ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра автоматизації, комп'ютерно-інтегрованих технологій та телекомунікацій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему «Розробка моделей та засобів для оцінки протоколів маршрутизації в безпротових сенсорних мережах»

ДРТР.201909017.06ПЗ

Виконав: студент 2 курсу, група ТР.-19-1 _____ А. І. Жалюк
підпис Ініціали, прізвище

Керівник: кандидат військ. наук, доцент _____ В. І. Лужанський
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, проф. _____ В.В. Мартинюк
підпис Ініціали, прізвище

10 12 2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *автоматизації, комп'ютерно-інтегрованих технологій і телекомунікацій*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність *172 – Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою_АКІТ і ТК В.В. Мартинюк_В.В.
«1» 09 2020р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

магістранту *Жалюку Андрію Івановичу*

1 Тема роботи: *Розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах* керівник роботи Лужанський В.І., к.в.н, доцент.
Затверджено наказом по університету від «1» вересня 2020р. № 118.
2 Строк подання студентом роботи на кафедру:05.12.2020р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи: детальне вивчення розробки моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах.
Об'єкт дослідження: бездротова сенсорна мережа.
Предмет дослідження: засоби для оцінки протоколів маршрутизації в бездротових сенсорних мережах.
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
Вступ. Аналіз інструментів моделювання. Аналіз протоколів маршрутизації. Моделі оцінки протоколу з одним стрибком. Моделі оцінки протоколу LEACH.

Завдання отримав А.І. Жалюк
Науковий керівник В.І. Лужанський

2

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз вітчизняної та зарубіжної наукової літератури по тематиці дипломної роботи	До 1.09.2020р	виконано
2	Аналіз інструментів моделювання	До 20.09.2020р	виканано
3	Протоколи маршрутизації	До 15.10.2020р	виканано
4	Моделі оцінки протоколу Single-hop	До 01.11.2020р	виканано
5	Моделі оцінки протоколу Leach	До 25.11.2020р	виканано
6	Підготовка дипломної роботи до друку	До 1.12.2020р	виканано
8	Підготовка та подання дипломної роботи на антиплагіат	До 03.12.2020р	виканано
9	Подання дипломної роботи до захисту	До 05.12.2020р	виканано

Студент _____ А.І.Жалюк

Керівник роботи _____ В.І. Лужанський

Зміст

Вступ

Актуальність теми. Бездротові сенсорні мережі, як правило, використовуються в різних сферах застосування, включаючи промислові, військові та цивільні. Це призводить до популяризації досліджень маси протоколів маршрутизації. В умовах збільшення частки таких протоколів особливої актуальності набуває детальне вивчення основних параметрів оцінки для розробки моделей бездротових сенсорних мереж та засобів їх моделювання.

Актуальність роботи обумовлена проблемами в галузі первинного дослідження, а саме енергоспоживання датчиків в бездротовій сенсорній мережі і поліпшення точності даних, сформованих на різноманітних параметрах оцінки. Бездротова сенсорна мережа складається з безлічі датчиків, розгорнутих у випадковому порядку або в заздалегідь визначеному стані в даному просторі. Такі датчики призначені для вимірювання однієї або декількох фізичних величин у просторі, таких як місце розташування або температура. Датчики повинні передавати ці зібрані дані керівнику або кінцевому користувачеві через Інтернет. Оскільки датчики, про які йде мова, є бездротовими, вони, як правило, живляться від батареї з обмеженим терміном служби та вихідною потужністю; майже неможливо зарядити або замінити такі батареї.

Таким чином, у реальній бездротовій сенсорній мережі необхідно враховувати ряд параметрів, таких як споживання енергії та термін служби мережі.

Мета дипломної роботи:

є детальне вивчення розробки моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах. Висвітлення взаємозв'язку між параметрами оцінки для визначення впливу кожного з них на певний протокол маршрутизації на основі інструменту моделювання J-Sim.

Для досягнення цієї мети необхідно розв’язати такі **завдання:**

- розробити структурну схему параметрів оцінки протоколів маршрутизації;

- розробити алгоритм взаємозв'язку між параметрами оцінки, щоб показати, що зміна одного параметра впливає або не впливає суттєво на інший;

- удосконалити методи оцінки протоколів маршрутизації в бездротових сенсорних мережах.

Об’єктом дослідження є процес роботи бездротової сенсорної мережі.

Предметом дослідження є засоби для оцінки протоколів маршрутизації в бездротових сенсорних мережах.

Методи досліджень:

При вирішенні поставлених завдань у роботі були використані засоби моделювання на основі Java, а також методи алгоритмізації та програмування.

Наукова новизна отриманих результатів:

Досягнуто кілька корисних результатів за допомогою моделювання. Було запропоновано певні моделі оцінки, засновані на різних протоколах маршрутизації в бездротових сенсорних мережах. Також висвітлює взаємозв'язок між параметрами оцінки, щоб показати, що зміна одного параметра впливає або не впливає суттєво на інший.

Практичне значення одержаних результатів:

У роботі розроблена система методів оцінки протоколів маршрутизації в бездротових сенсорних мережах у реальному масштабі часу на основі використання ряду параметрів, таких як споживання енергії та термін служби мережі. Використання такої системи дозволяє підвищити ефективність використання бездротових сенсорних мереж у ще більшій кількості галузей, окрім тих, що зазначені в даній магістерській роботі.

Магістерська робота складається з вступу, чотирьох розділів, загальних висновків по роботі та списку використаних джерел.

У вступі обґрунтована актуальність наукової задачі, сформульовано мету та задачі досліджень, відображено основні наукові результати та їх практичне значення.

У першому розділі магістерської роботи обговорюються ключові терміни, необхідні для розуміння цілей даної дипломної роботи: бездротові сенсорні мережі, J-Sim, параметри оцінки та протоколи маршрутизації..

У другому розділі розглянуто приклади трьох основних типів протоколів маршрутизації, а саме плоских, ієрархічних та заснованих на розташуванні.

У третьому та четвертому розділах магістерської роботи розглянуто протоколи Single-hop, LEACH та ближнього зв'язку, засновані на інструменті моделювання J-Sim, і знайдено кілька корисних результатів аналізу серед кількох ключових параметрів. На основі цих результатів побудовано математичну модель для кожного з трьох протоколів.

У загальних висновках по магістерській роботі висвітлені основні результати досліджень, які отримані в магістерській роботі.

Апробація результатів досліджень: результати досліджень представлені у збірнику наукових праць за матеріалами XI всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2019», Том1.

Розділ 1. Аналіз інструментів моделювання

У цьому розділі подано вступ до бездротових сенсорних мереж та їх застосувань. Як правило, вузли датчиків є дорогими і їх важко перевірити у великій кількості, тому інструменти моделювання стають необхідними для формування мереж. У цьому розділі також буде обговорена проблема управління енергією та представлені параметри моделювання та протоколи маршрутизації.

1.1. Бездротові сенсорні мережі

Датчик [1] - це конвертер, який вимірює фізичну величину і перетворює її в сигнал, який може зчитувати електронний прилад. Наприклад, термоелемент перетворює температуру на вихідну напругу, яку можна зчитати вольтметром. Датчики повинні бути розроблені так , щоб мати невеликий вплив на те, що вимірюється; зменшення датчика часто покращує це і може створити інші переваги. Технологічний прогрес дозволяє все більше і більше датчиків виготовляти в мікроскопічному масштабі як мікросенсори з використанням технології Micro-Electro-Mechanical Systems ‘(MEMS) [2–5]. MEMS складається з компонентів розміром від 1 до 100 мікрометрів, а пристрої MEMS зазвичай мають розмір від 20 мікрометрів до міліметра. Зазвичай вони складаються з центрального блоку, який обробляє дані (мікропроцесор), і декількох компонентів, які взаємодіють із зовнішнім середовищем, таких як мікросенсори. Таким чином, технологія MEMS дозволила побудувати вузли датчиків, здатних зондувати, обробляти та обмінюватися даними.

Бездротова сенсорна мережа [6–7] складається з просторово розподілених автономних датчиків для спільного моніторингу фізичних або екологічних умов, таких як температура, звук, тиск, рух. Наступний рисунок ілюструє типову модель передачі даних такої мережі.

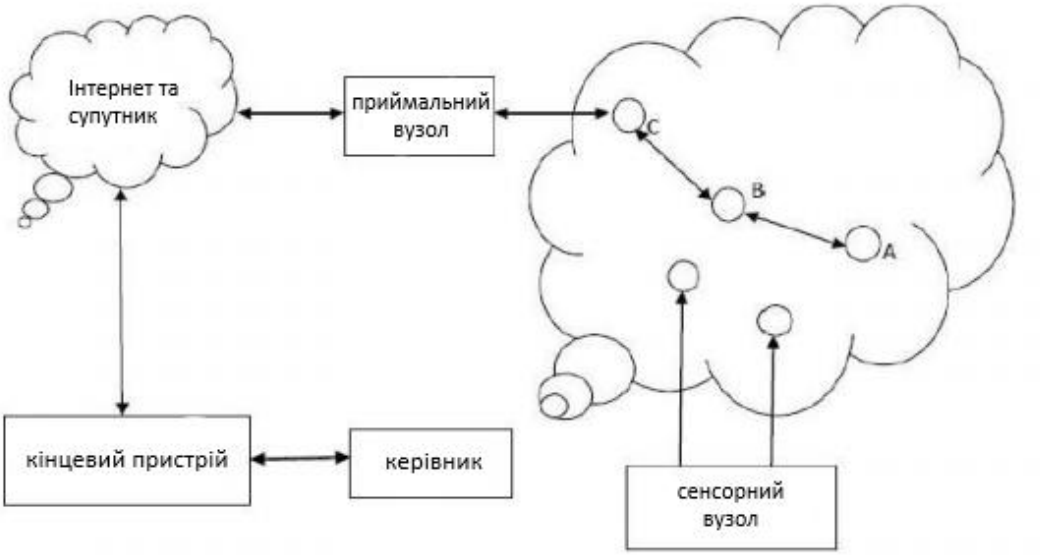


Рисунок 1.1 − Модель передачі даних бездротової сенсорної мережі

Вузол датчика передає дані на відповідні датчики, і, нарешті, оброблені дані надходять на сенсорний вузол або приймальний вузол, який підключений до кінцевого пристрою через інтернет або супутник. (Кінцевий пристрій може використовуватися для збору даних з приймального вузла або передачі даних на приймальний вузол. Він також може використовуватися для взаємодії з керівником. Комп’ютер зазвичай працює як кінцевий пристрій, але планшет або смартфон можуть бути кінцевим пристроєм також.) Тоді кервник (кінцевий користувач) може зробити аналіз.

Бездротові сенсорні мережі використовуються в різних сферах застосування, включаючи промислові, військові та цивільні. Деякі з них перелічені нижче:

а) Військові додатки [8]: Датчики широко використовуються в таких додатках, як спостереження, зв'язок з недоступних районів до базових станцій. Оскільки вони недорогі і використовуються у великій кількості, втрата деяких із цих датчиків не вплине на мету, з якою вони були створенні.

б) Розподілене спостереження [9]: Високомобільні сенсорні мережі, такі як підводний автономний апарат «Зевс», керований компанією Odyssey Marine

Exploration Inc., дозволяють передавати величезні обсяги даних при низькій потужності.

в) Моніторинг споруди [10]: Системи моніторингу споруди виявляють, локалізують та оцінюють ступінь пошкодження. За допомогою такого моніторингу споруди цивільного будівництва можна перевірити на надійність.

г) Моніторинг рівня забруднення та токсичного рівня [11]: Тут датчики збирають дані з промислових районів та районів, де відбувається розлив токсичних речовин. Це корисно для виявлення ядерних, біологічних та хімічних явищ у навколишньому середовищі та передачі їх на віддалені станції для аналізу.

д) Датчики для зору [12]: Ця програма включає спільну самоорганізуючу мережу датчиків, яка має багато мікросенсорів, побудованих на мікросхемах та імплантованих в око. Це покращує зір людей з відсутністю або обмеженим зором.

е) Розумні сенсорні мережі [13]: Ці мережі мають ряд незалежних датчиків. Кожен з датчиків має локальне рішення, і ці рішення потім об'єднують і зважують на основі певного алгоритму, з якого виноситься глобальне рішення.

є) Моніторинг опадів та паводків [14]: Ці мережі мають датчики рівня води, вітру та температури, і дані передаються в центральну базу даних для аналізу та прогнозування погоди.

ж) Інші програми: Деякі програми включають моніторинг довкілля для визначення біоскладності, а інші включають розвідку ресурсів, таких як видобуток та аналіз корисних копалин [15]. Програми охорони здоров’я [16] передбачають відстеження пацієнтів та моніторинг прийому ліків у лікарнях. Великі комерційні можливості існують у побутовій електроніці та в реалізації розумних будинків [17–18] та офісних середовищ.

Бездротові сенсорні мережі стали частиною життя людей, хоча нечисленні представники широкої громадськості знають про їх існування.

Основним застосуванням бездротових сенсорних мереж, яке буде змодельовано в цій дипломній роботі, є цільове програмне забезпечення, метою якого є збір та передача даних, надісланих з цільового вузла. Однією з цільових категорій є окремі об'єкти, які, як правило, мають дуже малий розмір порівняно з великою площею, на якій розгорнута сенсорна мережа, цілі можуть випромінювати шум, світло або сейсмічні хвилі тощо. Інша категорія - це суцільні об'єкти, які можуть поширюватися у дуже великій області, в якій розгорнута сенсорна мережа. Проте цільові програми мають деякі загальні характеристики. Дані, зібрані датчиками, можуть бути надлишковими або непослідовними, і датчикам, можливо, доведеться обмінюватись інформацією при обробці даних.

1.2. Інструменти моделювання бездротової сенсорної мережі

Бездротові сенсорні мережі складаються з багатьох вузлів (датчиків). Багато досліджень у цій галузі базуються на надто спрощеному аналізі, і тому лише обмежена впевненість може бути надана прогнозам, що випливають з таких експериментів, це все виявляється через обмежену кількість датчиків, які можна розподілити в реальній експериментальній мережі. Таким чином, моделювання стало звичним способом тестування нових додатків та нових протоколів перед реальним розгортанням [19]. Результати моделювання покладаються не лише на навколишнє середовище, а й на припущення фізичного рівня, які не є настільки точними. Хоча ця проблема існує, моделювання все ще є хорошим підходом для розгортання датчиків.

В дипломній роботі здійснимо моделювання для різних протоколів маршрутизації, отже буде можливість отримання надійних результатів (наприклад, час життя мережі, кількість пакетів, що передаються через датчики, тощо) - одна з особливостей, яку повинен мати інструмент моделювання.

Немає необхідності в інструменті моделювання для автоматичного створення корисних діаграм топології. Деякі моделі оцінки побудовані на основі

результатів роботи мережі, тому модель енергоспоживання необхідна в інструменті моделювання. Широко використовуються типові та базові протоколи маршрутизації. На основі результатів моделювання цих протоколів маршрутизації можна побудувати кілька корисних моделей оцінки, і ці протоколи маршрутизації повинні бути впроваджені в цій роботі. Тож інструмент моделювання з відкритим кодом є дуже важливим. Саме на цьому етапі немає необхідності підтримувати певні протоколи маршрутизації. Інструмент моделювання повинен бути імітатором дискретних подій і тому може працювати стільки часу, скільки потрібно для завершення моделювання. Масштабованість є важливим фактором для вибору користувачами інструменту моделювання. У цій дипломній роботі буде застосовано 300 вузлів моделювання. На основі результатів моделювання можна побудувати математичну модель, тому інструмент моделювання повинен підтримувати щонайменше 300 модельованих вузлів. Датчики в експериментах цієї магістерської роботи є статичними і розміщені випадковим чином. Хоча це не сувора вимога, для інструмента моделювання було б перевагою підтримувати автоматичне випадкове розміщення.

Подальша робота магістерської роботи спрямована на інтеграцію моделі споживання енергії в датчика SunSpot, тому слід вибрати засіб моделювання на основі Java. Далі наведено загальну модель інструменту моделювання. Модель включає кілька сенсорних вузлів, радіоканалів, середовищ, факторів та приймальних вузлів.

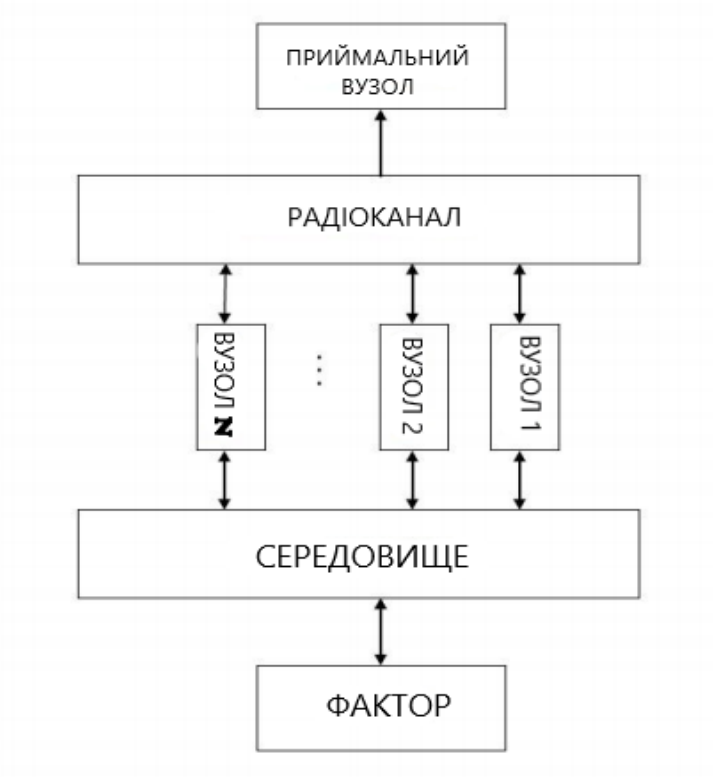


Рисунок 1.2 – Принцип моделювання [20]

Детальний опис компонентів на цьому рисунку такий:

а) Вузли: Вузли є базовими пристроями в цій моделі. Кожен вузол може зв’язуватись між собою через радіоканал. Існує також стек протоколів для управління цими комунікаціями.

б) Навколишнє середовище: Компонент навколишнього середовища моделює генерації та розповсюдження подій, які сприймаються вузлами датчика, і можуть призвести до інших дій датчика.

в) Радіоканал: Цей компонент характеризує поширення радіосигналів між вузлами в мережі.

г) Приймальні вузли: Приймальні вузли отримуватимуть дані із загальних сенсорних датчиків.

д) Фактори: Фактори відіграють роль генератора подій, що представляє запит для вузлів

На основі цієї імітаційної моделі далі проаналізовано кілька прикладів популярних інструментів моделювання:

1. **NS-2**

Network simulator version 2 [21–22] (NS-2) - це дискретний симулятор подій, орієнтований на дослідження мереж, який розроблений на C ++. C ++ є однією з найпопулярніших мов програмування загального призначення і реалізується на широкому спектрі апаратних засобів та платформ операційної системи.

NS-2 може реалізовувати такі протоколи, як Directed Diffusion або sensor medium access control (сенсорний контроль доступу до середовища) (S-MAC). S-MAC - це протокол MAC, спеціально розроблений для бездротових сенсорних мереж, який використовує менше енергії, ніж стандартний протокол. Крім того, існують такі проекти, як SensorSim, які планують забезпечити бездротову підтримку датчиків для NS-2.

Одним з недоліків NS-2 є те, що він заснований на плоскоземній моделі, в якій припускається, що навколишнє середовище є рівним, без опуклостей. Крім того, графічна підтримка NS-2 не дуже хороша, а масштабованість NS-2 обмежена. Це слугує тому, що в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

2. **OMNET++**

OMNET ++ [23–27] - це розширюваний модульний дискретний симулятор подій, написаний мовою C ++. Фреймворк OMNET ++ забезпечує дуже потужну функціональність, оскільки підтримує мережі масового обслуговування, оцінку продуктивності та комунікаційні мережі. Він також забезпечує підтримку моделювання в режимі реального часу, емуляції мережі, інтеграції баз даних та багатьох інших функцій. Порівняно з NS-2, OMNET ++ забезпечує кращу бібліотеку графічного інтерфейсу для підтримки трасування та налагодження.

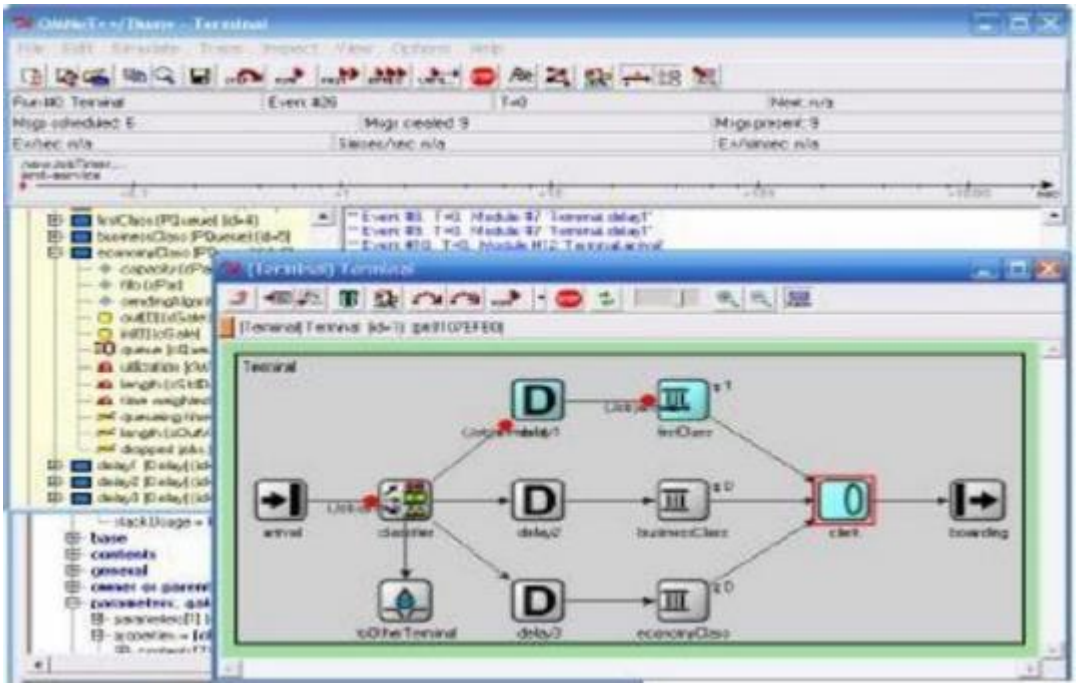


Рисунок 1.3 − Інтерфейс OMNET ++ [28]

Недоліком цього інструмента моделювання є те, що він не надає багато протоколів у своїй бібліотеці. Однак OMNET ++ став популярним інструментом моделювання бездротових сенсорних мереж. Незважаючи на це, в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

3. TOSSIM

TOSSIM [29–30] - це дискретний симулятор подій для сенсорних мереж TinyOS. Користувачі можуть компілювати код TinyOS (nesC) у фреймворк TOSSIM, який працює на ПК. Таким чином, користувачі можуть налагоджувати та тестувати різні алгоритми в повторюваному та контрольованому середовищі.

