
3	235,43	141,7	85,83	7,89
4	173,28	244,65	97,46	7,50
5	224,78	162,12	75,75	7,98
6	245,73	40,954	145,1	4,65
7	127,45	156,84	23,56	8,37
8	200	104,44	67,64	8,05
Головний вузол	150	150	[]	[]

На рис. 3.8 представлено графік зміни енергії.

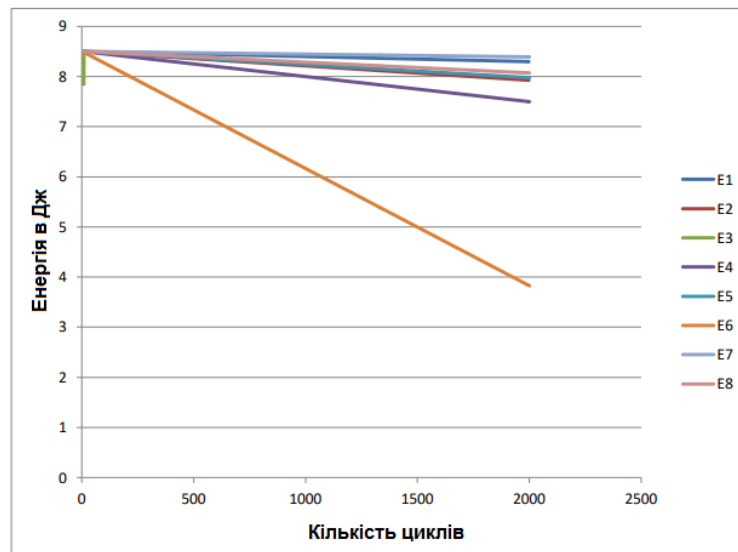


Рис. 3.8. Зміна енергії за 2000 циклів для восьми давачів

У третій моделі сенсорні вузли розподілені рівновіддалено від центру та один від одного на площині розміром 250м*250м. Число вузлів у мережі становить п'ять і базова станція знаходиться на межі сенсорного поля з координатами (150, 150)м (рис. 3.9). Головний вузол має постійне джерело енергії. Інші вузли заживляються від крони 9В із запасеною енергією в 8,5 Дж. Час життя моделі 2000 циклів.

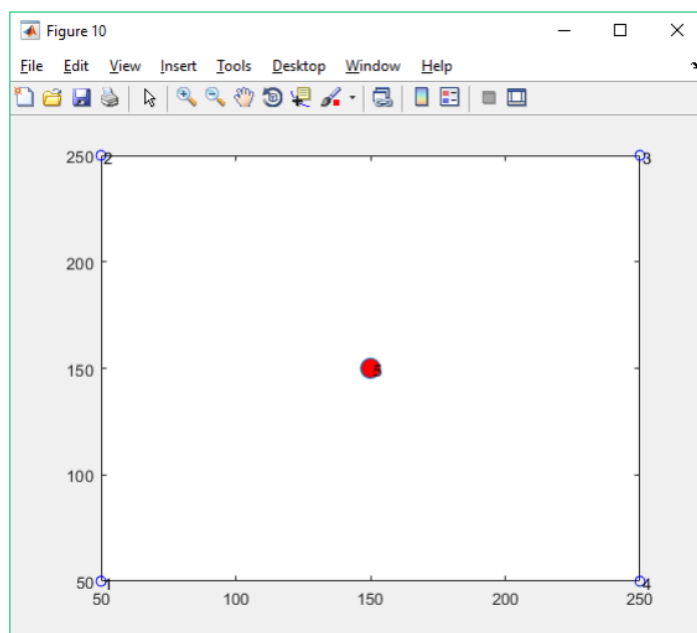


Рис. 3.9. Третя модель БСМ

Стан давачів для моделі 3

Номер вузла	Координати вузла по x	Координати вузла по y	Відстань від головного	Залишок енергії на 2000 циклів
1	50	50	141,42	4,30
2	50	250	141,42	4,30
3	250	250	141,42	4,30
4	250	50	141,42	4,30
Головний вузол	150	150	□	□

У третій моделі одна група давачів, оскільки вони рівновіддалені від центру.

На рис. 3.10 представлено графік зміни енергії.

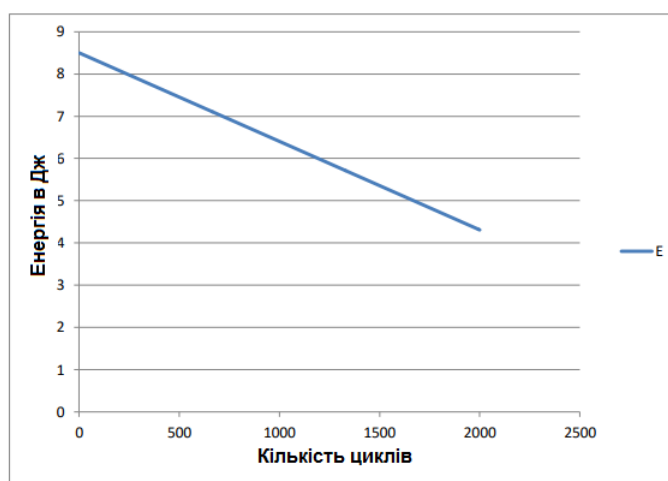


Рис. 3.10. Зміна енергії за 2000 циклів для 1 групи давачів

У четвертій моделі сенсорні вузли розподілені випадково, віддалено від центру та один від одного на площині розміром 250м*250м. Число вузлів у мережі становить п'ять, і базова станція знаходиться на межі сенсорного поля з координатами (150, 150) м (рис. 3.11). Головний вузол має постійне джерело енергії. Інші вузли живляться від 9В крони із запасеною енергією в 8,5 Дж. Час життя моделі становить 2000 циклів.

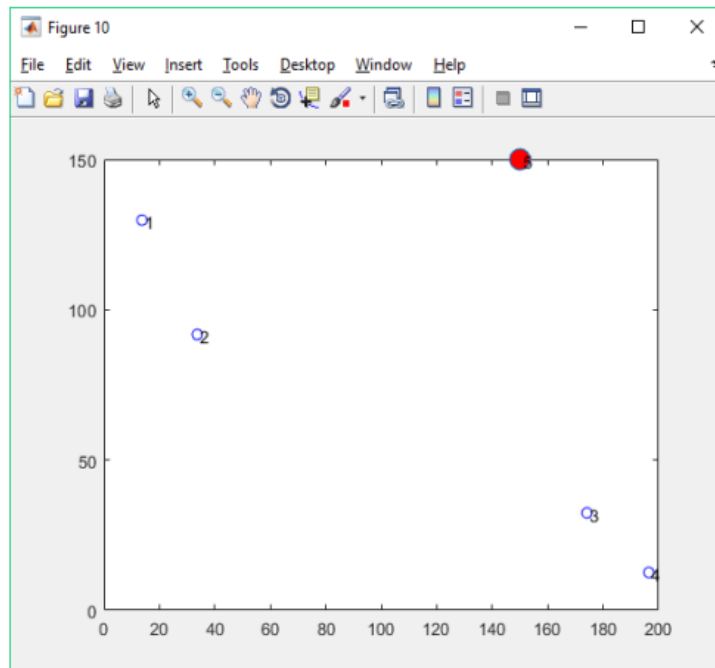


Рис. 3.11. Четверта модель БСМ

Таблиця 3.4

Стан давачів для моделі 4

Номер вузла	Координати вузла по x	Координати вузла по y	Відстань від головного	Залишок енергії на 2000 циклів
1	13,71	129,78	137,78	5,04
2	33,63	91,743	130,13	5,73
3	174,15	32,39	120,05	6,48
4	196,46	12,57	145,06	4,25
Головний вузол	150	150	□	□