TinyViz - це користувальницький інтерфейс TOSSIM, який надає користувачам зручне та високоефективне робоче середовище. Це означає, що користувачеві немає необхідності використовувати всі команди. Наступний малюнок ілюструє інтерфейс TinyViz. У зв’язку з цим, в даній дипломній роботі магістра ми не будемо розглядати даний інструмент для моделювання.

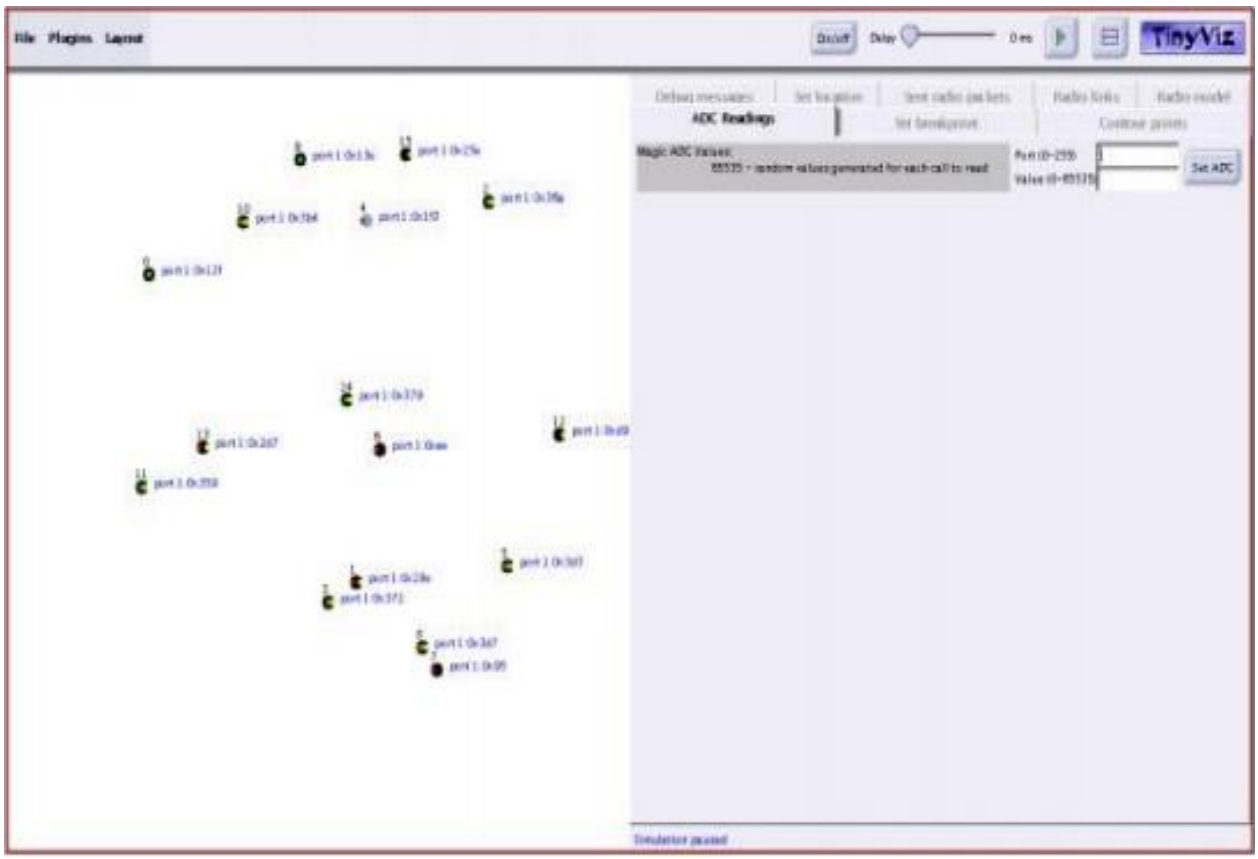


Рисунок 1.4 − Інтерфейс TinyViz [31]

TOSSIM призначений для імітації мереж TinyOS замість реального світу. Іншими словами, TOSSIM просто зосередиться на результаті TinyOS. Структура TOSSIM може імітувати величезну кількість датчиків; крім того, TOSSIM має гарну радіомодель. Таким чином, за допомогою TOSSIM можна отримати багато результатів моделювання. З іншого боку, TOSSIM не може забезпечити користувачів хорошим моделюванням енергоспоживання, що є головним недоліком цього симулятора. Тому в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

4. ATEMU

ATEMU [32] - це засіб моделювання бездротових сенсорних мереж на основі C, яке працює під управлінням операційної системи Linux. Процесор ATEMU називається AVR, який використовується в датчиках MICA2. Графічний інтерфейс для ATEMU отримав назву XATDB, що забезпечує хороший інтерфейс, щоб користувачі могли знати дії вузлів датчиків. На рисунку 1.5

показаний приклад моделювання шести сенсорних вузлів. ATEMU призначений для подолання розриву між реальними датчиками та моделюванням, оскільки він може бути реалізований не лише для реальних датчиків, але також надає користувачам імітацію взаємодії між вузлами датчиків. Виходячи з цього, в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

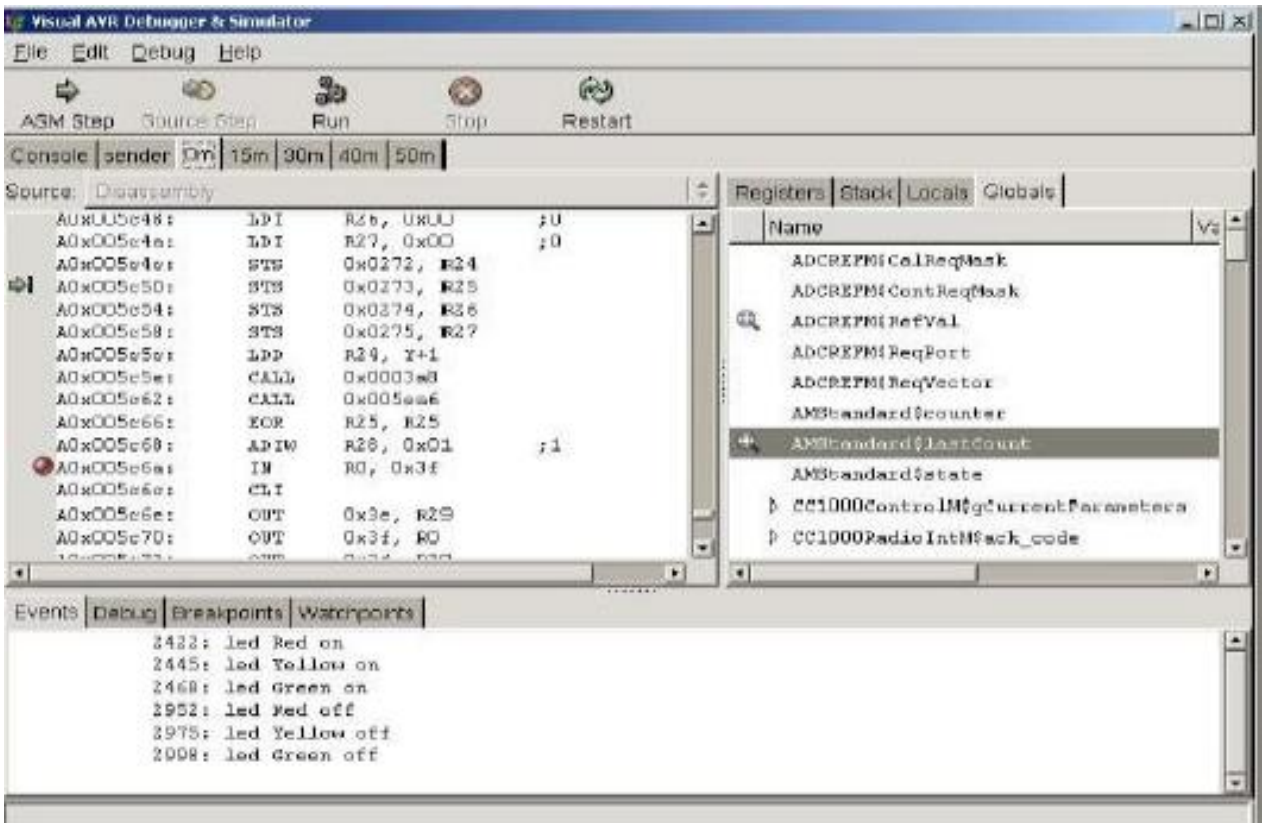


Рисунок 1.5 − Інтерфейс XATDB [32]

Головна перевага ATEMU полягає в тому, що він підтримує неоднорідну сенсорну мережу. Тобто можна моделювати не тільки на вузлах MICA2, але й на інших платформах. На основі моделювання ATEMU можна отримати багато корисних і точних результатів, які допомагають користувачам знаходити неупереджені порівняння. Основним недоліком ATEMU є те, що він підтримує лише обмежену кількість протоколів маршрутизації, тому, наприклад, він не надає жодних маршрутів щодо проблеми кластеризації. Тому в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

5. EmStar

EmStar [33] - це засіб моделювання бездротових сенсорних мереж на основі C, яке працює під управлінням операційної системи Linux. EmStar надає користувачам графічний інтерфейс (рис. 1.6), за допомогою якого користувачі безпосередньо керують пристроями.

Головною перевагою EmStar є те, що операція налагодження для EmStar дуже зручна, і користувачі можуть вільно перемикати моделювання та розгортання датчиків. Основним недоліком EmStar є те, що він може працювати лише в режимі реального часу. Однак симулятор дискретних подій може працювати стільки часу, скільки потрібно для завершення моделювання. Тому в даній магістерській роботі ми не будемо розглядати даний інструмент для моделювання.

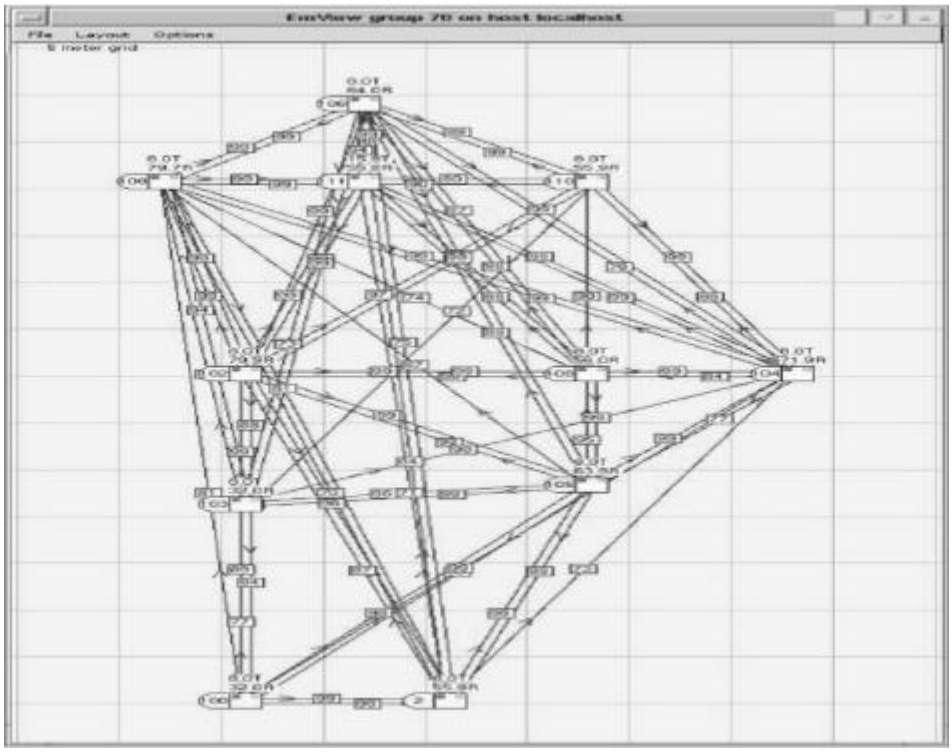


Рисунок 1.6 − Інтерфейс EmStar [34]

6. J-Sim

J-Sim [35] (раніше відомий як JavaSim) - це середовище симуляції композиційної мережі з відкритим вихідним кодом, що базується на

компонентах. Система базується на реалізації IEEE 802.11 [36], забезпеченої J-Sim. IEEE 802.11 - це перший стандарт бездротової локальної мережі (WLAN), запропонований в 1997 році. J-Sim забезпечує інтерфейс сценарію, що дозволяє інтегрувати його з Tcl, і був повністю розроблений на Java. Java - це об'єктно-орієнтована обчислювальна мова загального призначення, яка спеціально розроблена, щоб мати якомога менше залежностей від реалізації.

Головною перевагою J-Sim є те, що він надає деякі основні протоколи маршрутизації, такі як Greedy Perimeter Stateless Routing [37] та Directed Diffusion [38], а також надає користувачеві бездротову систему моделювання мережі з дуже детальною моделлю WSN.

У структурі J-Sim п'ятишаровий стек датчиків і модель живлення є основними компонентами ключового компонента, вузла датчика.

1.3. Деталі J-Sim

J-Sim був обраний в якості інструменту моделювання з наступних причин:

- Автори J-Sim провели детальне порівняння продуктивності [39], моделюючи кілька типових сценаріїв WSN у J-Sim та NS-2. Результати моделювання показують, що J-Sim та NS-2 мають порівнянний час виконання, але пам'ять, виділена для проведення моделювання в J-Sim, щонайменше на два порядки нижче, ніж у NS-2. В результаті, хоча в NS-2 часто не вистачає пам'яті, і не стає неможливим виконання широкомасштабного моделювання WSN, в той час як запропонована структура WSN у J-Sim демонструє хорошу масштабованість.
- Моделі J-Sim легко повторно використовувати, тому користувачі можуть вільно комбінувати компоненти у фреймворках. J-Sim також надає графічний інтерфейс, що полегшує управління моделюванням.

J-Sim - це платформа, заснована на Java. Датчики на основі Java в майбутньому можуть бути інтегровані з інструментами моделювання на основі Java.

Існує ряд моделей енергоспоживання, що використовуються для моделювання, ця робота детально описує модель, яку використовує J-Sim [35], а потім розглядає деякі інші моделі.

У J-Sim енергія, яка витрачається на один стрибок при передачі пакету даних від одного датчика до іншого, вважається пропорційною другій потужності відстані бездротової передачі. Таким чином, очікуване споживання енергії одним датчиком при передачі на приймальний вузол задається даною формулою:

$$O(E(h)E(d^2)), \quad (1)$$

де $E(h)$ - очікувана кількість стрибків від датчика до пункту призначення і $E(d^2)$ - очікуване значення квадрата відстані між датчиками. Це, звичайно, означає, що короткі скачки споживають менше енергії, ніж довгі.

Альтернативним, але непрямим показником, називається модель часової відстані [40]. У цій моделі потужність, яку отримує вузол на відстані від відправника, може бути виражена як:

$$P_0 \times (d_0/d)^a, \quad (2)$$

де P_0 - потужність сигналу, що приймається на відстані d_0 від відправника, а a - так званий показник втрати шляху. Значення a залежить від конкретного середовища поширення, і експерименти показали, що зазвичай $2 \leq a \leq 5$. У цій моделі вузли з'єднуються з мінімальною потужністю, необхідною для досягнення пункту призначення, з вимогою, щоб сигнал на приймачі перевищував деякий встановлений рівень чутливості. Тоді споживаною потужністю вважається лінійна функція отриманої потужності, задана формулою вище.

1.4. Параметри оцінки

Багато дослідників проводили моделювання для цільових застосувань у WSN, враховуючи їх значну роль у ефективності військових та цивільних застосувань, таких як моніторинг навколишнього середовища та спостереження за цілями [41–45]. Ці дослідники проаналізували взаємозв'язок між деякими параметрами оцінки, але більшість результатів у їх опублікованій роботі полягають у мінімізації споживання енергії або аналізі зв'язку між двома параметрами. Наразі не було запропоновано жодної математичної моделі з трьома і більше параметрами.

Проблема енергоефективності

Усередині WSN датчики відправляють пакети даних на інші датчики або прийомний вузол. Пакет - це відформатована одиниця даних; дані складаються з контрольної інформації та даних користувача. Інформація управління забезпечує дані, необхідні мережі для доставки даних користувача, таких як адреси джерел та контрольні суми, і, як правило, вони знаходяться в заголовках пакетів та файлами з даними про корисне навантаження між ними. Як випливає з назв, дані заголовка та файлів можна знайти відповідно на початку та в кінці пакета. Дані про корисне навантаження є основною метою передачі, за винятком інформації, що надсилається разом з ними.

Принцип прогнозованого динамічного управління енергією включає три основні аспекти:

- *Механізм динамічного пробудження*: Цей механізм динамічного пробудження приймає підхід стану пробудження, а також враховує час простою вузла. Алгоритм фільтрів частинок передбачає цільовий стан. Потім кожен вузол використовує передбачений цільовий стан для оцінки часу простою, щоб він міг як можна довше тримати період простою для економії енергії.
- *Розподілений генетичний алгоритм та модельована нормалізація*: Генетичний алгоритм кодує параметри в кінцеві бітові рядки. Кожен із цих

рядків забезпечує можливе вирішення проблеми, а потім працює з набором рядків. Модельована нормалізація починається із випадкового стану рішення, а потім генерує подальші стани ітеративно з нього.

- *Вузол переадресації*: У бездротових сенсорних мережах вузли датчиків поруч з ціллю можуть отримувати інформацію та передавати її в прийомний вузол в кожний період зондування.

Ванг та співавтори [46] зосереджувались на проблемі енергоефективності в мережах енергозбереження, вони не лише пропонували динамічний механізм управління енергією, заснований на прогнозуванні цілей, але також побудували спільну модель зондування та споживання енергії. Це може передбачити цільове розташування за допомогою підходу Фільтрування часток; на основі цієї інформації про місцезнаходження вузли датчиків можуть оновлювати свій розклад і переходити в режим сну, не втрачаючи жодної події. Тим часом, оскільки вузли-кандидати для зондування відомі заздалегідь, дослідники здійснили оптимізацію процесу зондування, використовуючи гібрид GA і SA, який використовує розподілені обчислювальні можливості WSN, щоб енергоспоживання можна звести до мінімуму без погіршення точності продуктивності. Більше того, була запропонована схема маршрутизації вузлів переадресації для досягнення додаткової економії енергії. Ця література, разом із багатьма іншими, запровадила безліч підходів до збереження енергії, але застосувати всі ці підходи в реальній системі буде непросто. (Існує кілька факторів обмеження, таких як обмеження простору для розгортання датчиків, вплив невизначеного середовища для мережі тощо). Моделювання, проведене вище дослідниками, порівнювало споживання енергії від цих різних підходів. Хоча ці концепти базуються на не зменшення точності продуктивності, у їхніх дослідженнях не проводиться аналіз між споживанням енергії та енергією (Точність зондування визначається еліпсом похибки.).

У роботі [47] дослідники пропонують нову нерівномірну схему кластеризації (DEUC) для побудови бездротової сенсорної мережі. З аналізу результатів

моделювання автори роблять висновок, що DEUC може ефективно збалансувати енергоспоживання кластерних голів і продовжити термін служби мережі.

Радіус та кількість вузлів

У роботі [2] Maity & Gupta розглядали випадково розподілену бездротову сенсорну мережу, що охоплює велику територію. Вони хотіли знайти оцінку кількості вузлів, необхідних з мінімальною критичною відстанню зв'язку, щоб забезпечити мережеве підключення та стабільність. Використання результатів теорії графів певних математичних алгоритмів, заснованих на формулах, вже існували для відносно невеликої кількості датчиків; однак автори запропонували нову формулу, засновану на математичному моделюванні, яка мінімізувала прогнозування критичного радіусу між вузлами для великої кількості вузлів.

Вони вибрали MATLAB як інструмент моделювання та побудували рівняння регресії між радіусом та кількістю вузлів. Теоретична модель давала кращі результати, якщо кількість вузлів менше 250, але їх рівняння регресії забезпечується незначною відповіддю на радіус, щоб зберегти зв’язок для більшої кількості вузлів.

Покриття та термін служби

Оскільки датчики можуть розповсюджуватися довільно, однією з основних проблем бездротової сенсорної мережі є проблема покриття. Загалом, це відображає, наскільки дана зона відстежується за даними. Як зазначалося в [48], концепція покриття є мірою якості обслуговування (QoS) функції зондування і піддається широкому спектру інтерпретацій через велику різноманітність датчиків та застосувань. Метою цієї роботи є зробити кожне місце у фізичному просторі в межах зони зондування принаймні одним вузлом датчика. Завданням авторів для вирішення проблеми охоплення цілей у роботі [49] є подовження терміну служби мережі енергообмежених беззахисних сенсорних мереж. Вузли датчика розгортаються навмання навколо цілі, і якщо ціль потрапляє в діапазон

зондування датчика, то датчик отримає інформацію про місце розташування цілі та надсилає її на центральний обробний вузол.

Для того, щоб продовжити термін служби мережі, автори поділяють вузли датчиків на кілька наборів, в яких всі цілі можуть бути охоплені датчиками в кожному наборі. Для економії енергії та продовження терміну служби датчиків ці набори активуються послідовно, таким чином, що в будь-який момент активним є лише один набір (активний стан містить передачу, прийом та очікування). Вузли в інших наборах перебуватимуть у стані сну з низьким енергоспоживанням. Вузли датчиків можуть регулювати свій стан між активним та режимом сну, що продовжить термін служби мережі порівняно з випадком, коли всі датчики активні. Одночасно кількість активних датчиків в області застосування зменшиться, що призведе до зменшення конфліктів на рівні MAC.

У цій дипломній роботі загалом датчики, проектуючи радіус передачі, зможуть охоплювати мережу географічно, і тому проблема покриття, в даному випадку, може трактуватися як тривалість часу, протягом якого це покриття зберігається. Слід зазначити, що експерименти щодо тривалості роботи мережі в цій дипломній роботі не стосуються безпосередньо цієї проблеми; однак, деякі (обмежені) експерименти розглядатимуть ситуацію, коли радіус передачі датчика недостатній для охоплення всієї мережі та вимірювання надійності отриманої системи.