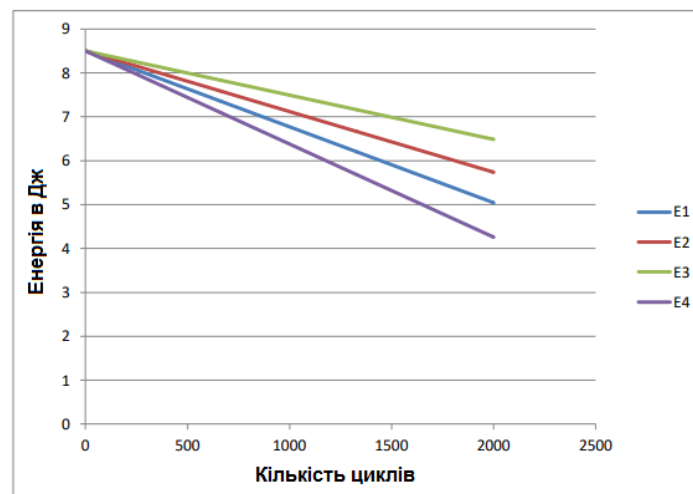


Рис. 3.12. Зміна енергії за 2000 циклів для 4 давачів

Проведений аналіз моделей свідчить, що за такої кількості датчиків у нашому випадку кращий детермінований спосіб розміщення датчиків. Він краще підходить для розміщення на конкретній області, що охороняється, так як датчики рівномірно покривають периметр, котрий охороняється. При випадковому розподілі видно, де датчики не тільки не покривають периметр, що охороняється, а навіть згрупувалися в одній області. По відстані в детермінованому способі розміщення дві групи датчиків були рівновіддалені від центру. Це вплинуло позитивно на залишок електроенергії, і на передбачення виходу з ладу датчиків через її нестачу, оскільки утворилося дві групи, одна з яких виходить з ладу трохи швидше. У другій моделі відстань від центру для кожного датчика різна. Це також позначилося на енергії, де залишок кожного датчика на завершення моделювання різний.

3.5. Висновок до розділу

У третьому розділі наведена інформація для здійснення дослідження та чинники, котрі впливають на створення моделі БСМ.

Описано алгоритм порівняння потужностей датчиків БСМ, пораховано радіуси дії, наведена програмна реалізація із використанням Python, наведено аспекти симуляції БСМ в середовищі Matlab.

Досліджено чотири різних моделі розрахунку споживання БСМ

На якість функціонування алгоритму матиме вплив розміщення датчиків відповідно до схеми та радіус детектування, а також електромагнітне випромінювання.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є розробка та дослідження алгоритмів, створення нової БСМ, яка згодом буде досліджуватися. Оскільки, проведення робіт з розробки та використання БСМ передбачає застосування комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки БСМ, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [33]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог;

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких

розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп'ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при

відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з розробки та дослідження алгоритмів, створення нової БСМ, яка згодом буде досліджуватися.

4.2. Функціонування державної системи спостереження, збирання, обробки та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу

Моніторинг довкілля – це система спостереження, збирання та аналізу інформації про ситуацію, що може скластись під час надзвичайних ситуацій мирного та воєнного часу. Також це система спостереження за визначеними об'єктами, явищами та процесами з метою оперативного оцінювання їх стану, виявлення результатів впливу на них зовнішніх чинників та прийняття відповідних управлінських рішень (ДСТУ 3891:2013) (див. ДСТУ 7295:2013).

Моніторинг потенційно небезпечних об'єктів це спостереження, контролювання за зміною параметрів технологічних режимів з метою збирання, збереження, передавання та аналізування інформації щодо поточного стану потенційно небезпечних об'єктів, наявності та кількості порушень вимог безпеки, відпрацювання рекомендацій щодо проведення 98 робіт із запобігання та ліквідування техногенних надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг джерел надзвичайних ситуацій це система спостереження за об'єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації стосовно стану об'єктів моніторингу та розроблення науково-обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування надзвичайних ситуацій (ДСТУ 7295:2013).

Моніторинг довкілля – це систематичні спостереження і контролювання, які проводять регулярно, за єдиною програмою для оцінювання стану довкілля, аналізування процесів, які відбуваються в ньому і своєчасне виявлення тенденцій його змінювання (ДСТУ 7295:2013).

Моніторинг надзвичайних ситуацій (НС) – система спостереження за об'єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної

інформації щодо об'єктів моніторингу та розроблення науково обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування НС [34].

Моніторинг небезпечних явищ та процесів це система спостереження та контролювання за розвитком небезпечних та стихійних природних явищ і процесів, чинниками, які спричиняють їх формування та розвиток, аналізування, збереження та передавання інформації щодо виявлення тенденцій їх змінювання, розроблення комплексу заходів щодо запобігання природним надзвичайним ситуаціям та ліквідування їх наслідків. Небезпечні природні явища і процеси підрозділяють на геофізичні, геологічні, гідрологічні, метеорологічні, медико-біологічні та пожежі в природних екосистемах (ДСТУ 7295:2013).

Моніторинг пожеж в екосистемах це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо 99 пожежної небезпеки в природних екосистемах (умов погоди, стану горючих матеріалів, інших пожежонебезпечних чинників), з метою своєчасного планування та здійснення заходів щодо запобігання виникненню і ліквідування пожеж та їх наслідків (ДСТУ 7295:2013).

Моніторинг радіаційної безпеки це спостереження і контролювання рівня радіоактивного забруднення місцевості, повітря, води, продовольства, об'єктів господарювання, дозових навантажень на населення з метою прийняття оперативних рішень щодо запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг хімічної небезпеки це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо визначення ступеня і характеру хімічного забруднення довкілля, санітарногігієнічний нагляд за дотриманням установлених нормативів з метою виявлення джерела надходження небезпечних хімічних речовин, запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Збір та аналіз інформації про стан довкілля під час мирного та воєнного стану дає можливість приймати оперативні рішення для адекватного реагування на ситуацію [34].

4.3. Висновки до розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки в надзвичайних ситуаціях, висвітлено питання функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного час.

ВИСНОВКИ

У роботі описаний алгоритм функціонування, порівняння потужностей виконуватиме функцію детектора дронів БСМ. На якість роботи алгоритму впливатиме розташування давачів згідно зі схемою та радіус виявлення, а також електромагнітне випромінювання.

Доведено, що чим краща чутливість давачів, тим на більшій відстані можуть вони вловлювати електромагнітне випромінювання. Для чутливості приймача 90 ДБ, і мінімальної потужності електромагнітного випромінювання квадрокоптера він становив 995 м, а для чутливості 105 Дб - 5596 м при тому ж випромінюванні. Дане дослідження проводилося з метою виявити можливість зменшення кількості мотів, використовуючи більш чутливі давачі, дійсно можна зменшити їх кількість, так як вони покриватимуть велику зону, і з метою оцінки ефективності роботи даної БСМ. Через протокол ZigBee відстань між мотами БСМ має бути меншою за 627 м. Звідси протокол ZigBee не підходить для такого типу БСМ, якщо відстань між мотами більша за 627 м без урахування перешкод.

В результаті даної роботи отримано порівняльну характеристику випадкового та детермінованого методів розміщення вузлів БСМ для гарантування покриття площі обслуговування. Експериментально доведено, що детермінований спосіб розміщення вузлів за умови досить точного розміщення вузлів забезпечує більшу ефективність.

Результати проведеного аналізу показали, що при обмеженій точності розміщення вузлів, а також при менш жорстких вимогах до частини покриття, випадкове розміщення вузлів може бути співставне за ефективністю з детермінованим.

Розроблено метод організації БСМ при детермінованому розміщенні вузлів для виконання операцій збору даних.

Запропонований метод кластерної організації мережі дозволяє суттєво знизити енерговитрати мережі на роботу зі збору даних.

У подальшому передбачається дослідити моделі випадкового розміщення

сенсорних вузлів, що забезпечують покриття заданої області великою кількістю вузлів та методи мінімізації витрати енергії в таких мережах.