Енергоефективний протокол

У літературі [50] дослідники пропонують енергоефективний протокол, що включає два алгоритми: RARE-Area (Зменшена площа звітування) для обмеження датчиків відповідно до якості даних та RARE-Node (Зменшення відновлення активного вузла) до зменшення надлишкової інформації, що надсилається на прийомний вузол . Робота протоколів полягає в наступному:

Коли датчик виявляє ціль, ціль може генерувати інформацію, а потім вага розраховується за алгоритмом звітування про зменшену площу. Якщо вага

перевищує або дорівнює верхньому порогу, встановленому на початку відстеження, вузол датчика надсилає повідомлення сигналу на всі пов’язані датчики і чекає отримання принаймні двох сигналів від інших датчиків, які виявили ціль так само. Використовуючи цю інформацію, датчик може обчислити цільове положення.

Потрібно розглянути наступні два випадки:

а) Якщо реалізовано лише алгоритм RARE-Area, після обчислення цільової позиції сприйнята інформація буде передана голові кластера.

б) Якщо обидва RARE-Area і RARE-node алгоритми реалізовані, вони продовжують перевіряти надмірність даних. У цьому випадку їм потрібно перевірити, чи немає додаткового вузла датчика в діапазоні зондування. Якщо ні, інформація буде передана безпосередньо голові кластера, оскільки вона не є надлишковою. В іншому випадку вони повинні підтвердити, чи інформація, яку сприймає поточний датчик, надлишкова чи ні, якщо ні, вони передаватимуть інформацію в головку кластера.

Результати моделювання порівнюють час життя з кожним з алгоритмів. Імітаційні дослідження показали, що при середніх значеннях порогової ваги реалізація протоколу RARE-Area окремо або використання як алгоритмів RARE-Node, так і RARE-Area разом знижує споживання енергії без зменшення, точність відстеження більше 20%.

Для параметрів моделювання дослідники порівняли взаємозв'язок між кількістю мертвих вузлів та термін служби мережі, крім того, вони побудували графік значення точності даних у часі.

У роботі [51] дослідники пропонують централізований протокол маршрутизації, який називається протоколом динамічної кластеризації, керованим базовою станцією (BCDCP), який розподіляє енергію, що розподіляється, рівномірно між усіма вузлами датчиків з метою покращення терміну служби мережі та зменшення середнього споживання енергії.

Дослідники також порівнюють BCDCP з Кластерним протоколом маршрутизації під назвою LEACH. Результати моделювання показують, що BCDCP може зменшити середнє споживання енергії та покращити термін служби мережі.

У літературі [52] представлений енергоефективний протокол маршрутизації, заснований на кластерах із використанням коефіцієнта успішності повідомлень. З аналізу дослідники дійшли висновку, що цей протокол може забезпечити кращу енергетичну ефективність, ніж існуючі підходи.

1.5. Постановка задачі

У цій главі представлені деякі формативні описи бездротових сенсорних мереж, а також надано деякі подробиці про J-Sim. Крім того, ця глава включає огляд роботи над параметрами оцінки WSN. У деяких роботах дослідники виконали певні моделювання та отримали корисні результати із відповідними параметрами оцінки. Однак жоден з них не створив математичної моделі для відповідних параметрів, ані підходи компромісу не були виявлені. Таким чином, інструменти моделювання не будуть необхідні для розгортання датчиків, що призводить до економії грошей і часу.

Крім того, в кількох опублікованих роботах дослідники запропонували кілька нових протоколів для поліпшення терміну служби мережі та економії енергії. У наступному розділі буде проаналізовано різні протоколи маршрутизації.

Розділ 2. Протоколи маршрутизації

В цьому розділі протоколи маршрутизації будуть розділені на плоскі, ієрархічні і на основі визначення місця розташування в залежності від структури мережі. У протоколах маршрутизацій плоских всім датчикам присвоюються однакові ролі. В ієрархічних протоколах маршрутизації різним датчикам рівня енергії будуть призначені різні ролі. У протоколах виїзду на основі місцезнаходження для передачі даних буде використовуватися інформація про місцезнаходження датчиків.

2.1 Плоскі протоколи маршрутизації

Плоскі протоколи маршрутизації в плоских мережах, важко визначити ідентифікатор для кожного датчика, так як всі вузли відіграють одну і ту ж роль і співпрацюють разом, щоб виконати завдання зондування і кількість датчиків, як правило, велике.

Протокол з одним стрибком

Це простий протокол, в якому датчики передають безпосередньо інформацію одним стрибком на приймальний вузол. Таким чином, затримка буде зведена до мінімуму, але зіткнення даних може відбуватися на приймальному вузлі, і датчики, розташовані далеко від приймального вузла, можуть витратити велику кількість енергії на передачу до приймального вузла.

Протоколи датчиків для отримання інформації за допомогою подолання перешкод (SPIN)

SPIN [54] - це сімейство протоколів, яке дозволяє користувачеві запитувати будь-який вузол та негайно отримувати будь-яку необхідну інформацію. Однією з переваг SPIN є те, що топологічні зміни локалізовані, оскільки кожен вузол повинен знати лише своїх односкачкових сусідів.

SPIN забезпечує значну економію енергії за протоколом затоплення (див. Нижче). Однак механізм реклами даних SPIN не може гарантувати доставку

даних. Недоліки SPIN : по-перше, він не є масштабованим; по-друге, вузли навколо приймача можуть швидко розрядити акумулятор, якщо приймач зацікавлений у занадто багатьох подіях. По-третє, для даної локалізованої події дані можуть надсилатися по всій мережі.

Спрямована дифузія (DD)

DD [55] - це протокол, який орієнтований на дані, тобто основною функцією протоколу є управління даними. Дані, що генеруються вузлами датчиків, називаються парами атрибут-значення. Вузол запитує дані, надсилаючи інтереси для іменованих даних. Дані, що відповідають відсотку, потім «відтягуються» до цього вузла. Проміжні вузли можуть кешувати або перетворювати дані та можуть спрямовувати інтереси на основі раніше кешованих даних. Усі вузли датчиків у спрямованій дифузійній мережі базуються на застосуванні, що дозволяє дифузії досягти економії енергії шляхом вибору емпірично хороших шляхів, кешування та обробки даних у мережі. DD використовує флуд для надсилання інформації про запит по мережі - загалом флудінг - це проста техніка маршрутизації, при якій датчик передає свої дані всім прийнятним приймачам.

На ефективність методів агрегування даних, що використовуються в парадигмі спрямованої дифузії, впливає кілька факторів, які включають положення вихідних вузлів у мережі, кількість джерел та топологію комунікаційної мережі.

Недоліки цього протоколу можуть бути описані наступними двома аспектами. По-перше, для реалізації агрегування даних використовується метод синхронізації часу, який важко реалізувати в сенсорній мережі. По-друге, агрегування даних - це накладні витрати, пов’язані із записом інформації. Ці два моменти можуть призвести до збільшення вартості вузла датчика.

Rumor Routing (RR)

RR [56] є різновидом спрямованої дифузії. У деяких випадках від вузлів вимагається лише невелика кількість даних, і тоді заповнення (як використовується в DD), не найкраща техніка для використання. Альтернативною стратегією є заповнення мережі, якщо кількість подій невелика, а кількість запитів велика.

Протокол Rumor Routing для заповнення подій через мережу використовує пакет середовища. Коли вузол виявляє подію, він додає цю подію до своєї таблиці подій і генерує діючу силу. Діюча сила подорожує по мережі з метою розповсюдження інформації про місцеві події до віддалених вузлів. Коли вузол генерує запит на подію, вузли, які знають маршрут, можуть відповісти на запит, перевіривши його таблицю подій. Отже, немає необхідності затоплювати всю мережу, що, в свою чергу, знижує вартість зв'язку. Крім цього, протокол RR має лише один шлях між джерелом і пунктом призначення, який відрізняється від протоколу спрямованої дифузії. Використовуючи цей підхід, протокол Rumor Routing може досягти значної економії енергії у порівнянні із затопленням подій, а також може обробляти збої вузлів.

Недоліком протоколу Rumor Routing є те, що він працює добре лише тоді, коли кількість подій невелика. Для великої кількості подій неможливо підтримувати ці діючі сили та таблиці подій.

Максимальний протокол маршрутизації використання енергії (MEURP)

У літературі [57] дослідники пропонують плоский протокол маршрутизації під назвою MEURP. Порівняно з попередніми протоколами плоских маршрутів, MEURP забезпечує очікувальний підхід для зменшення наводнення. MEURP також використовує схему вибору декількох маршрутів для передачі даних. За результатами моделювання MEURP може покращити термін служби мережі та пропускну здатність пакетів даних.

2.2 Ієрархічні протоколи маршрутизації

В ієрархічній мережі датчики низького рівня енергії можуть бути використані для виконання завдання зондування, тоді як датчики високого рівня енергії можуть бути використані для обробки та передачі даних на базову станцію. Завдяки цьому механізму може бути зменшено споживання енергії для всієї мережі. Буде представлено шість протоколів ієрархічної маршрутизації таким чином:

Порогово-чутливий енергоефективний протокол (TEEN)

Протокол TEEN у якого вузли датчиків постійно відчувають середовище, але передача даних здійснюється рідше. У цьому протоколі користувач може контролювати компроміс між енергоефективністю та точністю даних.

Головною особливістю цього протоколу є те, що якщо дані, які відповідають пороговим значенням, не отримуються датчиками, датчики ніколи не будуть спілкуватися між собою (зберігаючи енергію). У цьому випадку користувач більше не може отримувати дані з мережі. Тут пороги можна розділити на жорсткі та м'які. Жорсткий поріг - це абсолютне значення для сприйманого атрибута. Якщо вузол відчуває це значення, він вмикає свій передавач і передає дані. М'який поріг - це невелика варіація значення сприйманого атрибуту, що змушує вузол увімкнути його передавач [58].

LEACH

LEACH [59–63] - це протокол MAC на основі TDMA (TDMA розшифровується як множний доступ з розподілом часу. TDMA - метод доступу до каналу. Цей метод доступу може розділити сигнал на різні часові слоти, таким чином, користувачі можуть спільно використовувати один і той же частотний канал), який інтегрований з кластеризацією та простим протоколом маршрутизації в бездротових сенсорних мережах. LEACH - це ієрархічний протокол, в якому більшість вузлів передають головкам кластера, а головки кластера агрегують та стискають дані та передають їх на базову станцію.

Кожен вузол використовує стохастичний алгоритм на кожному етапі, щоб визначити, чи стане він головою кластера на певному етапі. LEACH припускає, що кожен вузол має радіостанцію, достатньо потужну, щоб безпосередньо дістатися до базової станції або найближчої головки кластера, але використання цієї радіостанції на повну потужність даремно витратить енергію.

Ця робота потребуватиме повного контролю потужності радіокомпонентів на імітаційній платформі, що, в свою чергу, робить можливим моделювання енергоспоживання. На додаток до цього LEACH надає сенсорні мережі безліч хороших функцій, таких як архітектура кластеризації та локалізована координація.

Кластерний протокол маршрутизації (CBR)

У літературі [64] дослідники запропонували ієрархічний протокол маршрутизації з назвою Кластерний протокол маршрутизації в WSN. У протоколі CBR головка кластера може отримувати дані від свого члена під час часового інтервалу TDMA та інших датчиків, які щойно потрапляють у кластер. З результатів моделювання MATLAB автори дійшли висновку, що протокол CBR зменшив втрату даних на 25% порівняно з протоколом LEACH.

Q-LEACH

У літературі [65] автори запропонували Quadrature-LEACH для однорідної мережі. У Q-LEACH мережа розділена на підсектори. Кластери, сформовані в цих підгалузях, є більш детермінованими. Отже, датчики можна добре призначити певному кластеру. З результатів моделювання MATLAB, ця робота дійшла висновку, що Q-LEACH значно покращив період стабільності, пропускну здатність та термін служби мережі.

Протокол кластеризованої маршрутизації на основі розташування (FLCRP)

Програма FLCRP, запропонована в [66], працює лише в середовищі нерухомих датчиків. Цей протокол залежить від енергії датчика та його

розташування. FLCRP має фазу налаштування та стадію стійкої фази. На основі моделювання цей документ дійшов висновку, що FLCRP дав кращі результати (коефіцієнт доставки пакетів; середня затримка від кінця до кінця), ніж LEACH.

Змішане середовище Протокол кластеризації маршрутизації на основі місцезнаходження

Протокол кластеризованої маршрутизації на основі місцезнаходження у змішаному середовищі (MLCRP), запропонований у [66], є модифікацією FLCRP, оскільки він може використовуватися як у фіксованому, так і в мобільному середовищі. Основна відмінність між MLCRP та FLCRP полягає в тому, що перший не надсилає жодного пакету запиту на приєднання після отримання рекламного пакету від головки кластера на етапі налаштування. З симуляційних експериментів у цій роботі зроблено висновок, що MLCRP дав кращі результати (коефіцієнт доставки пакетів; середня затримка від кінця до кінця), ніж LEACH.

2.3 Протоколи маршрутизації на основі місцезнаходження

У протоколах маршрутизації, що базуються на розташуванні, датчики адресуються за допомогою їх розташування. В цьому вигляді протоколу маршрутизації існує два підходи для отримання інформації про місцезнаходження. По-перше, вузли датчиків можуть отримати інформацію про своє місцезнаходження, якщо кожному датчику призначений приймач GPS. По-друге, інформацію про місцезнаходження можна отримати шляхом обміну такою ж інформацією між сусідами. Чотири приклади протоколів, що базуються на розташуванні, наведені нижче.

GPSR

Географічна маршрутизація - це принцип маршрутизації, який спирається на інформацію про географічне положення. Це вимагає, щоб кожен датчик міг визначати своє власне розташування, а також розташування інших датчиків і

вузол приймача. Використовуючи цю інформацію, пакет може бути направлений на вузол приймача без знання топології мережі. GPSR [37] є настільки типовим протоколом маршрутизації на основі місцезнаходження, це багатопротокольний протокол для бездротових мереж дейтаграм, який використовує географічне розташування вихідних вузлів, інтерактивних вузлів та вузлів призначення для пересилання пакету. Протокол GPSR використовує інформацію про безпосередніх сусідів маршрутизатора для пересилання пакету. Якщо область, до якої GPSR переадресовує, недоступна, цей протокол знайде іншу точку по периметру області для пересилання пакету. Оскільки цей протокол є інтеграцією протокорів Greedy та Perimeter, він стає більш точною та стабільною процедурою маршрутизації.

Найближчі з протоколом пересилання (NFP)

Протокол NFP [67] спирається на стратегію жадібної переадресації, яка намагається наблизити переданий пакет до вузла приймача на кожному кроці або стрибку, використовуючи лише локальну інформацію. Таким чином, кожен датчик передає повідомлення своєму сусідові, що є найбільш підходящим з місцевої точки зору. Діапазон передачі або радіус датчика - це максимальна відстань, при якій датчик може передавати свої дані.Прогрес визначається як відстань між передавальним датчиком і приймальним датчиком, що проектується на лінію, проведену від передавача до вузла приймача. Кажуть, що датчик знаходиться в прямому напрямку передавача, якщо негативний прогрес виробляється, коли датчик обраний приймачем передавача. Використовуючи це поняття переадресації для протоколу NFP, найбільш прийнятним сусідом тоді визначається найближчий сусід до передавача в межах його діапазону передачі, що призведе до просування вперед. Потім радіус передачі цього датчика обмежується до відстані до його найбільш підходящого сусіда, таким чином зберігаючи енергію датчика та уникаючи зіткнення даних. Сусідом може бути сам приймальний вузол; якщо існують два або більше відповідних сусідів, тоді пакет буде надісланий лише одному із випадковим вибором. Однак до мережі не

можна додавати нові датчики. Причину цього можна пояснити наступним чином: В експериментах цієї магістерської роботи датчики випадково розміщуються в області моделювання. Коли розгортання завершено, датчики статичні. Протоколи працюють лише у статичній мережі. Додавання або видалення датчиків змінить стратегію маршрутизації, і це дослідження не було враховано в цій дипломній роботі. Як і будь-яка жадібна стратегія, протокол NFP загалом не забезпечує оптимальну мережеву маршрутизацію, а натомість таку, яка може наблизити таку маршрутизацію за розумний час.

Протокол ближнього зв'язку (Nearest Closer - NC)

Протокол NC також покладається на стратегію жадібної переадресації, яка намагається наблизити переданий пакет до вузла приймача на кожному кроці або стрибку, використовуючи лише локальну інформацію. Різниця між NC та NFP полягає в тому, що в NC відстань між вузлом датчика приймача та вузлом приймача менша, ніж відстань між датчиком передавача та вузлом приймача, замість прогресу вперед, як у NFP. Таким чином, просто кажучи в NC, датчик передавача передаватиме своєму найближчому сусіду, який знаходиться ближче до вузла приймача. Різниця між NFP та NC проілюстрована на рисунку 2.1.

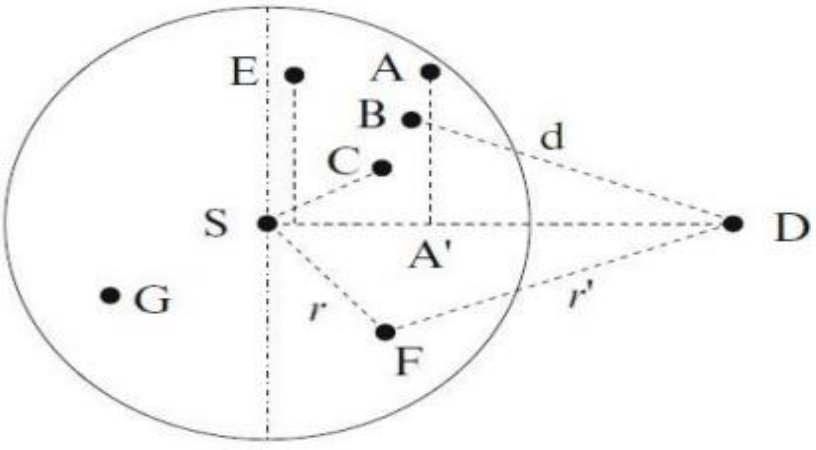


Рисунок 2.1 − Стратегії маршрутизації [68]

На рисунку 2.1 точки A, B, C, E та F знаходяться у прямому напрямку від S. (Ця теза більше не буде стосуватися A, B та F). Решта вузол G знаходиться у

зворотному напрямку від S Тут S означає відправник, а D - пункт призначення. Хоу та Лі [67] запропонували найближчий з прямим прогресом, де кожен вузол відправляє пакет до найближчого сусіда з прямим прогресом (наприклад, вузол E на рисунку 2.1). Стойменович та Лін [69] визначили найближчий ближчий, що є модифікацією NFP, враховуючи відстань, а не прогрес, тобто пакети пересилаються до найближчого сусіда серед усіх сусідів, що знаходяться ближче до пункту призначення (наприклад, вузол C на рисунку 2.1).

Локалізований енергоефективний багатоадресний алгоритм (DLEMA)

DLEMA зосереджується на пошуку найкоротших шляхів енергії, що ведуть через датчики до пунктів призначення. Симуляційні експерименти демонструють, що DLEMA забезпечує низькі затримки та високий рівень успіху. Таким чином, дослідники роблять висновок, що DLEMA можна розглядати як рішення для географічного розповсюдження мультимедійних потоків у складних сенсорних мережах.

Для протоколів, заснованих на розташуванні, багато дослідників вибирають затримку як ключовий параметр для оцінки протоколу. Термін затримка відноситься до часу, який потрібно пакету для передачі через мережу від вузла-джерела до вузла призначення, що включає всі можливі затримки, викликані під час виявлення маршруту, затримки повторної передачі на рівні MAC, поширення. Протокол із великою затримкою означає, що продуктивність протоколу погана через перевантаження мережі та навпаки.

2.4 Причини вибору протоколів маршрутизації

Існує низка причин для вибору трьох протоколів маршрутизації, детально розглянутих у цій дипломній роботі. Вибір протоколу маршрутизації Single-hop із категорії flat забезпечить базову лінію [70], з якою можна порівняти інші протоколи маршрутизації. Протокол маршрутизації Single-hop є найпростішим з

усіх протоколів маршрутизації, тому побудова математичної моделі результатів моделювання повинна бути порівняно простою. Протокол маршрутизації Single-hop також використовується в бездротових сенсорних мережах, де зв'язок відбувається лише між вузлом датчика і приймальним вузлом (без проміжних датчиків), і він може бути реалізований за допомогою недорогих датчиків. Найбільш відомим і широко використовуваним протоколом ієрархічної маршрутизації є LEACH. Результати всіх ієрархічних протоколів важче математично моделювати, оскільки датчики виконують різні ролі в різний час. У програмі LEACH ці ролі обмежені двома: діяти як звичайний датчик або виконувати роль головки кластера, що робить завдання моделювання здійсненним. Таким чином, вибір LEACH в основному ґрунтується на тому, що він широко використовується. Нарешті, протоколи маршрутизації на основі місцезнаходження, яких існує велика кількість, але їх важко реалізувати у J-Sim Greedy Perimeter Ridering Routeing (GPSR), по суті, дозволяє відстежувати, якщо досягнуто глухий кут, тому в рамках будь-якої програми реалізації GPSR та інших подібних протоколів маршрутизації має бути велика кількість вкладених умовних операторів форми _IF 'і _THEN'. Це означає, що поведінка протоколу може принципово змінитися під час моделювання залежно від географічного та стану потужності мережі, так що тенденції результатів, отримані в результаті моделювання з використанням таких протоколів, буде важко (якщо неможливо) проаналізувати. Щоб уникнути такої обумовленості та очевидної складності будь-якої результуючої математичної моделі, вибір зводиться до найближчих із прямим прогресом (NFP) або найближчих ближчих (NC) для роботи. Маршрути в NFP, по яких датчики передають дані на вузол приймача, будуть дуже нерівними (з великою кількістю «злетів» і «спадів») порівняно з маршрутами в NC за визначенням.

Причину, за якою протоколи маршрутизації поділяють на три категорії, можна знайти в посиланнях[71]. Може бути так, що деякі гібридні протоколи маршрутизації перетинають межі між трьома основними типами протоколів маршрутизації. Ще раз поведінка такого гібрида буде залежати від стану

бездротової сенсорної мережі, так що під час моделювання він може неодноразово виступати як плоский протокол маршрутизації на основі ієрархічної або локації залежно від обставин.

Результати моделювання з протоколу маршрутизації, які допускають багаторазові і принципові зміни поведінки, буде практично неможливо математично змоделювати без ефективного зворотного проектування програми реалізації протоколу.

2.5 Висновки до друго розділу

У цьому розділі було розглянуто три різні категорії протоколів маршрутизації, для кожної категорії було розглянуто та описано ряд прикладів. Описано підмножину протоколів маршрутизації для аналізу, таких протоколів маршрутизації як: Single-hop, LEACH та Nerely Closer, які приймаються як представники плоских, ієрархічних та протоколів маршрутизації, які базуються на розташуванні відповідно.

Перед початком моделювання в наступному розділі буде визначено важливі параметри оцінки, які слід враховувати та використовувати в рамках таких моделювань.

Розділ 3. Моделі оцінки протоколу Single-hop

По-перше, основні параметри оцінки надійності (R) та термін служби (L) будуть визначені для використання у наступних розділах. Зокрема, термін служби використовуватиметься як міра споживання енергії. Ця дипломна робота також буде зосереджена на зміні параметрів радіуса (Ra) та щільності (D), які також визначені нижче. Інший параметр, який тут визначено, - це латентність (L), хоча цей параметр у цій роботі розглядається лише побіжно. На основі результатів експериментів варіювання цих останніх трьох параметрів та вимірювання впливу на термін служби та надійність, з часом будуть побудовані моделі оцінки.

У цій дипломній роботі було прийнято управління потужністю радіодеталей на J-Sim, що робить можливим моделювання енергоспоживання.

У цій тезі передбачається, що всі датчики можуть передавати дані про явища, які вони виявляють, а також можуть отримувати та повторно передавати дані від інших датчиків про будь-яке явище, виявлене в системі.

3.1 Параметри оцінки та експериментальне встановлення

Зараз ми розглянемо параметри оцінки: надійність, термін служби, радіус, щільність та латентність.

1. Надійність

У цій дипломній роботі експерименти проводяться з використанням концепції надійності, що визначається формулою:

$$Надійність = \frac{\text{кількість пакетів даних, що надходять до приймального вузла}}{\text{кількість пакетів даних, що передаються до приймального вузла}}. \quad (3)$$

Як визначено, що переваги використання надійності є подвійні. По-перше, це визначення можна використовувати в польових та лабораторних умовах. За умови, що приймальний вузол (кінцевий користувач) знає, скільки є голів кластера або датчиків і середня кількість пакетів даних, що реєструються, на

датчик за одиницю часу, тоді надійність можна оцінити в будь-який час протягом життя мережа з використанням кількості одиниць часу, що минули. Будь-яка різниця між надійністю, виміряною в польових умовах та лабораторією, може бути використана для виявлення, скільки пакетів даних втрачається між датчиками та головками кластера або приймальним вузлом (Сюди входить підрахунок датчиків, які вийшли з ладу або були втрачені системою) . По-друге, це визначення дозволяє легко аналізувати зв'язок між вузлами датчиків; зокрема, це робить можливим оцінку зіткнення даних у бездротовій сенсорній мережі.

2. Термін служби

Термін служби мережі став ключовою характеристикою для оцінки сенсорних мереж специфічним способом. Термін служби мережі [72] - це проміжок часу від розгортання датчиків до моменту, коли мережа вважається нефункціональною. Не функціональність настане в той момент, коли перший датчик вийде з ладу, настане втрата покриття або певна частина датчиків перестане працювати. Визначення для *терміну служби* мережі, яке розглянуто в експериментах у цій дипломній роботі, це момент, коли останні дані надійшли до приймального вузла. Причиною вибору цього визначення для *терміну служби* є те, що сенсорна мережа не має сенсу, якщо приймальний вузол не може отримати будь-які дані. (В експериментах за протоколами Single-hop та LEACH останній датчик може підтримувати швидкість передачі даних, поки він не зможе передати дані на приймальний вузол. У цьому випадку моделювання слід призупинити, поки приймальний вузол не зможе отримати будь-яку інформацію. У цьому випадку, якщо процес передачі даних буде заблокований, датчики продовжуватимуть працювати довгий час, поки не вийдуть з ладу. Тож вибрати момент, коли останній датчик перестає працювати, для визначення терміну служби мережі - це невдалий вибір.)

3. Радіус

У бездротовій сенсорній мережі всі вузли розгортаються із заздалегідь визначеним радіусом зв'язку [73]. У кожному експерименті даної магістерської

роботи всі загальні датчики матимуть однаковий радіус зв'язку. Це обмежує область, в якій датчики можуть виявляти явища, так що в цій дипломній роботі магістра також буде висвітлено вплив цього обмеження на радіус зв'язку на *термін служби* та *надійність*, змінюючи *радіус*.

4. Щільність

Щільність - параметр для дослідників для оцінки протоколів маршрутизації. Зі збільшенням щільності вузлів датчиків ефективність роботи сенсорної мережі може покращуватися або погіршуватися. Тож у деяких моделюваннях дослідників турбує кількість датчиків, які вони використовують у мережі. Очевидно, що в реальній бездротовій сенсорній мережі деякі вузли не працюють. Таким чином, увага, природно, звернеться на кількість датчиків, які все ще працюють. Кількість датчиків, розміщених у фіксованій зоні, буде прийнято як параметр щільності [74] в цій дипломній роботі. Очевидно, що зі збільшенням кількості датчиків зростає і середня кількість датчиків на квадратний метр, тобто щільність датчиків.

5. Латентність

Латентність в даній роботі вказує на (середню) кількість стрибків від датчика до приймального вузла або головки кластера. Загалом латентність відноситься до часу, необхідного для передачі даних на приймальний вузол, кожен необхідний стрибок включає пакет даних, який потрібно прийняти, обробити та переслати по шляху передачі.

Експериментальне встановлення

На рисунку 3.1 модельована площа для наступних експериментів визначена як квадрат 10 метрів × 10 метрів із випадково розгорнутими датчиками. Вузол приймача для цієї програми розташований посередині цієї області. Однією з основних причин вибору цього набору є можливість узагальнення результатів на великих ділянках шляхом конкатенації мереж, подібних до цієї. Наприклад, область 50 метрів × 50 метрів можна налаштувати,

використовуючи 25 екземплярів набору, що використовується тут, у формації сітки 10 × 10. (Для розширення 50 метрів × 50 метрів потрібно 25 приймальних вузлів. Кожен приймальний вузол розташований в центрі окремого квадрата 10м х 10м. У цьому випадку є 25 маленьких квадратів. Вузли датчиків все ще розміщені випадковим чином. Радіус передачі такий же, як і раніше. Ця теорія була введена в літературі [53], але теорія ігнорувала ефект зіткнень даних між малими квадратами. Це є потенційною слабкістю цього підходу.) У кожному експерименті моделювання існує цільовий вузол, і цей цільовий вузол генерується стимул кожну секунду. Всі датчики активні на початку моделювання, і часу моделювання достатньо для отримання даних у кожному окремому експерименті. Усі пункти (на рисунках) у цій дипломній роботі є середнім значенням з 5 окремих експериментів. У кожному експерименті один раз датчики стають статичними, а вузли датчиків переставляються випадковим чином для 5 експериментів. Час роботи мережі буде вимірюватися в секундах. Максимальний час моделювання для всіх експериментів у цій магістерській роботі становить 100 000 секунд.

Ця модель застосовується у багатьох випадках, включаючи теплове випромінювання, світло, звук, магнітні та гравітаційні поля. Згідно з цим налаштуванням, всі вузли залишаються активними, і не відбувається сплячого режиму будь-яких вузлів.

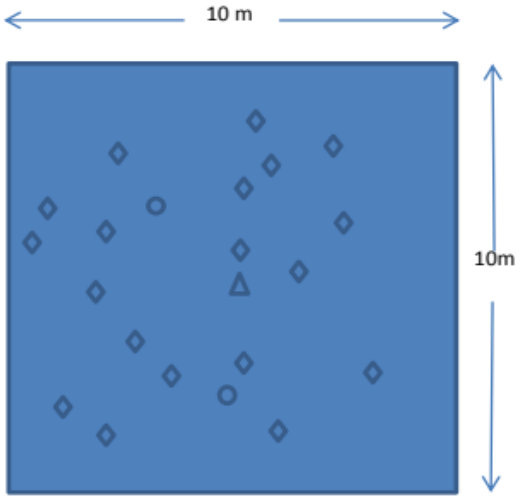


Рисунок 3.1 − Область моделювання

На рисунку 3.1 круги означають головки скупчення (для LEACH), ромби - нормальні датчики, а трикутник –приймальний вузол.

У цій магістерській роботі обрано відповідний протокол MAC для кожного протоколу маршрутизації. Для протоколу Single-hop в якості протоколу рівня MAC було обрано Carrier Sense Multiple Access (CSMA), оскільки він може забезпечити механізм управління зв'язком між датчиками, що дозволить уникнути зіткнень даних. Для протоколу LEACH в якості протоколів MAC були обрані Time-Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), оскільки TDMA має природну перевагу доступу до середовищ без зіткнень, а CDMA може дозволяти датчикам з різних кластерів передавати їхні дані одночасно без зіткнення даних. Для протоколу Nearest Closer було обрано протокол ALOHA MAC з прорізами, оскільки він може змусити один активний датчик майже безперервно передавати з повною швидкістю каналу, таким чином, можна отримати кращі результати для NC.

3.2. Single-hop протокол

Велика кількість вузлів датчиків споживає багато енергії, отже, сенсорна мережа потребує протоколи мережевої маршрутизації, що забезпечують функції управління та управління мережею. У цьому підрозділі буде проаналізовано найпростіший з так званих плоских протоколів, а саме протокол Single-hop. Та буде встановлено взаємозв'язок між радіусом, терміном служби та надійністю для цього протоколу шляхом моделювання. Причиною вивчення цього добре відомого протоколу є надання базової лінії, щоб потім можна було провести порівняння між цим протоколом та складнішими.

Протокол маршрутизації Single-hop, також відомий як прямий метод або метод одного переходу, має всі вузли датчиків, що безпосередньо обмінюються даними з базовою станцією. Зазвичай ця модель недоступна для більшості додатків через суворі обмеження та неефективність. Основна його помилка полягає в тому, що датчики традиційно оснащені радіостанціями відносно

низької потужності, що обмежують відстань, на яку вони можуть передавати сигнал. Отже, будь-які датчики, які розташовані на більшій приймальним вузлом (тобто немає прямої видимості), матимуть вищий SNR або, можливо, не зможуть дістатися до базової станції.

Протокол Single-hop також включає рівень MAC. Рівень MAC базується на MAC-CSMA, спеціальному протоколі MAC, що базується виключно на Carrier Sense Multiple Access (CSMA).

У цьому непостійному протоколі CSMA перед відправкою даних станція виявляє канал, і якщо канал не працює, вона починає передавати дані. З іншого боку, якщо канал зайнятий, станція не розпізнає це постійно, а натомість чекає випадкову кількість часу і повторює алгоритм.

3.3. Будова системи та експериментальна установка

Коли різні датчики хочуть обмінюватися даними, вони не можуть це робити одночасно через перешкоди на каналі, тому потрібен рівень MAC для опосередкування використання каналу та повторної передачі невдалих пакетів.

J-Sim - це засіб моделювання на основі Java, який також забезпечує 802.11 для всіх користувачів. Рівень MAC, як правило, використовує механізм RTS / CTS [75] для управління зв'язком між датчиками, але ці контрольні повідомлення можуть бути втраченими через зіткнення даних.

Експериментальна установка в J-sim була згадана під час опису протоколу маршрутизації - Single-hop. Оскільки датчики випадково розміщуються в зоні імітації, положення вузлів буде змінюватися при різному моделюванні, що матиме вплив на результати, якщо кількість датчиків буде обмежена.

3.4. Надійність та термін служби моделей

В даному підрозділі ми розглянемо 2 види моделей. Це модель із

фіксованим радіусом та модель із змінним радіусом.

1. Модель із фіксованим радіусом

Взаємозв'язок між кількістю датчиків і надійністю для фіксованого 15-метрового радіуса передачі проілюстровано у формулі:

$$100.014 – 0.0126857142857145n, \quad (4)$$

де n являє собою кількість датчиків. Значення 100 слід вживати, коли n = 1, тоді як рівняння 100,001343 вказує на те, що ця лінійна модель добре підходить для реальності. З іншого боку, надійність дорівнює 0 за цією моделлю, коли n = 7884, хоча екстраполювати поки що важко згідно з отриманими експериментальними даними.

Дуже просту модель тривалості життя можна створити, припустивши, що датчик починається із загальним часом автономної роботи K і датчик споживає в середньому за секунду (передаючи з фіксованим радіусом). Тоді мережа матиме фіксовану тривалість життя K/e незалежно від кількості датчиків. Для експериментів, проведених з радіусом 15 метрів, середнє значення K/e становило 15600.

Для обґрунтування цієї моделі в J-Sim енергія, яку споживає датчик, пропорційна квадрату його відстані d до центру. Фактом є те, що випадковий розподіл n-кількості датчиків на квадраті та усереднення відстані (або його квадрата) до його центру є однаковим із випадковим розподілом лише одного датчика та усереднення його відстані (або його квадрата) за n-кількість повторень експерименту. Звідси випливає, що $E(d^2)$, усереднене по всіх датчиках мережі, виміряне за великою кількістю експериментів, не залежить від кількості датчиків і приблизно дорівнює 16,6 метра. Таким чином, термін служби мережі повинен моделюватися за формулою:

$$K/16/6\alpha, \quad (5)$$

де α – це константа. Тому $e = 16.6\alpha$ чи дорівнює $K = 258960\alpha$.

2. Модель із змінним радіусом

Оскільки радіус передачі змінюється, очікувана кількість датчиків в межах діапазону буде задаватися формулою:

$$20\pi r^2/100, \tag{6}$$

при чому $0 \leq r \leq 5$.

Ця формула надає відповіді 0,62831853, 2,513274123, 5,654866776, 10,05309649 та 15,70796327 для r = 1, 2, 3, 4 та 5 метрів відповідно, і очевидно, що відповідь 20 при $r \geq 5\sqrt{2}$ метрів. При $5 < r < 5\sqrt{2}$ деяка елементарна геометрія показує нам, що площа всередині квадрата, але поза колом, центром якого є приймальний вузол, визначається за формулою:

$$A = 2(5 - \sqrt{r^2 - 25})^2 + (50 - r^2) - 4(\frac{\pi}{4} - 0)r^2, \tag{7}$$

де $\theta = \tan^{-1}(\sqrt{r^2 - 25/5})$. Таким чином, очікувана кількість датчиків у цьому випадку становить 20 – A/5, що означає 19,016 при r = 6 метрів.

Датчики в мережі Single-hop, які розглядаються, залишалися активними весь час. Датчик, що знаходиться в радіусі дії приймального вузла, може регулювати діапазон його передачі на відстань до центру і таким чином економити потужність. З іншого боку, кожен датчик поза діапазоном передає повний радіус передачі. Вузли, що перебувають поза межами дії, все ще передаються, має узгоджуватися з пізнішими експериментами, так що єдиною поведінковою зміною від експерименту до експерименту є протокол маршрутизації. Передача датчиків поза діапазоном не контролюється протоколом CSMA, і, зокрема, може спричинити зіткнення даних з даними, що передаються датчиками в межах дальності, що негативно впливає на надійність. Вивчення вихідних даних експериментів виявляє, що існує, як можна було б очікувати, лінійна залежність між кількістю датчиків в діапазоні передачі, *s*, (при $r \leq 5$) і кількістю пакетів даних, отриманих приймальним вузлом. Більш дивно,

що існує також лінійна залежність між *s* (при r ≤ 5) і кількістю пакетів даних, відправлених на приймальний вузол.

Отримані дані усереднювали для постійних значень *s* для різних значень *r*, а потім за допомогою методу найменших квадратів загальна кількість переданих пакетів даних була приблизно

$$206230.002000859 - 9193.8288407016s,$$

при 0 ≤ r ≤ 5. Також, використовуючи той самий метод, кількість пакетів даних, отриманихприймальним, становить приблизно

$$436.736796908544 + 1280.42582653499s,$$

при 0 ≤ r ≤ 5. Таким чином, в середньому надійність для 20 датчиків та 0 ≤ r ≤ 5, може бути наближена наступною формулою:

$$\frac{436.736796908544 + 1280.42582653499\frac{\pi r^2}{5}}{206230.002000859 - 9193.8288407016\frac{\pi r^2}{5}}, \quad (8)$$

Ця формула загалом надмірно оцінює показники надійності, отримані в результаті проведених експериментів, але має правильну загальну форму. Графік функції, представленої наведеною вище формулою зображений червоною кривою на рисунку 3.2.

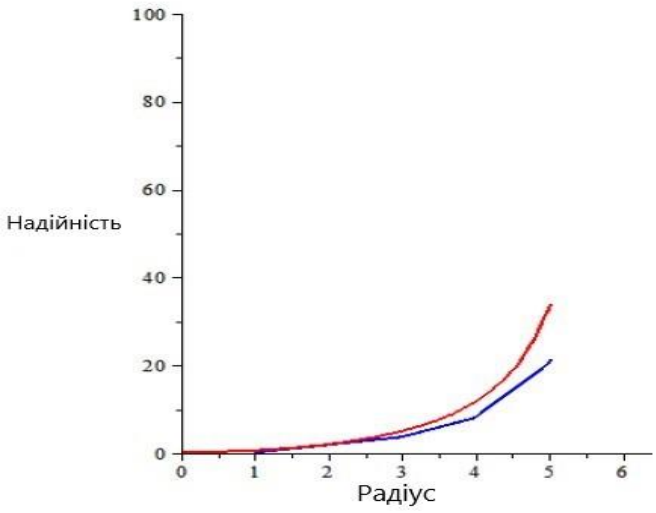


Рисунок 3.2 − Модель надійності зі зміним радіусом передачі

Тепер, якщо кількість датчиків зафіксовано на рівні 20 і $r \geq 5\sqrt{2}$ метрів, то основний показник надійності з лінійного рівняння становить 99,76%. Найкраща формула, яка може бути запропонована для $5 < r < 5\sqrt{2}$, полягає в тому, що надійність задається формулою:

$$\left(1 - \frac{A}{100}\right) \times (0.9976), \tag{9}$$

де A - площа, виявлена вище.

Нарешті, ми розглядаємо термін служби мережі, оскільки радіус змінюється. Експерименти показують, що середній термін служби постійний і становить приблизно 15600 (насправді це 15587) незалежно від радіуса, за умови, що є принаймні один датчик, який може успішно передавати на приймальний вузол. Тепер очікуваний квадрат середньої відстані датчиків у діапазоні передачі збільшиться з радіусом до $5\sqrt{2}$ метрів, але, як розраховано вище, очікувана кількість датчиків у діапазоні збільшується пропорційно квадрату радіуса при $0 \leq r \leq 5$. Таким чином, для меншого радіусу менша кількість датчиків в межах дальності передаватиме більше, ніж у випадку більшого радіуса. Проведені експерименти дозволяють припустити, що швидкість передачі пропорційна квадрату відстані датчика від приймального вузла, так що споживання енергії та швидкість передачі фактично заперечують один одного, приводячи до постійного терміну служби (швидкість передачі - це кількість пакетів даних, що надсилаються в секунду, споживаною енергією є енергія, необхідна для відправки одного пакета даних наприймальний вузол. Отже, швидкість передачі в рази, витрачена енергія на пакет даних, дає енергію, спожиту в секунду; ділення K (значення загальний час автономної роботи) на e формує термін служби).

Імовірність, p, що відсутні датчики в діапазоні передачі, задається значенням:

$$(1 - \frac{E(s)}{20})^{20}, \tag{10}$$

де $E(s)$ - очікувана кількість датчиків у діапазоні передачі, розрахована вище. Отже, очікуваний термін служби задається формулою $15600(1-p)$. Ця формула дає значення (майже точно) 15600 при $r \geq 3$ і задається формулою

$$15600(1-(1-\frac{\pi r^2}{100})^{20}) , \quad (11)$$

при $0 \leq r < 3$. Зокрема, ця формула дає 7361 та 14537 при r = 1 та 2 метри відповідно. Графік функції, представленої наведеною вище формулою зображений червоної кривою на рисунку 3.3.

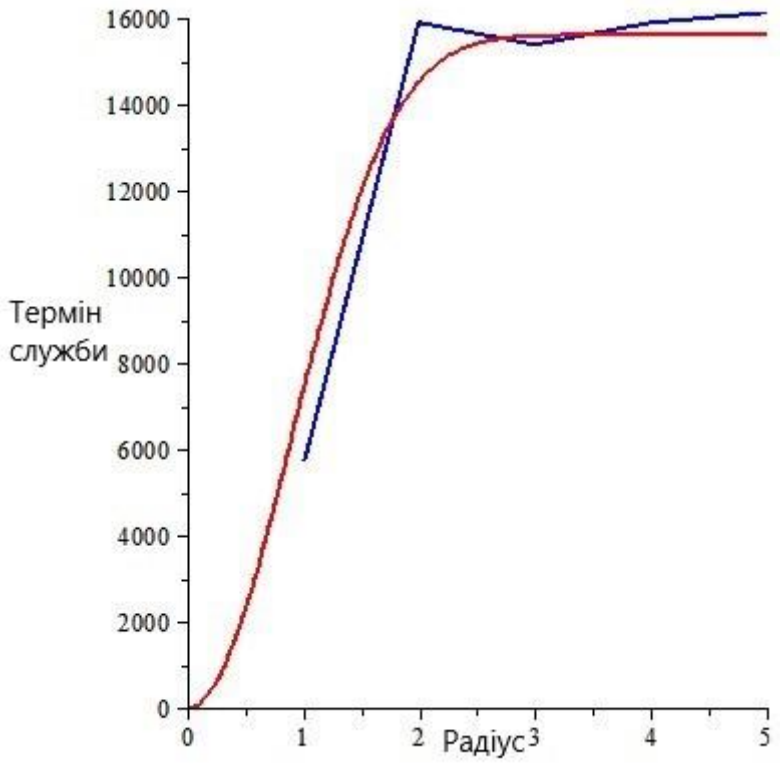


Рисунок 3.3 – Модель терміну служби

В експериментах цього підрозділу датчики поза зоною дії все ще повинні передавати пакети даних на приймальний вузол (цей процес споживає багато енергії). Ці датчики можна розглядати як надлишкові вузли датчиків. Тож немає потреби економити енергію для цих надлишкових вузлів. Може статися зіткнення даних, але ефект надійності слабкий. Якщо зайві датчики припинять передачу, весь час моделювання буде значно збільшено. У майбутньому, якщо датчик знає свою відстань відприймального вузла, і ця відстань перевищує його

діапазон, датчику не потрібно буде передавати дані. У цьому випадку надійність можна збільшити. Це стосується протоколу LEACH та протоколу Nearest Closer.

3.5. Висновки до третього розділу

У цьому розділі отримано кілька корисних результатів серед параметрів щільності, радіуса, надійності та терміну служби.