Отримані результати можуть бути використані в охоронних системах безпеки, у захисті військових об'єктів та об'єктів державної ваги, що не допускають на свою територію проникнення дронів тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015,
2. A. Caric and K. Toivo, "New generation network architecture and software design," in IEEE Communications Magazine, vol. 38, no. 2, pp. 108-114, Feb. 2000
3. Основи радіоелектроніки : навчальний посібник / В. М. Кичак, Ю. В. Крушевський, Д. В. Гаврілов. Вінниця : ВНТУ, 2010. 368 с..
4. Проектування ефективних систем безпроводного зв'язку / М. М. Климаш, В. О. Пелішок. Львів, 2010. 232 с.
5. Siva Ram Murthy C., Manoj B.S. Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, 2004. 880 p.
6. Що таке ZigBee в IoT? Повний путівник у 2024 році. URL: <https://www.dusuniot.com/uk/blog/the-definitive-guide-for-zigbee-gateway-for-solution-vendors/> (дата звертання 26.11.2024).
7. Гераїмчук М. Д. Основи побудови перспективних безпроводових сенсорних мереж : моногр. / М. Д. Гераїмчук, О. В. Івахів, М. І. Паламар, Б. М. Шевчук. К. : ЕКМО, 2010. 124 с.
8. Крайник Н.М. ZIGBEE GREEN POWER // Інформаційні моделі, системи та технології: Праці XII наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 18-19 грудня 2024 р.) С. 65.
9. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. Київ: Наукова думка, 2017. 730 с.
10. Крайник Н.М. Вимоги до бездротових сенсорних мереж // Інформаційні моделі, системи та технології: Праці XII наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 18-19 грудня 2024 р.) с. 67.
11. P. Bauer, M. Sichitiu, R. Isteanian, K. Premaratne, The mobile patient: wireless distributed sensor networks for patient monitoring and care, Proceedings 2000

IEEE EMBS International Conference on Information Technology Applications in Biomedicine, 2000, pp. 17-21.

12. M. Bhardwaj, T. Garnett, A.P. Chandrakasan, Upper bounds on the lifetime of sensor networks, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.

13. Луцик Н. С., Луцків А. М., Осухівська Г. М., Тиш Є. В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. ТНТУ. 2024. 44 с

14. Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Програма та методичні рекомендації з проходження практики за тематикою кваліфікаційної роботи для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. ТНТУ. 2024. 45 с.

15. Варавін А.В., Лещишин Ю.З., Чайковський А.В. Методичні вказівки до виконання курсового проєкту з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль. ТНТУ, 2024. 32 с.

16. Felemban, E. Advanced border intrusion detection and surveillance using wireless sensor network technology. International Journal of Communications, Network and System Sciences, 2013, 6(05), pp. 251-259.

17. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 1 [навчальний посібник]. Львів : «Магнолія 2006», 2013. 256 с.

18. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с..

19. Velychko D., Osukhivska H., Palaniza Y., Lutsyk N., Sobaszek L. Artificial Intelligence Based Emergency Identification Computer System. *Advances in Science and Technology Research Journal*, 18 no. 2, 2024, P. 296-304.

20. Skorenkyy Y., Kozak R., Zagorodna N., Kramar O., Baran, I. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cybersecurity education. *Journal of Physics: Conference Series*. 2021. Vol. 1840, No. 1. DOI: <http://dx.doi.org/10.1088/1742-6596/1840/1/012026>

21. Wireless Sensor Network (WSN). URL: <https://www.geeksforgeeks.org/wireless-sensor-network-wsn/> (дата звертання 28.11.2024).

22. Osseiran, A. The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions / A. Osseiran, V.Braun, H. Taoka, P. Marsch, H. Schotten, H. Tullberg, MAUusitalo, M.Schellman // *Vehicular Technology Conference (VTC Spring)*, 2013 IEEE 77th. IEEE, 2013. C. 1-5.

23. Palamar A., Palamar M., Osukhivska H. Real-time Health Monitoring Computer System Based on Internet of Medical Things. *CEUR Workshop Proceedings, 3rd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2023)*, Ternopil, Ukraine, Opole, Poland, November 22–24, 2023. Vol. 3628. P. 106-115.

24. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyy R. Technology of relational database management systems performance evaluation during computer systems design. *Scientific Journal of TNTU*, Ternopil, Ukraine, 2023. Vol. 109, No 1. P. 54–65.