Зі збільшенням кількості датчиків з 10 до 60 надійність зменшилась. Надійність вище 99% у всіх розглянутих випадках. Термін служби становить від 14900 до 16100 секунд, оскільки кількість датчиків збільшується з 10 до 60.

Надійність зростала із збільшенням радіуса від 1 до 7 метрів. Коли радіус збільшується з 7 до 10 метрів, надійність більше не може зростати. Тривалість служби - це, по суті, горизонтальна лінія, коли радіус дорівнює 2 або більше 2 метрів.

Таким чином, результати демонструють (принаймні в експериментальній установці), що термін служби не залежить від кількості датчиків (припускаючи, що ця кількість не дуже мала або велика). Може бути так, що загальний термін служби переважно вимірюється терміном служби найближчого датчика до приймального вузла (який повинен мати найменші витрати енергії). Збільшення щільності датчиків в середньому зменшить відстань найближчого датчика доприймального вузла, але це зменшення буде дуже незначним у діапазоні від 10 до 60 датчиків, і тому матиме лише дуже мінімальний вплив на термін служби.

Інтуїтивно можна було б очікувати, що зі збільшенням кількості датчиків кількість зіткнень даних зростатиме, а отже, надійність падатиме. Враховуючи, що це дуже простий протокол, зв’язок між кількістю датчиків і надійністю також є прямим, оскільки він є лінійним. Можливо, більш дивним є те, що надійність настільки висока у всіх розглянутих випадках. У випадку будь-якого мережевого протоколу датчик не передаватиме, якщо він знає, що в мережі присутній інший сигнал (він покладається на зворотній зв'язок з приймальним вузлом), і, схоже,

дуже проста реалізація протоколу - надзвичайно ефективна в наших експериментах.

Здається, термін служби вимірюється в протоколі Single-hop, переважно на датчику, найближчому до приймального вузла. У певному сенсі цифра на рисунку 3.3 для одного метра є майже (не кількісно визначеною) частотною мірою того, як часто найближчий датчик знаходиться в межах одного метра відприймального вузла.

Крім того, було запропоновано дві моделі оцінки серед параметрівтерміну служби, надійності та щільності. На основі цих інтелектуальних моделей оцінки користувачі бездротової мережі датчиків можуть безпосередньо передбачити термін служби та надійність. Це означає, що вузли датчиків можуть бути розгорнуті в такій мережі без подальшого моделювання.

Після аналізу найпростішого Single-hop протоколу, в наступна розділі ми звернемо увагу на один із типових протоколів маршрутизації на основі ієрархічної системи, а саме LEACH. Для цього протоколу також будуть запропоновані деякі результати моделювання J-Sim та моделі оцінки.

Розділ 4. Моделі оцінки протоколу Leach

На основі визначень, наведених у розділі 3, для протоколу LEACH було проведено певний аналіз терміну служби, щільності, радіусу та надійності. Побудовано моделі оцінки параметрів тривалості життя, щільності, радіусу та надійності. Ці моделі оцінки означають, що користувачі бездротових сенсорних мереж можуть передбачати тривалість та надійність безпосередньо на основі LEACH протоколу. Таким чином, інструменти моделювання не будуть потрібні для розгортання датчиків, що призводить до економії часу та грошей.

4.1. Будова та оцінка LEACH протоколу

LEACH - це протокол MAC на основі TDMA, який інтегрований з кластеризацією та простим протоколом маршрутизації в бездротових сенсорних мережах.

Протокол LEACH відрізняється від інших кластерних протоколів маршрутизації тим, що:

а) Він використовує рандомізоване обертання кластера головок;

б) Це зменшує обсяг даних, які потрібно передавати на приймальний вузол;

Використання кластерів зменшує кількість проміжних вузлів. Крім того, використовуючи обертові головки кластерів та адаптивні кластери, енергетичні потреби системи в цілому розподіляються між усіма датчиками.

LEACH - це один з ієрархічних протоколів, в якому більшість вузлів датчиків передають сприйняті дані головам кластерів; головки кластеру агрегують і стискають дані, і, в свою чергу, пересилають дані на приймальний вузол. Кожен вузол використовує стохастичний алгоритм на кожному етапі, щоб визначити, чи стане він кластерною головкою на цьому етапі. Цей алгоритм можна пояснити наступним чином:

Рішення вузла n стати головкою кластера чи ні приймається шляхом вибору випадкового числа від 0 до 1. Якщо число менше порогового значення, вузол стає головкою кластера для поточного етапу. Фактично встановлюється рівним, якщо вузол належить до безлічі вузлів датчиків, які не були головками кластера в останніх раундах, а в іншому випадку він встановлюється рівним 0. Тут (з цілим числом) - бажаний відсоток головок кластера та стендів для поточного етапу див. [59] для більш детальної інформації.

Отже, якщо енергію, що залишилася для кожного вузла, можна виміряти, це зробить значний внесок у цю область досліджень.

LEACH є одним із репрезентативних ієрархічних протоколів, і LEACH надає сенсорним мережам безліч хороших функцій, таких як архітектура кластеризації та локалізована координація. Крім того, LEACH - це найпростіший ієрархічний протокол, який буде реалізований у J-Sim, що скоротить час моделювання. Таким чином, ця магістерська робота аналізує деякі критичні параметри на основі протоколу LEACH у J-Sim.

Втрата даних

Є три основних вкладників в скиданні пакетів даних, а саме:

а) Датчик може отримувати дані від цілі, але не може передавати їх на будь-яку головку кластера через відсутність потужності або недостатній радіус.

б) Агреговані дані, надіслані з головок кластера, можуть бути видалені через зіткнення даних з пакетами з інших головок кластера.

(c) Агреговані дані, надіслані з головки кластера, можуть бути втрачені через відсутність потужності або недостатній радіус.

Надійність виключає дані, викинуті першим чином, тому першочерговим завданням у цій дипломній роботі має бути зіткнення даних та відсутність потужності головок кластерів. Зіткнення даних - це одночасна наявність сигналів від двох вузлів у мережі. Зіткнення може статися, коли два вузли думають, що мережа простоює, і обидва починають передавати приблизно одночасно. Коли відбувається зіткнення даних, усі дані з двох (або більше) джерел втрачаються.

Будова системи та експериментальна установка

Розглядаючи окремий кластер ізольовано, використання TDMA гарантує відсутність зіткнення даних всередині кластера. У протоколі LEACH також використовується CDMA з множинним доступом Code Division [76–78], він використовує технологію розширеного спектру та спеціальну схему кодування, що дозволяє датчикам з різних кластерів передавати свої дані одночасно без зіткнення. Однак дані з різних головок кластера можуть зіштовхуватися на шляху до або на приймальних вузлах, що призводить до серйозної втрати даних.

Усі експерименти, проведені в рамках цієї дипломної роботи, засновані на інструменті моделювання J-Sim (згаданому в 1.3). Протокол маршрутизації - LEACH. Модельована площа для наступних експериментів визначається як квадрат 10 метрів на 10 метрів із довільно розгорнутими вузлами. Приймальний вузол для цієї програми розташований у центрі цієї області.

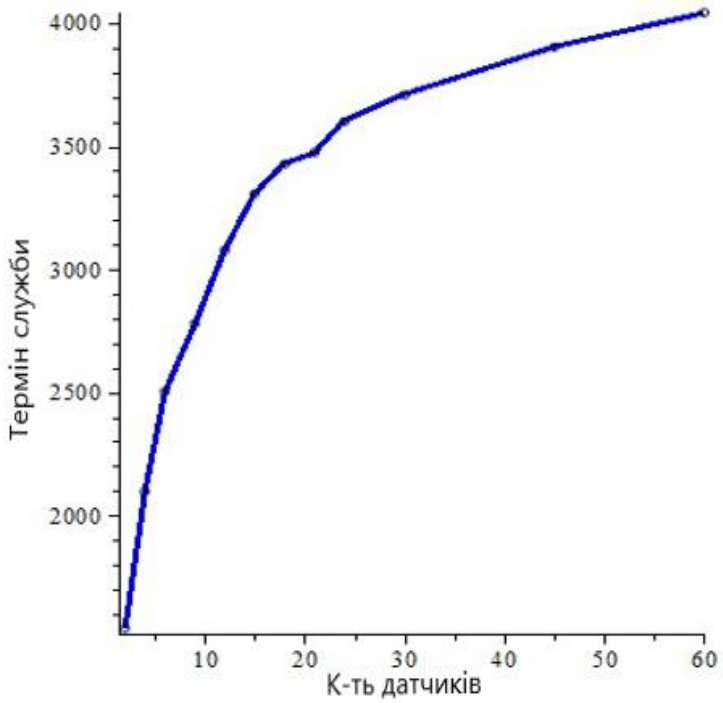
Результати оцінки

1. Щільність —термін служби - надійність

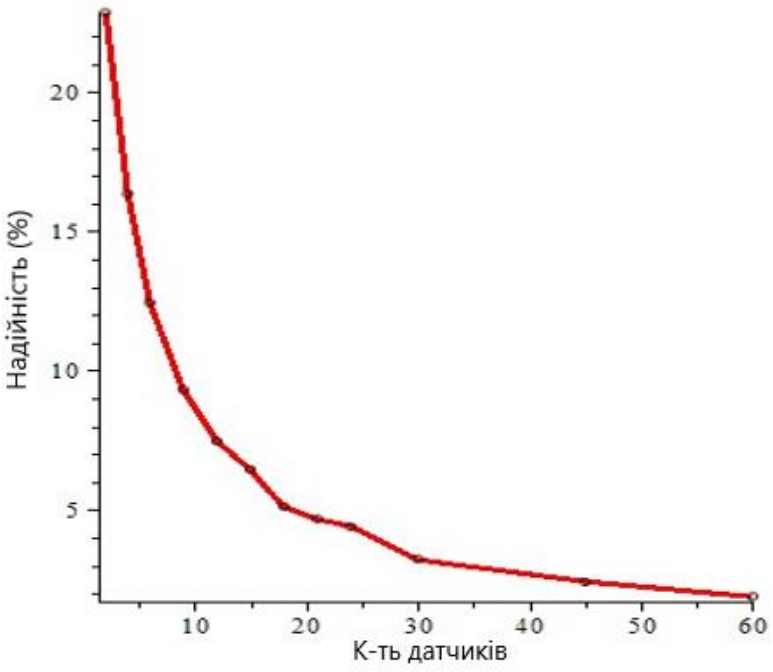
Для того, щоб проаналізувати вплив щільності, терміну служби та надійності мережі на продуктивність WSN, була проведена серія експериментів, що змінювали кількість вузлів датчиків, починаючи з 2, збільшуючи до 4, 6, 9, 12, 15, 18, 21, 24, 30, 45 і, нарешті, 60. (Кількість датчиків в одній стрибковій моделі приймали 10, 20 30, ..., 60, і після цих експериментів було зрозуміло, що

термін служби була по суті постійною, а надійність лінійною. У випадку LEACH потрібно було провести більше експериментів, щоб продемонструвати криві, що випливали з експериментів.) Радіус передачі для кожного датчика залишався на рівні 10 метрів, а кількість кластерів для цього додатка становила два (Найпростіша ситуація - мати дві головки кластера аналізувати з точки зору зіткнень даних на приймальному вузлі, що означає, що можна застосувати інтуїтивне розуміння того, що відбувається. Проте зміна кількості кластерів розглядається в підрозділі 4.1). Радіус передачі для цільового вузла також був встановлений на рівні 10 метрів. Швидкість передачі датчика фіксована в цьому експерименті, що означає, що датчики будуть передавати з тією ж швидкістю, що й інші.

У міру збільшення кількості вузлів датчиків у фіксованому просторі, більше датчиків може бути обрано головками кластера, і таким чином можна зберегти енергію для кожного датчика. Таким чином, термін служби мережі повинен збільшуватися із збільшенням кількості датчиків. Рисунок 4.1 підтверджує, як очікувалося, термін служби мережі збільшується із збільшенням щільності. Іншими словами, взаємозв'язок між щільністю та терміном служби мережі є позитивною кореляцією



а)



б)

Рисунок 4.1 – а) Взаємозв’язок кількості датчиків та терміну служби

б) Взаємозв’язок кількості датчиків та надійності.

Тривалість служби для цього експерименту на малюнку 4.1 (а) збільшується з 1541 до 2097, 2503, 2779, 3077, 3307, 3427, 3475, 3601, 3707, 3903 і, нарешті, до 4043. На рисунку 4.1 а) показано взаємозв'язок між надійністю і кількість датчиків. Надійність для цього експерименту знизилася з 22,86% до 16,35%, 12,44%, 9,31%, 7,46%, 6,45%, 5,13%, 4,67%, 4,38%, 3,23%, 2,40% і, нарешті, до 1,89%. Таким чином, взаємозв'язок між кількістю датчиків та надійністю пов'язаний з негативною кореляцією. Це можна пояснити наступним чином: Зі збільшенням щільності головки кластера будуть споживати набагато більше енергії для зв'язку з вузлами датчиків. Тоді енергія, що залишилася для кожної головки скупчення, буде швидко зменшуватися зі збільшенням щільності. Крім того, передача даних на приймальний вузол споживає багато енергії, і тоді все більше і більше обраних головок кластера не можуть передавати дані на приймальний вузол.

Таким чином, доцільно очікувати, що надійність зменшиться із збільшенням щільності.

Коли число датчиків дорівнювало 60, надійність виявилася 1,89%. Порівняно з попередніми даними (коли кількість датчиків дорівнює 10-50), Надійність досягла дуже низького рівня, але на даний момент термін служби мережі досяг найвищого значення 4043. Таким чином, користувачі можуть вибрати оптимальне значення щільності для цього застосування залежно від необхідної надійності.

Термін служби для LEACH набагато нижчий, ніж для одноразового стрибка. Це пов’язано з тим, що головки кластерів будуть споживати енергію для зв’язку з датчиками в кластерах, агрегування даних та передачі агрегованих даних у приймальний вузол. Незважаючи на те, що у програмі LEACH ця роль змінена, це призводить до великих витрат енергії. Наприклад, якщо у нас є два кластери з тридцятьма датчиками, то кожна головка кластера повинна мати справу приблизно з 15 датчиками. Наша модель показує, що кожна головка кластера витрачає втричі більше енергії одного нормального датчика за одиницю

часу, а це означає, що мережа витрачає більше енергії за одиницю часу, порівняно з тим, що не використовується головки кластера, що призводить до зменшення терміну служби. Також трапляється так, що час життя одноразового хмелю переважно вимірюється завдяки терміну служби найближчого датчика до приймального вузла, який буде дуже тривалим. Співвідношення тривалості життя для одноразового стрибка до LEACH у цих експериментах становить приблизно 4 для 60 датчиків.

Надійність для LEACH набагато нижча, ніж в Single-hop. Це пов'язано з тим, що головки кластерів будуть споживати багато енергії для зв'язку з датчиками в кластерах. Можливо, у кластерних головок недостатньо енергії для передачі пакетів на приймальний вузол, але вони продовжуватимуть запускати та скидати пакети. Крім того, коли трапляються зіткнення даних, вони будуть катастрофічними, оскільки всі дані з головок кластера втрачаються за одне зіткнення, тоді як це будуть лише дані, втрачені від окремих датчиків у випадку одного стрибка.

Якщо кількість датчиків, надійність та термін служби мережі помножити разом, у 12 випадках отримають такі цифри: 705, 1371, 1868, 2329, 2755, 3200, 3164, 3408, 3785, 3592, 4215 та 4585. Це дає показник того, скільки даних приймає приймальний вузол, час життя збільшується зі щільністю, тоді як надійність зменшується. Цифри вказують на те, що загальна кількість пакетів даних, отриманих приймальним вузлом, збільшуватиметься із збільшенням кількості датчиків, хоча дані, втрачені датчиками до того, як вони досягнуть головки кластера, ігноруються.

З даних можна помітити, що надійність, термін служби та кількість датчиків пов'язані за такою формулою:

$$\frac{\text{Надійність}}{\text{Термін служби}} \times \text{Кількість датчиків} = \text{Константа}$$

Це рівняння говорить, що швидкість успішного прийому пакетів даних за одиницю часу не залежить від кількості датчиків. Константа у наведеному вище

рівнянні буде залежати від параметрів моделювання, і це розумна модель, якщо кількість головок кластера невелика. Кількість датчиків у кластері є одним із способів вимірювання отриманих пакетів, але знову ігнорує дані, втрачені від датчиків, перш ніж вони досягнуть головки кластера. Такі втрачені дані збільшуватимуться із збільшенням кількості датчиків, так що для невеликої, середньої чи великої кількості датчиків, можливо, доведеться знаходити константу в правій частині рівняння.

Цей експеримент дає такі «константи» у 12 випадках (до шести знаків після коми): 0.000297, 0.000312, 0.000298, 0.000302, 0.000291, 0.000293, 0.000269, 0.000282, 0.000292, 0.000261, 0.000277, 0.000280, оскільки ці цифри дуже близькі одна до одної, вказує на розумність моделі.

Тепер, оскільки існує постійний коефіцієнт успішного прийому пакетів за одиницю часу, з підрахунку випливає, що будуючи графік надійності, помноженого на кількість датчиків відносно терміну служби, слід отримати рядок $ax + b$, де x представляє тривалість життя і a є константою отриманою вище.

Метод наближення найменших квадратів [79] був використаний для проходження лінії через точки даних, як показано на рисунку 4.2, це дає лінію:

$$0.00025x + 0.10993$$

Інвертуючи цю лінійну залежність, отримуємо таке рівняння:

$$= 4000y - 439.72, \quad (12)$$

де y – добуток надійності на кількість датчиків. 4000 - це швидкість, з якою використовується тривалість життя (енергія) на одиницю y. Постійна 439,72, здається, є показником терміну служби, що використовується в діяльності головки кластера, яка не залежить від кількості датчиків.

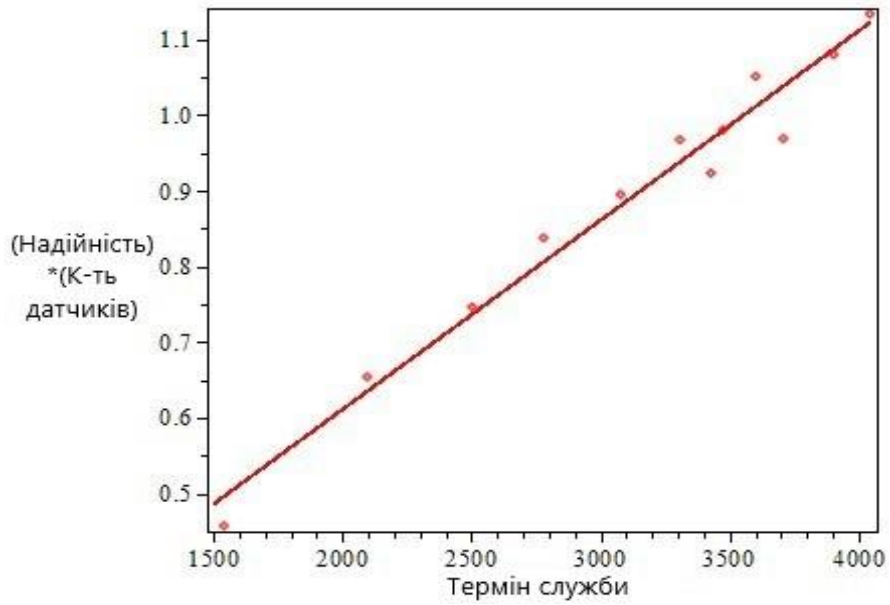
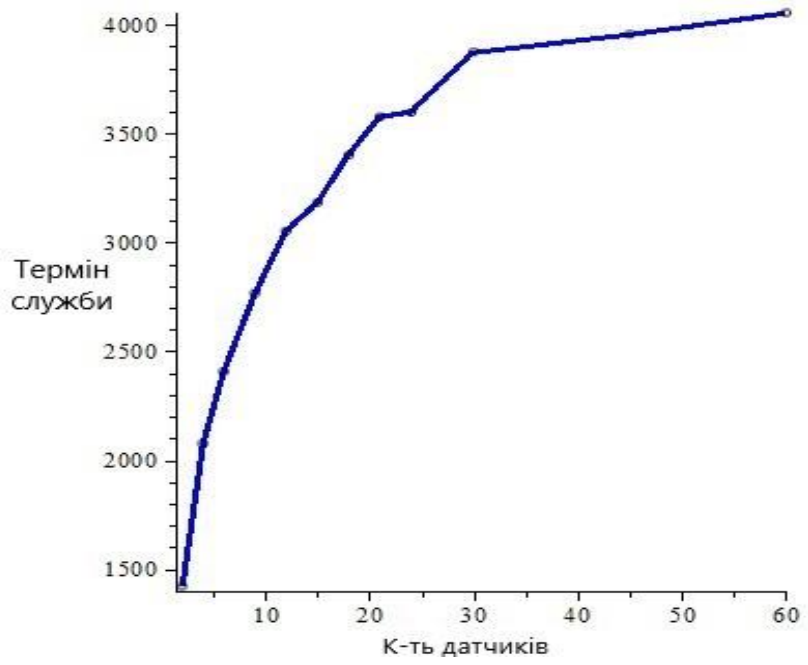


Рисунок 4.2 – Взаємозв’язок терміну служби і надійності *(кількості датчиків)

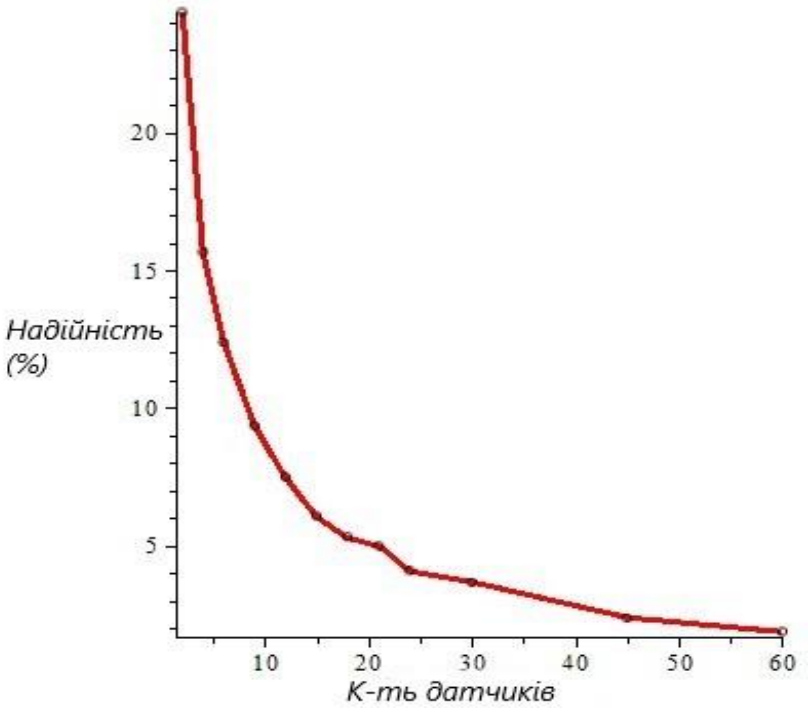
Неформальні випробування на радіуси менше 10 м. показали, що це призведе до подібних кривих як на рис. 4.1.