25. Shabliy N., Lupenko S., Lutsyk N., Yasniy O., Malyshevskaya O. Keystroke dynamics analysis using machine learning methods. *Applied Computer Science*. 2021. Vol. 17, No. 4. P. 75-83

26. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. *CEUR Workshop Proceedings, 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022)*, Ternopil, Ukraine, November 22–24, 2022. Vol. 3309. P. 194-204

27. Lupenko S., Lutsyk N., Yasniy O., Sobaszek Ł. Statistical analysis of human heart with increased informativeness. *Acta mechanica et automatica*. 2018. Vol. 12. No. 4. P. 311–315. DOI: <https://doi.org/10.2478/ama-2018-0047>
28. Yatsyshyn V., Pastukh O., Palamar A., Zharovsky R. Technology of relational database management systems performance evaluation during computer systems design. *Scientific Journal of TNTU*. 2023. Vol. 109, No 1. P. 54–65
29. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с
30. Lupenko S., Orobchuk O., Stadnik N., Zozulya A. Modeling and signals processing using cyclic random functions. In *Proceedings of the 13th IEEE International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. Lviv, Ukraine, 11–14 September, 2018. P. 360–366.
31. Лупенко С. А., Пасічник В. В., Тиш Є. В. Комп'ютерна логіка. Львів: Видавництво «Магнолія - 2006». 2015. 354 с.
32. Tysh Ie. Approach And Method Of Evaluation Of The General Reliability Indicator Of Computer Systems. *International Scientific Journal Computer Systems And Information Technologies*. Khmelnytskyi : Khmelnytskyi National University. №3. 2021. С.74-80.
33. Заїкіна Д., Глива В. Основи охорони праці та безпека життєдіяльності. 2019. URL: <https://doi.org/10.31435/rsglobal/001> (дата звернення: 14.12.2024).
34. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / укл.: Стручок В. С. Тернопіль: ФОП Паляниця В. А., 2022. 156 с.

ДОДАТОК А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

МАТЕРІАЛИ

ХІІ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

**«ІНФОРМАЦІЙНІ МОДЕЛІ,
СИСТЕМИ ТА ТЕХНОЛОГІЇ»**



18-19 грудня 2024 року

ТЕРНОПІЛЬ
2024

ZIGBEE GREEN POWER

O.V. Krainyk

ZIGBEE GREEN POWER

Альянс ZigBee, активний розробник стандартів і рішень для бездротових сенсорних мереж (BSM), оголосив у 2009 році про своє рішення випустити стандарт ZigBee Green Power (GP) для пристроїв з власними альтернативними джерелами живлення, заснованими на технології запозичення енергії. Грунтуючись на стандарті ZigBee GP, у 2014 році NXP Laboratories, випустила Посібник із використання стандарту GP під час роботи з мікроконтролерами серії NXP jn516x.

– використання більш короткого формату кадрів GP і, отже, меншого часу передачі, ніж у разі кадрів ZigBee стандартного формату IEEE 802.15.4, що дозволяє заощаджувати енерговитрати на передачу;

– вузли не обов'язково повинні бути повноцінними компонентами BSM, можливо, що вузли передають дані лише у разі потреби.

Кадр GP відноситься до проксі-вузла, який є компонентом сенсорної мережі та оснащений «тунелем», який перетворює кадр GP на звичайний формат кадру ZigBee для повторної передачі в сенсорну мережу. Кластер GP не потребує вихідного вузла, але повинен взаємодіяти як з проксі-вузлом, так і з дренажем, щоб отримати кадри GP, що інтерпретуються. Базовий алгоритм стандарту GP ZigBee показано на рис. 1., де кадр 1 - це кадр GP, а кадр 2 - тунельований кадр GP.

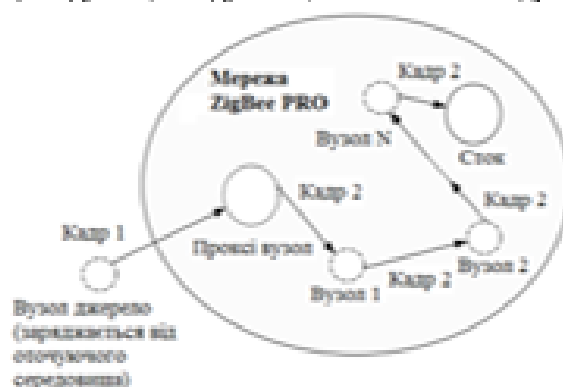


Рисунок 1 – Базовий механізм ZigBee GP

Переваги використання ZigBee GP полягають у наступному:

– підходить для вузлів, розташованих з можливістю підтримки роботи;

– можливість використання вузлів, основні джерела енергії при яких, батареї належним чином не захищені або недоступні, а також використання ізольованих вузлів або вузлів, розташованих небезпечно;

– використання відновлюваних джерел енергії вузлами;

– можливість усунення потреби в

батареї у вузлах BSM, колективне підтримання працездатності, споживання та відновлення енергії;

– дешева, швидка та проста установка вихідних вузлів.