На рисунку 4.3 радіус передачі для датчиків і цільового вузла збільшено з 10 до 15 метрів (вибір радіуса відповідає попереднім експериментам). Усі вузли (включаючи загальні датчики, приймальні вузли та цільові вузли) розташовані в квадраті 10м x 10м. Найдовша відстань між вузлом і цільовим вузлом становить менше 14,15 метрів. Таким чином, радіус 15 м достатньо великий, щоб усі вузли отримали повідомлення від цільового вузла. (Ціль передає періодичний сигнал на всі датчики.) Термін служби для цього експерименту на рисунку 4.3(а) збільшується з 1421 до 2077, 2407, 2767, 3053, 3183, 3401, 3577, 3597, 3875, 3957 і, нарешті, до 4055. Надійність на рисунку 4.3 (б) зменшилась з 24,38% до 15,66%, 12,38%, 9,35%, 7,48%, 6,07%, 5,31%, 4,98%, 4,08%, 3,65%, 2,35% і, нарешті, до 1,87%. Порівнюючи Рисунок 4.1 та Рисунок 4.3, можна зробити висновок, що збільшення терміну служби та надійності не сильно впливає на збільшення радіуса з формою кривих, приблизно такою ж, як і раніше. Однак є певний експериментальний розкид результатів, оскільки головки кластерів будуть довільно розміщені в різних положеннях. Отже, коли кількість датчиків лише

два, радіус не повинен впливати на надійність або термін служби, оскільки ці датчики повинні передаватись в якості кластера голови.



а)



б)

Рисунок 4.3 – а) Взаємозв’язок кількісті датчиків та терміну служби

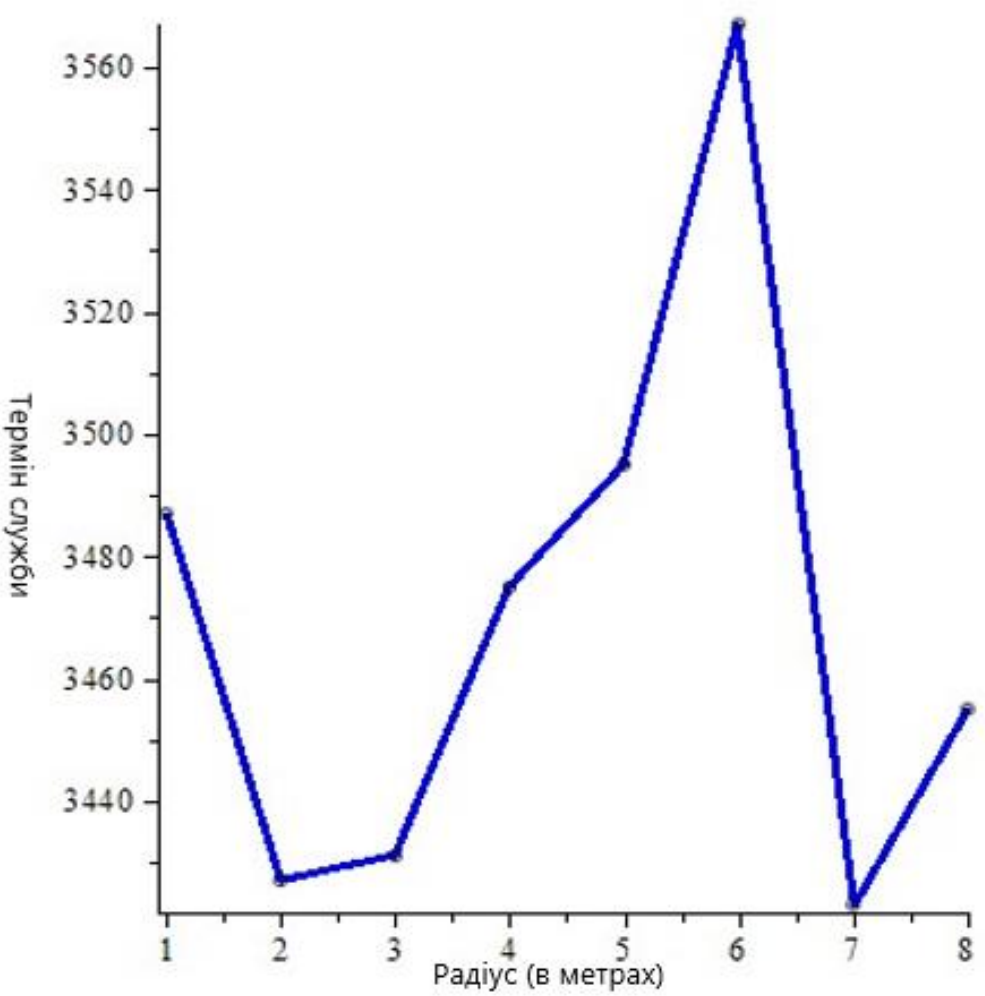
б) Взаємозв’язок кількості датчиків та надійності

2. Радіус —термін служби– надійність

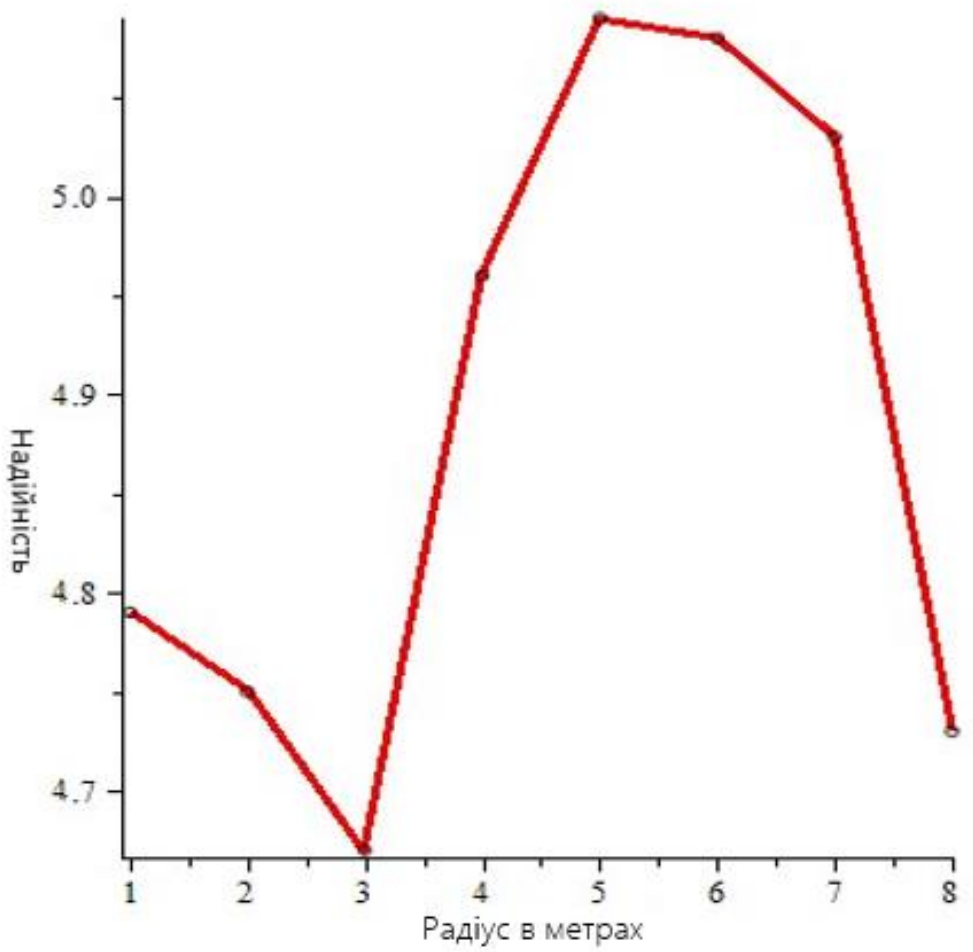
Для того, щоб проаналізувати вплив радіуса, терміну служби та надійності мережі на продуктивність WSN, була проведена серія експериментів з радіусом передачі кожного вузла, починаючи з одного метра, а потім збільшуючи з кроком з одного метра до восьми метрів. Можливість зв'язку з приймальним вузлом для датчиків обмежена радіусом передачі. У цьому експерименті було встановлено фіксоване значення 20 датчиків для щільності. Кількість кластерів для цього додатка становила два, а радіус передачі для цільового вузла також становив 15 метрів (Наявність двох головок кластера - це найпростіша ситуація для аналізу з точки зору зіткнень даних у приймальному вузлі. 15 метрів достатньо великий для цільовий вузол для передачі пакетів. Крім того, вибір цього налаштування такий самий, як встановлення цифр у Додатку.).

На рисунку 4.4 (а) значення терміну служби починається з 3487, а потім стає 3427, 3431, 3475, 3495, 3567, 3423 і, нарешті, 3455.

На рисунку 4.4 (б) значення надійності починається з 4,79%, а потім стає 4,75%, 4,67%, 4,96%, але за п'ятим сценарієм воно досягає найвищої точки 5,09%, а потім падає до 5,08%, 5,03% і нарешті до 4,73%.


3560
3540
3520
3500
3480
3460
3440
Термін служби
1
2
3
4
5
6
7
8
Радіус (в метрах)

а)



б)

Рисунок 4.4 − а) Радіус, термін служби. б) Взаємозв’язок радіусу та надійності.

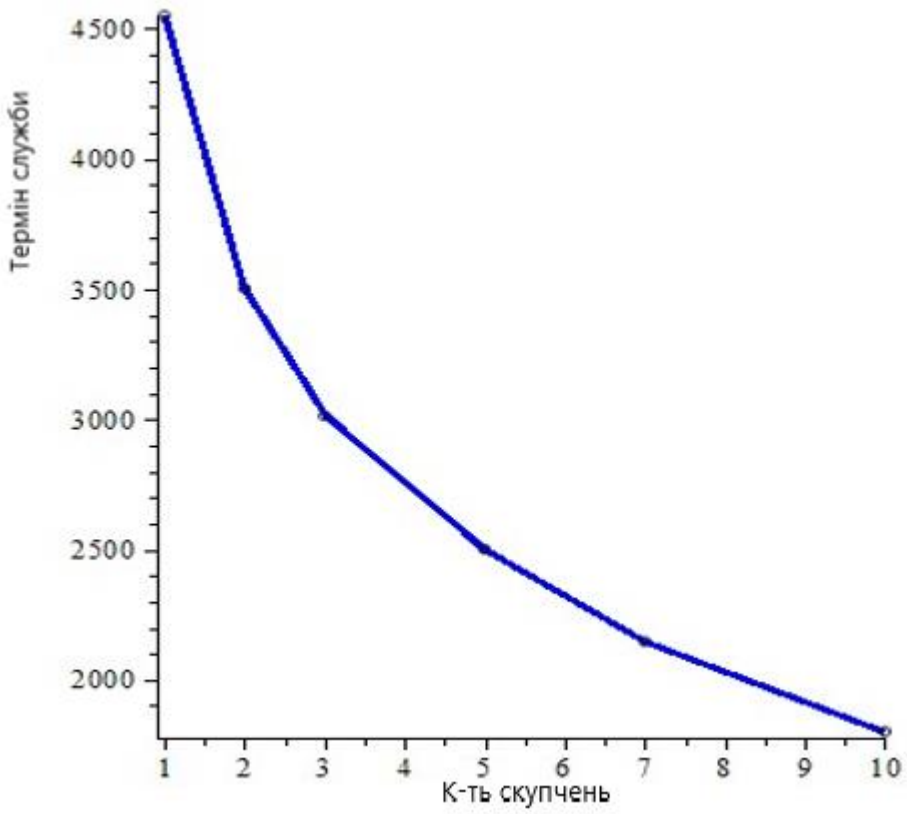
На рисунку 4.4, термін служби становить від 3400 до 3600, оскільки радіус збільшується з одного до восьми метрів. З іншого боку, надійність коливається між 4,6 і 5,2% із збільшенням радіуса. Причину такої кривої можна пояснити наступним чином: Коли датчики, розташовані близько до приймального вузла, стають кластерними головками, вони можуть передавати пакети на приймальний вузол. Тож на термін служби та надійність в основному впливає кількість датчиків, які можуть зв’язуватися з приймальним вузлом. Таким чином, ефект радіусу здається дуже слабким, і експерименти показують, що параметр радіус не є критичним для LEACH.

3. Кластер — термін служби — надійність

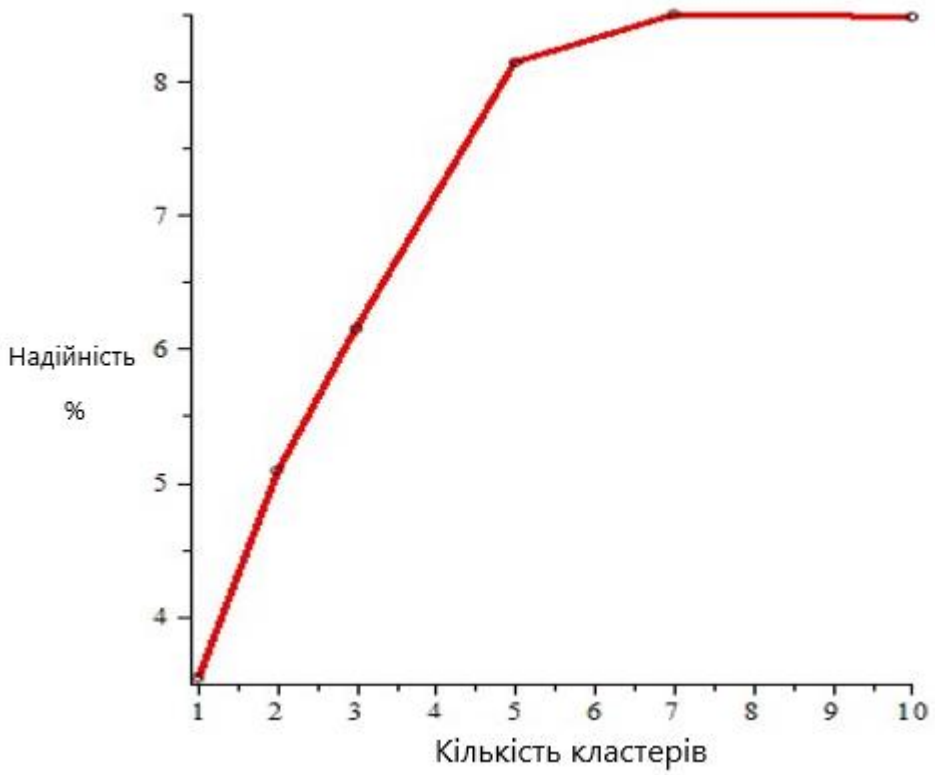
Кількість кластерів - ще один ключовий параметр для терміну служби мережі і ще один ключовий параметр для надійності мережі.

На рисунку 4.5 показано ефект зміни кількості кластерів.

На рисунку 4.5, коли число кластерів стає більшим, починаючи з 1, збільшуючись до 2, 3, 5, 7 і, нарешті, до 10, термін служби мережі зменшується, але надійність досягає найвищого значення, коли кількість кластерів дорівнює семи. Радіус передачі для кожного датчика залишається на рівні 15 метрів, а кількість датчиків - 20. Радіус передачі для цільового вузла також становить 15 метрів. Результат тут протягом терміном служби очікуваний, з кількістю датчиків та радіусом. Ця робота передбачає зменшення терміну служби із збільшенням кількості кластерних головок, оскільки вони забезпечують більшу витрату енергії системи.

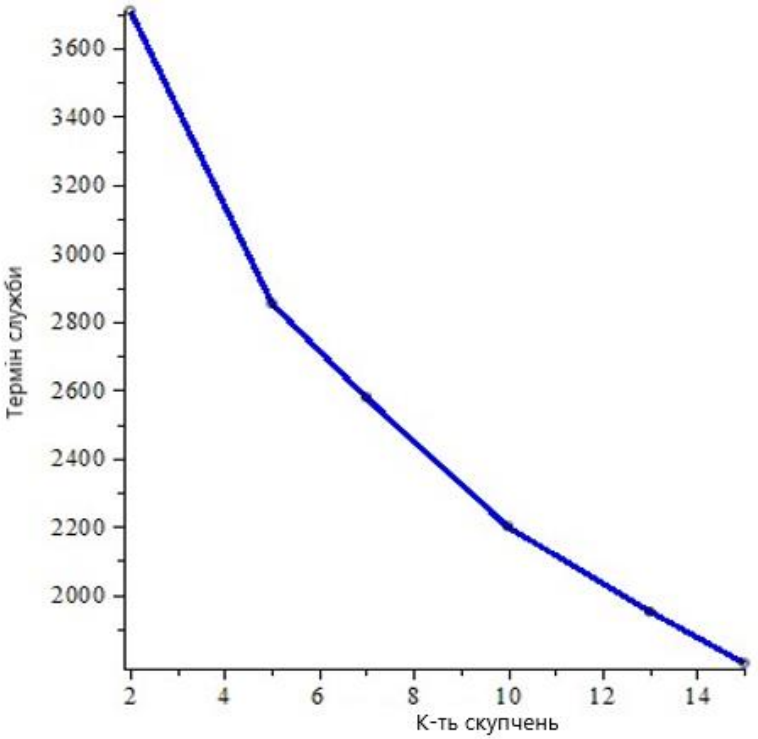


а)

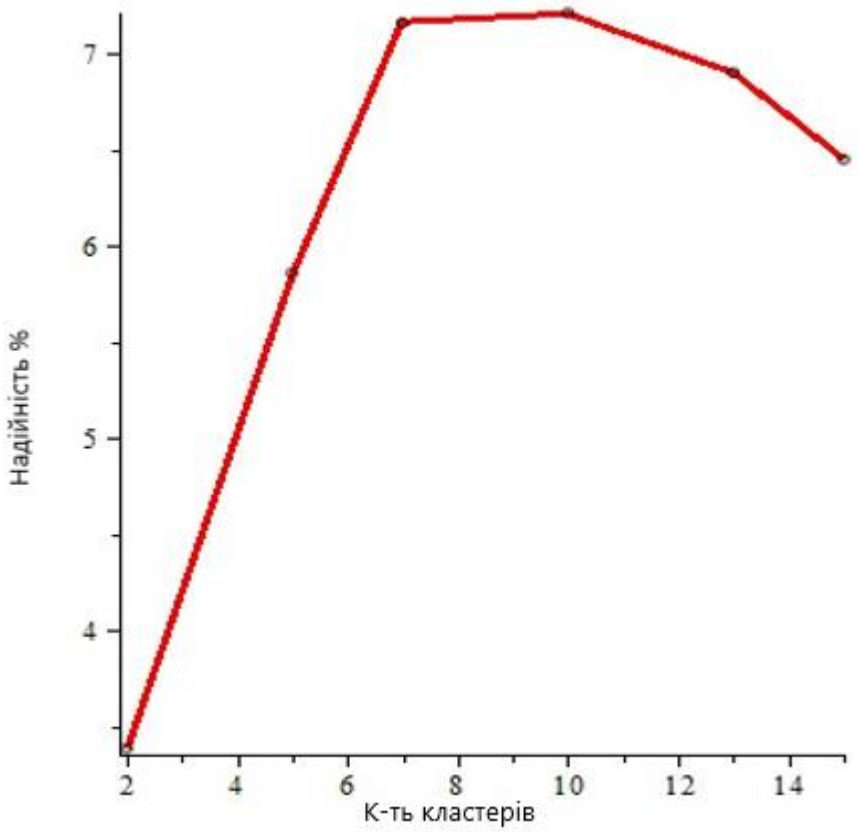


б)

Рисунок 4.5 − а) Взаємозв’язок кількісті кластерів та терміну служби (20 датчиків). б) Взаємозв’язок кількісті кластерів та надійності (20 датчиків).



а)

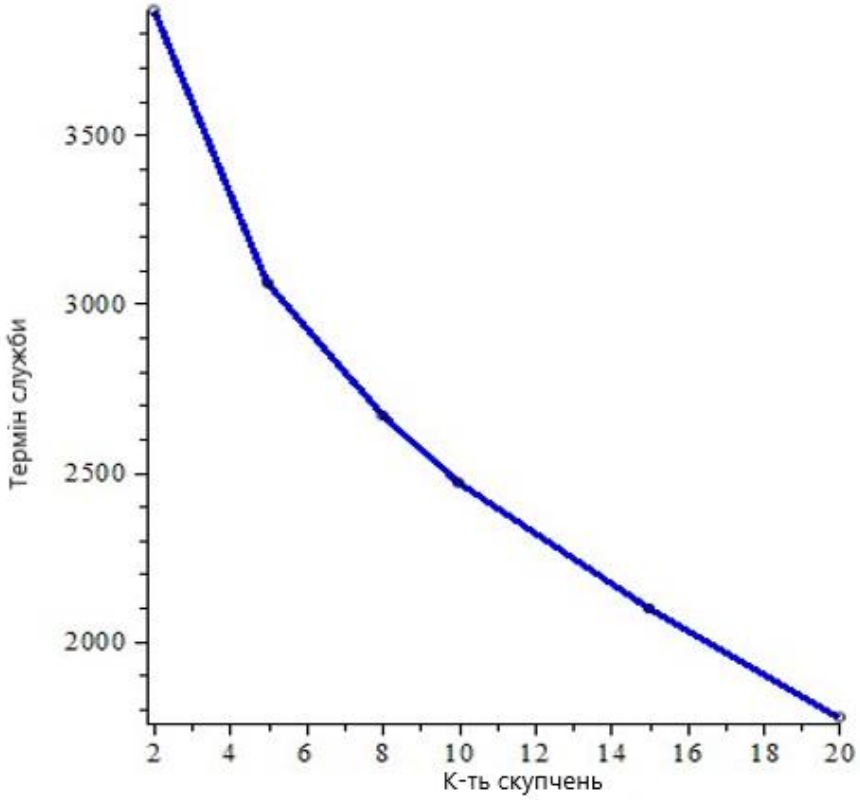


б)

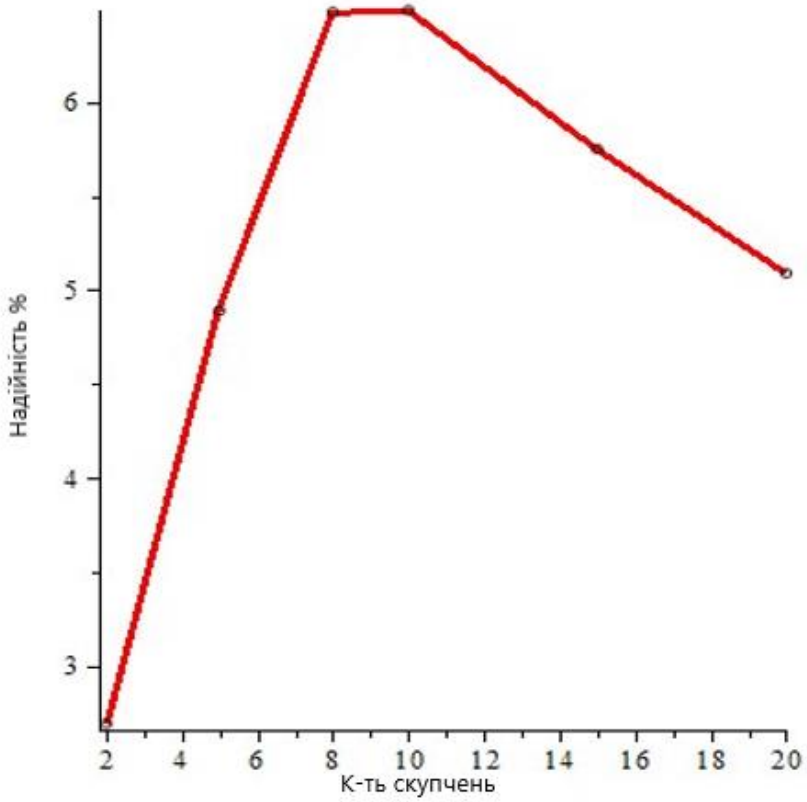
Рисунок 4.6 – а) Взаємозв’язок кількісті кластерів та терміну служби (30 датчиків). б) Взаємозв’язок кількісті кластерів та надійності (30 датчиків).

На рисунку 4.6, коли число кластерів стає більшим, починаючи з 2, збільшуючись до 5, 7, 10, 13 і, нарешті, до 15, термін служби мережі зменшується, але надійність досягає найвищого значення, коли кількість кластерів дорівнює 10. Радіус передачі для кожного датчика залишається на рівні 15 метрів, але кількість датчиків зараз становить 30. Радіус передачі для цільового вузла знову становить 15 метрів.

На рисунку 4.7, коли число кластерів стає більшим, починаючи з 2, збільшуючись до 5, 8, 10, 15 і, нарешті, до 20, термін служби мережі зменшується, але надійність досягає найвищого значення, коли кількість кластерів дорівнює 10. Радіус передачі для кожного датчика і цільового вузла все ще 15 метрів, але кількість датчиків зараз становить 40.


Термін служби
3500
3000
2500
2000
2
4
6
8
10
12
14
16
18
20
К-ть скупчень

а)


Надійність %
6
5
4
3
2
4
6
8
10
12
14
16
18
20
К-ть скупчень

б)

Рисунок 4.7 – а) Взаємозв’язок кількісті кластерів та терміну служби (40 датчиків). б) Взаємозв’язок кількісті кластерів та надійності (40 датчиків).

4.2. Параметри оцінки

1. Термін служби моделі

У цьому розділі буде запропоновано просте співвідношення між часом експлуатації та кількістю датчиків, якщо всі інші параметри залишаються незмінними. Термін служби може бути змодельована за допомогою рівняння з двома параметрами, що включає енергію, використовувану в діяльності головки кластера за одиницю часу та *e*, енергія, яка використовується в звичайній діяльності датчика за одиницю часу.

(Ця теза передбачає, що всі розгорнуті датчики мають однакові моделі енергоспоживання)

Енергія, яка використовується в звичайній діяльності датчика, повинна бути незалежною від кількості датчиків і, отже, є постійною. З іншого боку, збільшуватиметься кількість датчиків, оскільки кожен кластер буде містити більше датчиків, і тому головці кластера доведеться агрегувати (і передавати) більше даних. Проте вважається постійною, знаходячи для неї середнє значення.

Нехай *K* - це повна енергія батареї датчика, нехай *n* загальне число датчиків і нехай *r* кількість кластерів. Тоді термін служби повинна регулюватися рівнянням

$$nK = rtE + (n - r)te, \tag{13}$$

де *t* позначає термін служби. Головка кластера діє як звичайний датчик, а також об'єднує дані інших датчиків. Він передає всі ці сукупні дані (включаючи свої власні як датчик) на приймальний вузол. Головка кластера, що діє як звичайний датчик, незвична тим, що вона не повинна передавати свої дані на головку кластера, і з цієї причини на рисунку включена енергія, використана

головкою кластера, яка діє як "нормальний" датчик, а не присвоює її значення (яке було б занадто великим).

$$t = nK/[rE + (n - r)e]. \quad (14)$$

Оскільки $n \to$, $t \to K/e$ - це, звичайно, не залежить від r та E. Тож горизонтальна лінія повинна утворювати горизонтальну лінію $t = K/e$ на графіку щільності та терміну служби. З іншого боку, коли $n = r$, $t = K/E$, як і слід було очікувати.

Рисунок 4.1 складається з наступних дванадцяти точок даних: (2, 1541), (4, 2097), (6,2503), (9, 2779), (12, 3077), (15, 3307), (18, 3427), (21, 3475), (24, 3601), (30, 3707), (45, 3903), (60, 4043). Дані для 15 і 30 датчиків можна використовувати для отримання середнього значення.

Зараз

$$15K = 6614E + 42991e. \quad (15)$$

і

$$30K = 7414E + 103796e. \quad (16)$$

Виключення з цих рівнянь дає

$$13228E + 85982e = 7414E + 103796e. \quad (17)$$

і так

$$5814E = 17814e. \quad (18)$$

тоді

$$e = 0.326372516E\ . \quad (19)$$

так, що

$$K = 1376.338722E. \quad (20)$$

Використовуючи ці наближення

$$t = 1376.338722n/2 + 0.326372516(n - 2). \quad (21)$$

Отож, оскільки $n\rightarrow$, $t\rightarrow 4217.079119$ - це повинно бути завищенням терміну служби через середнє значення, прийняте за E.

Графік функції (n, t), визначений за наведеною вище формулою (червона крива на рисунку 4.8), був накладений на графік довічного періоду на рисунку 4.1 (синім на рисунку 4.8), що підтверджує, що це хороша модель.

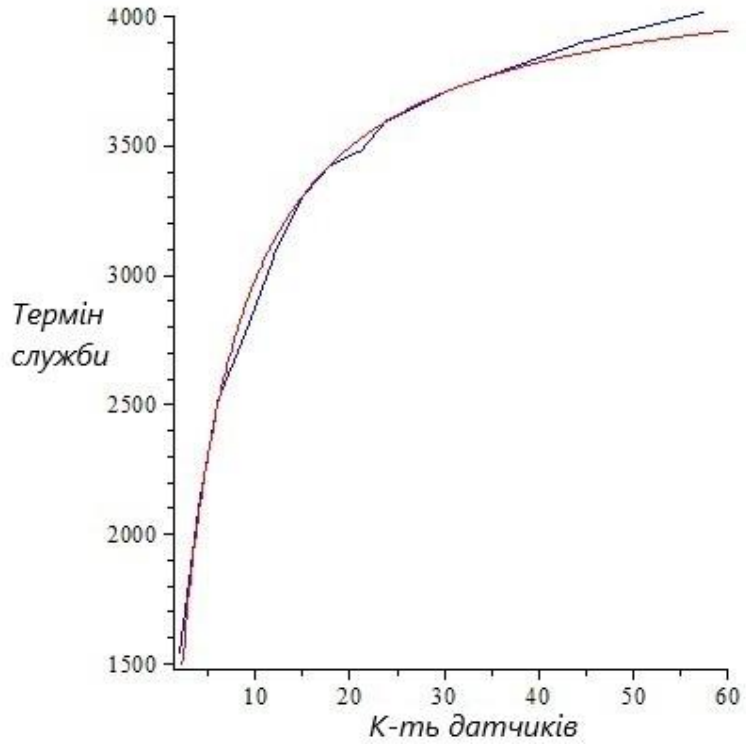


Рисунок 4.8 – Модель терміну служби

Якщо n великий у порівнянні з більш простими відносинами можна знайти шляхом заміни – r на n в наведеному вище рівнянні, так що

$$nK = rtE + nte, \quad (22)$$

де t позначає термін служби.

Тоді

$$t = nK/[rE + ne]. \quad (23)$$

Повторення вищезазначеного аналізу (не припускаючи цього) дає результат

$$e = 0.24225rE, \tag{24}$$

та

$$K = 1135.237983rE, \tag{25}$$

Використовуючи ці наближення

$$T = 1135.237983n/[1 + 0.24225n], \tag{26}$$

незалежно від r.

Звичайно, насправді буде відома (середня) загальна енергія батареї датчика, оскільки її можна виміряти до розгортання.

2. Надійність моделі

Формула, що з'єднує надійність і термін служби наведена вище, тепер буде поєднана з рівнянням для терміну служби, наведеною у попередньому пункті, щоб отримати наступну формулу для надійності:

$$Надійність = \frac{K}{rE+(n-r)e} \times Константа, \tag{27}$$

де константа повинна бути визначена експериментально. На основі даних на рисунку 4.1 (r = 2) та середнього арифметичного 0,000288 констант, отримано таке рівняння:

$$Надійність = \frac{0.396385551}{2+0.326372516(n-2)}, \tag{28}$$

Побудова цього графіку (червоним на малюнку 4.9) над графіком 4.2 для надійності (синім на рисунку 4.9) показує, що це хороша модель для надійності.

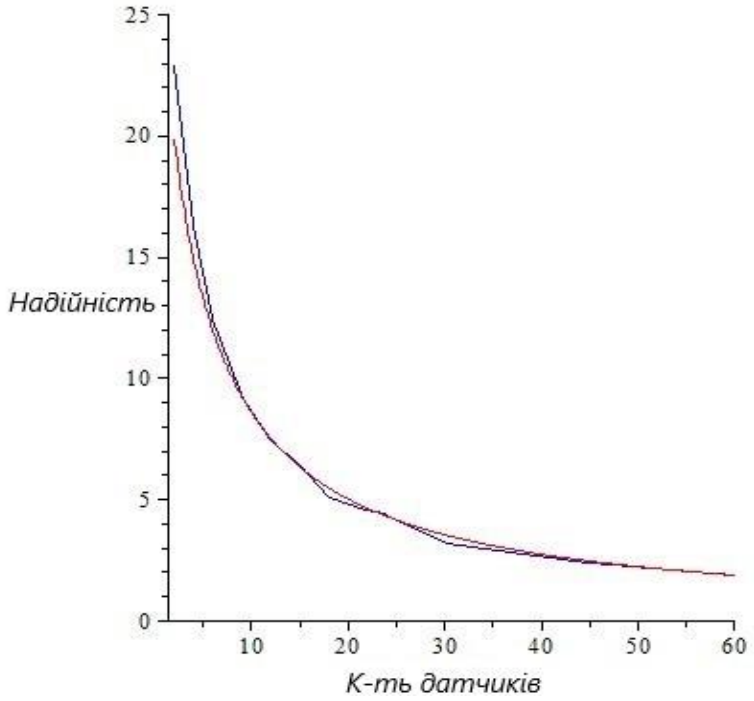


Рисунок 4.9 – Модель надійності

У цих двох підрозділах докладно викладено базову версію LEACH, яка все ще широко використовується. Протокол LEACH успішно змодельований математично. Однак протягом багатьох років були розроблені нові протоколи на основі LEACH для отримання покращених результатів від WSN.

4.3. Оцінка моделей для протоколу ближнього зв'язку

Як правило, багатоскачкова маршрутизація в бездротовій сенсорній мережі є більш ефективною, ніж односкачкова, особливо якщо мережа велика. У мульти-скачковій маршрутизації дані передаються від датчика до датчика, використовуючи певний протокол, поки не досягнуть приймального вузла.

Оскільки зв’язок стає дедалі складнішим із використанням протоколу маршрутизації з кількома переходами, зіткнення даних буде більш складним, ніж для протоколу з одним переходом, а це, в свою чергу, впливає на надійність та термін служби. Для зменшення ефекту зіткнення даних у бездротових сенсорних мережах радіус передачі повинен бути встановлений відповідним чином. Метрики, що використовуються при моделюванні, зазвичай відображають мету

розробленого алгоритму. Оптимальний шлях маршрутизації для передачі зібраних даних від вихідного вузла до приймального може бути визначений метрикою. Більшість схем маршрутизації просто використовують кількість метрів як метрику [80], де кількість стрибків - це кількість передач на маршруті від джерела до пункту призначення. Однак, якщо вузли можуть регулювати свою потужність передачі (знаючи місце розташування своїх сусідів), постійну метрику на стрибок можна замінити метрикою потужності, яка залежить від відстані між вузлами.

Протокол ближнього зв'язку є як типовим протоколом маршрутизації на основі місцезнаходження, так і протоколом маршрутизації з кількома стрибками. Отже, ця робота реалізувала протокол у J-Sim як приклад. Для реалізації цього протоколу кожен вузол повинен знати своє власне положення, положення своїх сусідів в межах свого діапазону передачі та ближнього зв'язку ближчого полягає в тому, що датчик передавача передаватиме свого найближчого сусіда, який знаходиться ближче до приймального вузла.

Будова системи та експериментальна установка

Як протокол рівня MAC вибрано прорізний протокол ALOHA. Слотовий ALOHA - це тип системи передачі TDMA, який покращує управління конфліктами завдяки використанню маяків. Слот ALOHA може змусити один активний датчик майже безперервно передавати з повною швидкістю каналу, таким чином, можна отримати кращі результати для протоколу ближнього зв'язку.

Модельована площа для наступних експериментів визначається як квадрат 10 метрів на 10 метрів із довільно розгорнутими вузлами. Протокол маршрутизації –протокол ближнього зв'язку. Приймальний вузол для цієї програми розташований у центрі цієї області.

Результати оцінки моделей для протоколу ближнього зв'язку

1. **Щільність – термін служби – надійність**

Була проведена серія експериментів з кількістю датчиків, починаючи з 10, і збільшуючи з кроком від 10 до 300 датчиків. Радіус передачі для кожного датчика був встановлений на рівні 15 метрів, оскільки він є достатньо великим для передачі даних в будь-яку точку площі. Надійність та термін служби для цього експерименту представлені в таблиці 4.1.

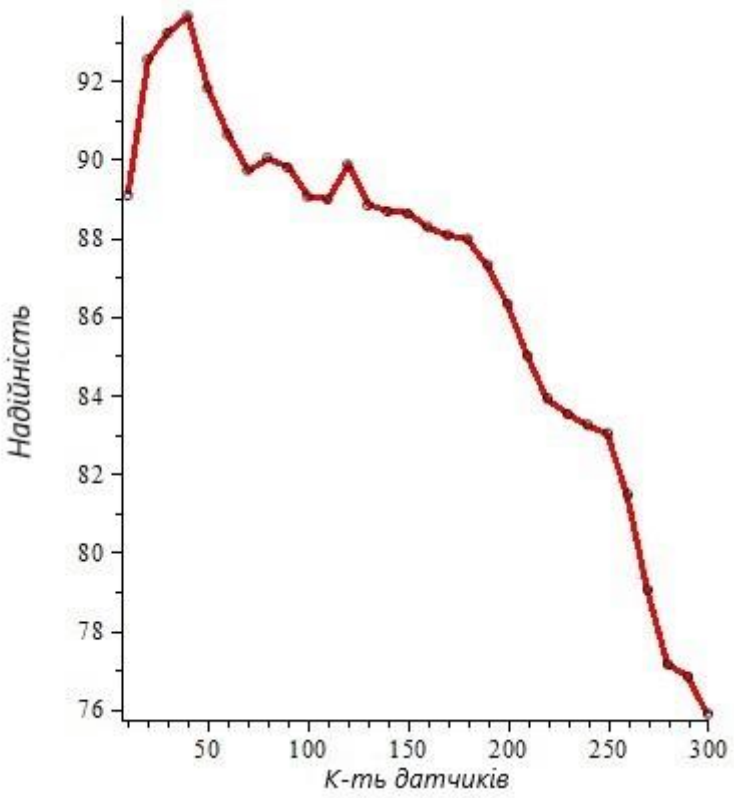


Рисунок 4.10 – Взаємозв’язок надійності та щільності для протоколу ближнього зв’язку

На рисунку 4.10 взаємозв'язок між кількістю датчиків та надійністю дуже чіткий. Надійність для цієї програми зросла, коли кількість датчиків зросла до 40, коли вона досягла найвищого значення. Потім воно суттєво зменшилось, оскільки кількість датчиків зросла з 40 до 300, коли досягло найнижчого значення. Це можна пояснити зауваженням, що зі збільшенням щільності вузлів все більше датчиків приєднується до процесу передачі даних і, отже, зв'язок між датчиками стає все більш і більш складнішим. Тож втрачені дані через зіткнення та затримку даних не можна ігнорувати. Отже, розумно очікувати, що надійність зменшиться із щільністю.

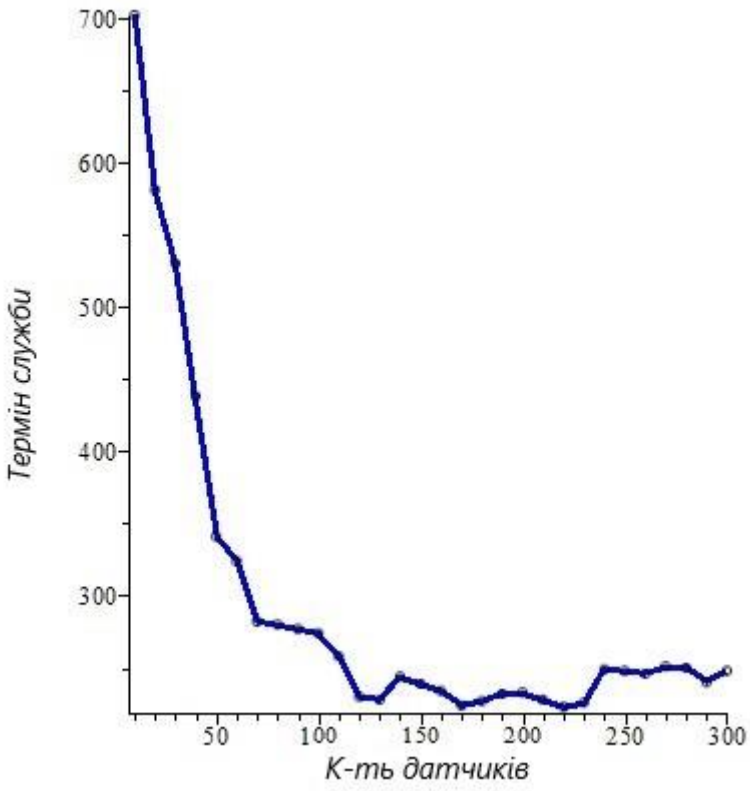


Рисунок 4.11 − Взаємозв’язок терміну служби та щільності для протоколу ближнього зв’язку

На рисунку 4.11 термін служби досяг найнижчого значення, коли кількість датчиків дорівнювало 220, тоді як найвище значення терміну служби було, коли було 10 датчиків.

У протоколі ближнього зв’язку, відправка пакету на приймальний вузол вимагатиме від кожного датчика передачі своїх даних по шляхах передачі до найближчих датчиків до приймального вузла. Ці найближчі датчики (лише близько двох або трьох) будуть приймати всі дані в мережі і передавати їх у приймальний вузол, використовуючи велику кількість енергії. Таким чином, мережа ближнього зв’язку, як правило, досить швидко відділяється від приймального вузлу. Якби мережа LEACH з двома або трьома кластерами працювала з фіксованими головками кластера, то можна було б очікувати, що її термін служби буде дуже коротким, оскільки кожна головка кластера повинна збирати та передавати всі дані в мережі (як мережа ближнього зв’язку на початку). Однак найважливішою особливістю LEACH є те, що кластерні головки

обертаються між датчиками, що дозволяє рівномірно розподілити цей енергетичний тягар між датчиками, що призводить до набагато більш тривалого терміну служби.

На рисунку 4.11 зверніть увагу, що коли кількість датчиків дорівнює 40, надійність становила 93,64%, що є найвищим рівнем, але з цим числом термін служби досить короткий. Це ілюструє, що користувачі можуть вибрати оптимальне значення щільності для цього додатка залежно від необхідної надійності та терміну служби.

Таблиця 4.1 − Кількість датчиків, надійність, термін служби для протоколу ближнього зв’язку

К-ть датчиків	*Надійність %*	*Термін служби*
10	89.08	702
20	92.53	581
30	93.21	530
40	93.64	438
50	91.81	341
60	90.63	324
70	89.72	282
80	90.03	280
90	89.78	277
100	89.05	274
110	88.98	258
120	89.86	230
130	88.83	228
140	88.67	244
150	88.61	239
160	88.28	234

170	88.07	224
180	87.97	227
190	87.31	232
200	86.31	233
210	84.99	228
220	83.91	223
230	83.51	226
240	83.24	249
250	83.02	248
260	81.46	246
270	79.04	251
280	77.15	250
290	76.84	240
300	75.89	248

2. Радіус – термін служби – надійність

Була проведена серія експериментів з радіусом передачі, який починався з 1 метра і збільшувався з кроком в один метр до 10 метрів. Кількість датчиків було встановлено на рівні 200.

На рисунку 4.12 показано взаємозв'язок між надійністю та радіусом передачі. Необхідно, щоб усі вузли датчиків застосовували найближчу техніку ближчого передавання для доставки повідомлень. Коли радіус дорівнює одному метру, надійність є найнижчою; однак, якщо радіус перевищує один метр, величина надійності залишається відносно стабільною і коливається менше ніж на 10%. Причину цього можна пояснити наступним чином:

- Для з'єднання радіусом в один метр багато даних буде втрачено в процесі передачі, а отже, надійність у системі негативно позначається. З іншого боку,

із збільшенням радіуса відбуватиметься більше зіткнень даних, так що це впливатиме і на надійність.

- Значення надійності коливається в межах від 85 до 90% для радіуса, більшого або рівного двом метрам.