Таким чином, можна сказати, що для оснащення BSM можливістю запозичення енергії з навколишнього середовища пропонуються як готові рішення (наприклад, Silicon Lab), так і стандарти для створення модулів для запозичення енергії з навколишнього середовища.

Можна виділити Zigbee Alliance, яка розробила спеціалізований стандарт GP standard для доповнення стандартної мережі відновлюваними джерелами енергії. Ну, а як сфери застосування даної технології, щоб підвищити енергетичний потенціал сенсорної мережі можна розглянути розробку енергонезалежних модулів для BSM.

ВИМОГИ ДО БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

O.V. Krainyk

REQUIREMENTS FOR WIRELESS SENSOR NETWORKS

Автономія. Ліквідація якогось вузла бездротової сенсорної мережі (БСМ) не має нести впливу на її функціонування. Так як мережа не має мати центрального вузла, який-небудь користувач здатен здійснювати функції віддаленої маршрутизації.

Енергетична ефективність. Протоколи маршрутизації мають максимально ефективно використовувати енергію.

Масштабованість. БСМ складаються із сотень вузлів, саме тому протоколи маршрутизації повинні функціонувати з таким їх числом.

Стабільність. Давачі здатні раптово перестати працювати через поломку батареї живлення або із якихось зовнішніх причин. Маршрутизаційні протоколи мають опрацьовувати цю ймовірність так, щоб якщо струм у мотях пропаде, можна було використовувати альтернативний маршрут.

Неоднорідність приладів. Хоча більшість додатків БСМ залежить від однорідності вузлів, використання різних типів давачів може забезпечити значний привілей.

Мобільність. За певних подій вузли здатні переміщуватися під час роботи.

Особливості та обмеження БСМ створюють спеціальні умови до маршрутизаційних протоколів.

Базується на параметрах. Для цих алгоритмів вузол надсилає запити до певних ділянок мережі та очікує відповіді від давачів, розташованих у цій частині. Вибір параметрів перебуває у залежності залежить від визначеної програми. Головна особливість такої схеми – зміст меседжу даних піддається аналізу під час кожного етапу маршрутизації.

Енергетична ефективність. У цих алгоритмах можна вибрати шляхи, котрі, як сподівається, найбільше сприятимуть зберіганню енергії в мережі. З цією метою маршрут містить вузли із вищими енергетичними ресурсами.

Агрегування даних. Відносно близькі вузли можуть робити аналогічні дані, котрі здатні поєднуватися з деякою прийнятною втратою точності.

Застосування давачів істотно залежить від зв'язку між мотами, так як це потрібно для втілення визначених алгоритмів або процедур. На ділі є три головні типи алгоритмів маршрутизації для БСМ – централізовані, розподілені і локальні.

Алгоритми, що використовуються, є важливим фактором, який необхідно враховувати при виборі маршрутизаційного алгоритму. Коли застосовуються локальні алгоритми, тоді основною буде значна комунікаційна зв'язаність вузлів, які знаходяться поруч. Для централізованих алгоритмів консолідація повідомлень буде значним привілеєм. Розподілені ж алгоритми мають надавати вірне з'єднання між двома мережевими мотами. Для локальних алгоритмів варто зважати на те, що застосування побічних механізмів позиціонування (як варіант GPS) здатне досить збільшити вартість такої мережі.

Класифікація за методом розрахунку шляхів: проактивні протоколи - всі шляхи розраховуються заздалегідь, як вони знадобляться; реактивні протоколи - шляхи розраховуються на вимогу; гібридні протоколи – це поєднання двох підходів.