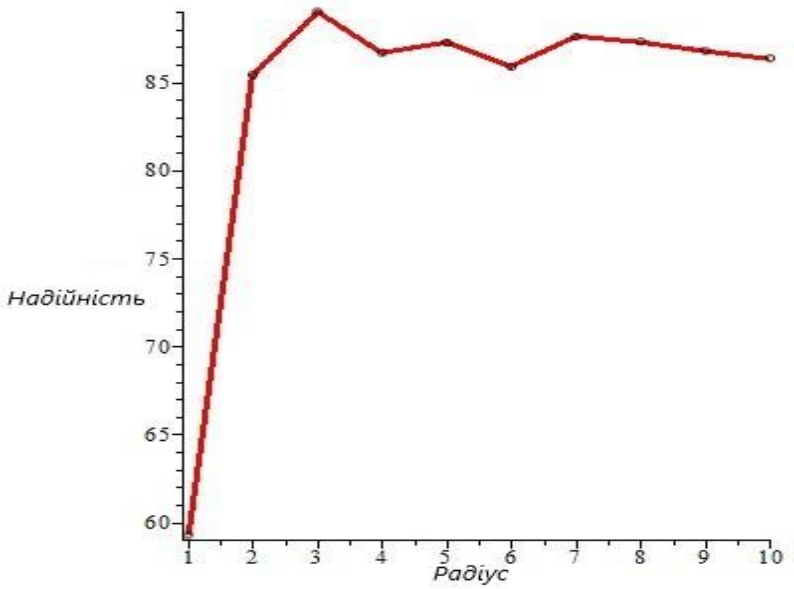


Рисунок 4.12 − Взаємозв’язок радіусу та надійності для протоколу ближнього зв’язку

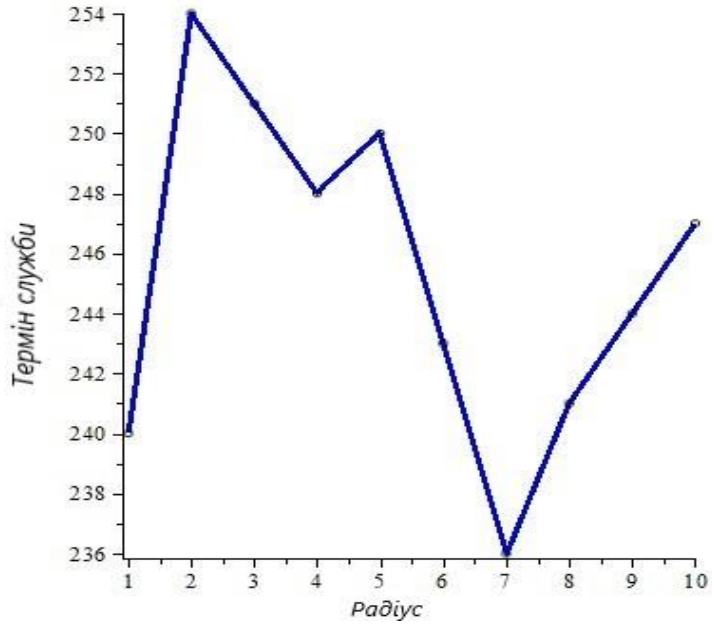


Рисунок 4.13 − Взаємозв’язок радіусу та терміну служби для протоколу ближнього зв’язку

На рисунку 4.13 показано взаємозв'язок між терміном служби та радіусом передачі. На цьому показнику немає чіткої тенденції, оскільки термін служби коливається лише від 236 до 254, і його можна вважати постійним для будь-якого радіуса від 1 до 10 метрів. Якщо кількість датчиків налаштовано на 20, результати будуть такими:

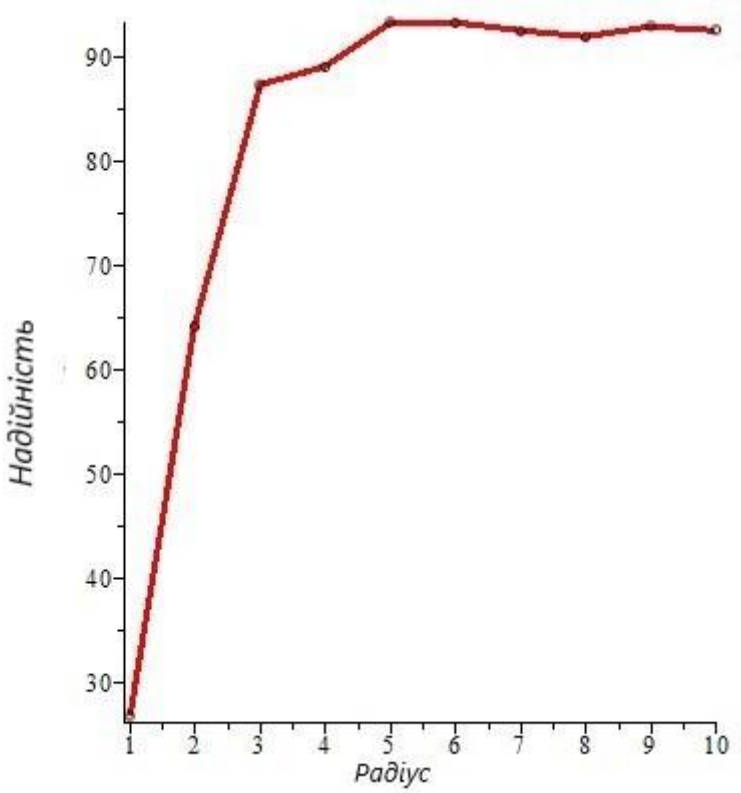


Рисунок 4.14 − Взаємозв’язок радіусу та надійності для протоколу ближнього зв’язку (20 датчиків)

На рисунку 4.14 показано взаємозв'язок між надійністю та радіусом передачі. Надійність для цієї програми зросла, оскільки радіус передачі збільшився з 1 до 5 метрів. Надійність досягла 93,28%, коли радіус становив 5 метрів. Коли радіус збільшився з 5 до 10 метрів, значення надійності дещо коливалось, оскільки радіус досить великий, щоб передавати дані для цього найближчого ближчого протоколу на приймальний вузол.

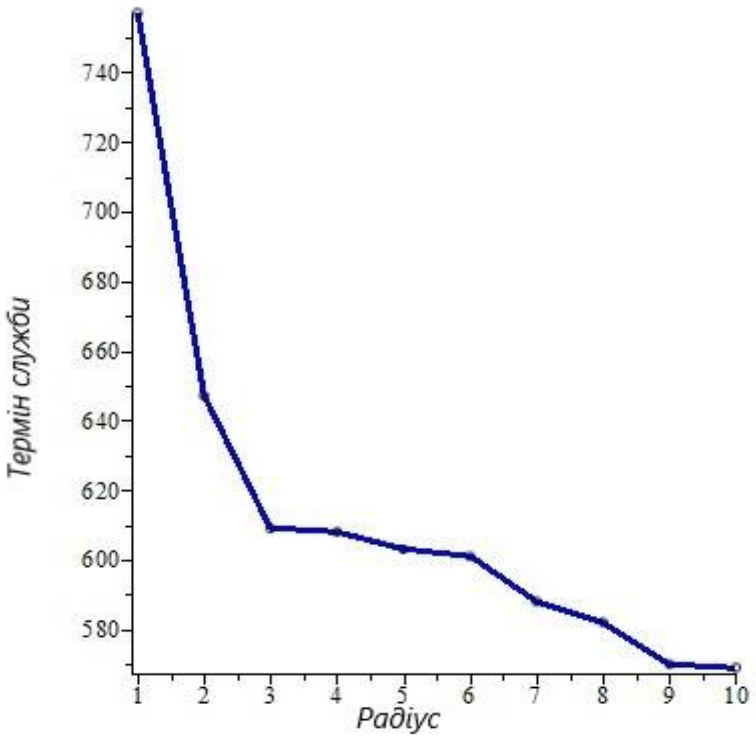


Рисунок 4.15 − Взаємозв’язок радіусу та терміну служби для протоколу ближнього зв’язку (20 датчиків)

На рисунку 4.15 показано взаємозв'язок між терміном та радіусом передачі. Коли радіус збільшувався з 1 до 10 метрів з кроком в один метр, термін служби зменшився з 757 до 569. Причина цього падіння могла бути пов’язана з тим, що зі збільшенням радіуса зв'язок між датчиками ускладнювався, отже, набагато було витрачено більше енергії, що призвело до зменшення терміну служби.

4.4. Висновки до четвертого розділу

У цьому розділі була проведена серія експериментів із інструментом моделювання J-Sim на основі протоколу LEACH, і було зроблено кілька висновків:

a) Термін служби мережі збільшується із збільшенням кількості датчиків.
b) Існує лінійна залежність між кількістю пакетів даних, отриманих приймальним вузлом та терміном служби.

c) Вплив радіуса слабкий, що вказує на те, що цей параметр не є критичним для LEACH.
d) Кількість кластерів впливає на зіткнення даних та енергію, а отже, на надійність та термін служби мережі.

На основі цих результатів моделювання побудовано деякі моделі у вигляді рівнянь.

Також у цьому розділі, виходячи із серії експериментів, проведених в інструменті моделювання J-Sim, для протоколу ближнього зв'язку випливає кілька висновків:

a) Надійність для цієї програми зросла, коли кількість датчиків зросла до 40, коли вона досягла найвищого значення. Потім воно суттєво зменшилось, оскільки кількість датчиків зросла з 40 до 300.
b) Термін служби зменшився, оскільки кількість датчиків зросла до 130, а потім вона дещо коливалась, коли кількість датчиків зросла до 300. Термін служби досяг найнижчого значення, коли число датчиків дорівнювало 220, тоді як найвище значення терміну служби було при 10 датчиках.
c) Радіус може суттєво вплинути на надійність та термін служби, коли є лише 20 датчиків. Коли радіус збільшився з 1 до 10 метрів, термін служби зменшився з 757 до 569. З іншого боку, надійність зросла, коли радіус передачі збільшився з 1 до 5 метрів. Потім надійність трохи коливалась, коли радіус збільшувався до 10 метрів.

Висновки

1. Проаналізовано та досліджено описи бездротових сенсорних мереж, а також надано деякі подробиці про J-Sim. Крім того, зроблено огляд роботи над параметрами оцінки WSN. Опрацьовано роботи дослідників, які виконали певні моделювання та отримали корисні результати із відповідними параметрами оцінки. Однак виходячи з їх досліджень не створено ані математичні моделі для відповідних параметрів, ані підходи для компромісу. Таким чином, інструменти моделювання не будуть необхідні для розгортання датчиків, що призводить до економії грошей і часу.

2. Розглянуто три різні категорії протоколів маршрутизації, для кожної категорії було розглянуто та описано ряд прикладів. Описано підмножину протоколів маршрутизації для аналізу, таких протоколів маршрутизації як: Single-hop, LEACH та Nerely Closer, які приймаються як представники плоских, ієрархічних та протоколів маршрутизації, які базуються на розташуванні відповідно.

3. Після аналізу найпростішого Single-hop протоколу запропоновано дві моделі оцінки серед параметрів терміну служби, надійності та щільності. На основі цих інтелектуальних моделей оцінки користувачі бездротової мережі датчиків можуть безпосередньо передбачити термін служби та надійність. Це означає, що вузли датчиків можуть бути розгорнуті в такій мережі без подальшого моделювання.

4. Проведена серія експериментів із інструментом моделювання J-Sim на основі протоколу LEACH. В результаті було виявлено, що:

- термін служби мережі збільшується із збільшенням кількості датчиків;
- існує лінійна залежність між кількістю пакетів даних, отриманих приймальним вузлом та терміном служби;
- кількість кластерів впливає на зіткнення даних та енергію, а отже, на надійність та термін служби мережі.

Також виходячи із серії експериментів, проведених в інструменті моделювання J-Sim, для протоколу ближнього зв’язку випливає, що надійність, термін служби та радіус напряму залежать від кількоті датчиків.

ПЕРЕЛІК ПОСИЛАНЬ

1) I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. "A survey on sensor networks", Communications magazine, 40(8), IEEE, 2002, pp.102-114.
2) J. Oakes. "A pressure sensor for automotive applications", Proceedings of the Third International Conference on Automotive Electronics, London, October 20-23, United Kingdom, 1981, pp. 143–149.
3) R. Brown, K. Carton, and W. Wright. "Considerations in high-volume production of hybrid pressure sensor modules for automotive applications", IEEE Solid-State Sensor and Actuator Workshop, South Carolina, USA, June 2-5, IEEE, 1986, pp. 34–37.
4) D. Sparks and R. Brown. "Buying micromachined sensors in large volumes", Sensors–The Journal of Applied Sensing Technology, 12 (2), 1995, pp. 53–57.
5) W. Baney, D. Chilcott, X. Huang, S. Long, J. Siekkinen, D. Sparks, and S. Staller. "A comparison between micromachined piezoresistive and capacitive pressure sensors", SAE Technical Paper 973241, 1997, pp. 61–64.
6) Шахнович И.А. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – с. 288.
7) F.L. Lewis. "Wireless sensor networks", In: Smart Environments: Technologies, Protocols, and Applications, Wiley & Sons, New Jersey, USA, November 11, 2004, pp. 11–46.
8) T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, T. Yan, R. Stoleru, L. Gu, G. Zhou, J. Hui, and B. Krogh. "Vigilnet: an integrated sensor network system for energy efficient surveillance", ACM Transactions on Sensor Networks, 2 (1), ACM, 2006, pp. 1–38.
9) C. McGann, F. Py, K. Rajan, J. Ryan, and R. Henthorn. "Adaptive control for autonomous underwater vehicles", Proceedings of the Twenty-Third AAAI Conference on Artificial Intelligence, Chicago, USA, July 13-17, 2008, pp. 1319–1324.
10) Гуйда О.Г., Петрова В.М., Бондарук О.А. Вибір протоколу маршрутизації за допомогою імітаційного моделювання безпровідних сенсорних мереж //

Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського – 2017 – С. 3-6

11) K.K. Khedo, R. Perseedoss and A. Mungur. "A wireless sensor network air pollution monitoring system", International Journal of Wireless & Mobile Networks, 2010, pp. 31-45.
12) "Vision Sensors" – Режим доступу: http://www.tektron.ie/vision_sensors.htm
13) "Distributed Detection for Smart Sensor Networks" – Режим доступу: http://www.antd.nist.gov/wctg/smartsensors/sensornetworks.html
14) V. Seal, A. Raha, S. Maity, S.K. Mitra, A. Mukherhee and M.K. Naskar. "A simple flood forecasting scheme using wireless sensor networks", International Journal of Ad-hoc Sensor and Ubiquitous Computing, 2012.
15) S. Molina, I. Soto and R. Carrasco. "Detection of gases and collapses in underground mines using WSN", Industrial Technology (ICIT), IEEE, 2011, pp. 219-225.
16) S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser and M. Turon. "Wireless sensor networks for structural health monitoring", Proceedings of the 4th international conference on Embedded networked sensor systems, ACM, 2006, pp. 427-428.
17) N.K. Suryadevara, S.C. Mukhopadhyay, R. Wang and R.K. Rayudu. "Forecasting the behavior of an elderly using wireless sensors data in a smart home", Engineering Applications of Artificial Intelligence, 26(10), 2013, pp. 2641-2652.
18) J. Byun, B. Jeon, J. Noh, Y. Kim and S. Park. "An intelligent self-adjusting sensor for smart home services based on ZigBee communications", Consumer Electronics, 58(3), IEEE, 2012, pp. 794-802.
19) H.N. Pham, D. Pediaditakis and A. Boulis. "From simulation to real deployments in WSN and back", World of Wireless, Mobile and Multimedian Networks, Espoo, Finland, IEEE, 2007, pp. 1-6.
20) E. Egea-Lopez, J. Vales-Alonso, A.S. Martinez-Sala, P. Pavón-Mariño, and J. García-Haro. "Simulation tools for wireless sensor networks", Proceedings of

the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS05), Article 24, Philadelphia, USA, July 24-28, 2005.

21) "The Network Simulator–NS-2" – Режим доступу: http://www.isi.edu/nsnam/ns/ (accessed 3rd July 2014).

22) I. Downard. "Simulation sensor networks in NS-2", Technical Report NRL/FR/5522-04-10073, Naval Research Laboratory, Washington DC, USA, 2004.

23) U. Kaage, V. Kahmann, and F. Jondral. "An OMNET++ TCP model", Proceedings of the European Simulation Multiconference, Prague, Czech Republic, June 6-9, 2001, pp. 409–413.

24) M. Erdei, A. Wagner, K. Sója, and M. Székely. "A networked remote simulation architecture and its remote OMNET++ implementation", Proceedings of the European Simulation Multiconference, Prague, Czech Republic, June 6-9, 2001, pp. 235–242.

25) A. Wagner and M. Erdei. "Agent-based resource management for remote simulation systems and an implementation for remote OMNET++", Proceedings of the European Simulation Multiconference, Prague, Czech Republic, June 6-9, 2001, pp. 270–274.

26) A. Varga. "The OMNET++ discrete event simulation system", Proceedings of the European Simulation Multiconference, Prague, Czech Republic, June 6-9, 2001, pp. 319–330.

27) C. Mallanda, A. Suri, V. Kunchakarra, S.S. Iyengar, R. Kannan, A. Durresi, and S. Sastry, "Simulating wireless sensor networks with OMNET++" – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.331.6889&rep=rep1&typ=pdf

28) A. Varga and R. Hornig. "An overview of the OMNET++ simulation environment", Proceedings of the 1st International Conference on Simulation

Tools and Techniques for Communications, Networks and Systems & Workshops, Article 60, ICST, Marseille, France, March 3-7, ACM, 2008

29) P. Levis, N. Lee, M. Welsh and D. Culler. "TOSSIM: Accurate and scalable simulation of entire TinyOS applications", Proceedings of the 1st international conference on Embedded networked sensor systems, New York, USA, ACM, 2003, pp. 126-137.

30) P. Levis and N. Lee. "Tossim: A simulator for tinyos networks", UC Berkeley, 2003.

31) P. Levis and N. Lee, "TOSSIM: A simulator for TinyOS networks" – Режим доступу: http://www.tinyos.net/tinyos-1.x/doc/nido.pdf

32) J. Polley, D. Blazakis, J. McGee, J. Rusk, and J.S. Baras. "ATEMU: a fine-grained sensor network simulator", First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, USA, October 4-7, IEEE, 2004, pp. 145–152.

33) L. Girod L, J. Elson, A. Cerpa, T. Stathopoulos, N. Ramanathan, and D. Estrin. "EmStar: A software environment for developing and deploying wireless sensor networks", Proceedings of the General Track: USENIX Annual Technical Conference, Boston, USA, June 27-July 2, 2004, pp. 283–296.

34) L. Girod, N. Ramanathan, J. Elson, T. Stathopoulos, M. Lukac, and D. Estrin. "Emstar: A software environment for developing and deploying heterogeneous sensor-actuator networks", ACM Transactions on Sensor Networks, 3 (3), Article 13, 2007.

35) A. Sobeih, W. Chen, J.C. Hou, L. Kung, N. Li, H. Lim, H. Tyan, and H. Zhang. "J-Sim: a simulation environment for wireless sensor networks", Proceedings of the 38th Annual Symposium on Simulation, Washington DC, April 4-6, IEEE, 2005, pp. 175–187.

36) Борисенко А.С., Галкин П.В. Адекватность моделей беспроводных сенсорных сетей в средах имитационного моделирования // Восточно-Европейский журнал передовых технологий. – 2013. – № 4/ 9 (64). – С. 52–55.

37) B. Karp and H.T. Kung. "GPSR: greedy perimeter stateless routing for wireless networks", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Massachusetts, USA, August 6-11, ACM, 2000, pp. 243–254.

38) C. Intanagonwiwat, R. Govindan and D. Estrin. "Directed diffusion: a scalable and robust communication paradigm for sensor networks", Proceedings of the 6th annual international conference on Mobile computing and networking, New York, USA, ACM, 2000, pp. 56-67.

39) A. Sobeih, J.C. Hou, L.-C. Kung, N. Li, H. Zhang, W.-P. Chen, H.-y. Tyan, and H. Lim. "J-Sim: a simulation and emulation environment for wireless sensor networks", Wireless Communications, 13 (4), IEEE, 2006, pp. 104–119.

40) T.S. Rappaport. "Wireless communications: principles and practice", 1996.

41) W. Lee and Y. Xu. "On localized prediction for power efficient object tracking in sensor networks", Proceedings of the 23rd International Conference on Distributed Computers Systems Workshops, Rhode Island, USA, May 19-22, 2003, pp. 434–439.

42) K. Niyogi, S. Mehrotra, N. Venkatasubramanian, and X. Yu. "Adaptive target tracking in sensor networks", Proceedings of the Communication Networks and Distributed Systems Modelling and Simulation Conference, San Diego, USA, January 18-24, 2004, pp. 253–258.

43) C.F. Huang, H. Lee, S.P. Kuo, and Y.C. Tseng. "Location tracking in a wireless sensor network by mobile agents and its data fusion strategies", The Computer Journal, 47 (4), 2004, pp. 448–460.

44) F. Zhao, J. Shin, and J. Reich. "Information-driven dynamic sensor collaboration for tracking applications", Signal Processing Magazine, 19 (2), IEEE, 2002, pp. 61–72.

45) G. He and J.C. Hou. "Tracking targets with quality in wireless sensor networks", Proceedings of the 13th IEEE International Conference on Network Protocols, Boston, USA, November 6-9, IEEE, 2005, pp. 63–74.

46) X. Wang, J. Ma, S. Wang, and D. Bi. "Prediction-based dynamic energy management in wireless sensor networks", Sensors, 7 (3), 2007, pp. 251–266.

47) Q. Zhang and W. Qu. "An Energy Efficient Clustering Approach in Wireless Sensor Networks", International Conference on Computer Science and Electronics Engineering, 1, Hangzhou, China, IEEE, 2012, pp. 541-544.

48) S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava. "Coverage problems in wireless ad-hoc sensor networks", Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies, 3, Anchorage, USA, April 22-26, IEEE, 2001, pp. 1380–1387.

49) M. Cardei, M.T. Thai, Y. Li, and W. Wu. "Energy-efficient target coverage in wireless sensor networks", Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 3, Miami, USA, March 13-17, IEEE, 2005, pp. 1976–1984.

50) E. Olule, G. Wang, M. Guo, and M. Dong. "Rare: an energy-efficient target tracking protocol for wireless sensor networks", International Conference on Parallel Processing Workshops, Xi-an, China, September 10-14, IEEE, 2007, pp. 76.

51) S.D. Muruganathan, D.C.F. Ma, R.I. Bhasin, and A. Fapojuwo. "A centralized energy-efficient routing protocol for wireless sensor networks", Communications Magazine, 43 (3), IEEE, 2005, pp. S8–13.

52) M. Yoon, Y.K. Kim and J.W. Chang. "An energy-efficient routing protocol using message success rate in wireless sensor networks", Journal of Convergence, 4(1), 2013, pp. 15-22.

53) R. Tynan, M.J. O'Grady, G.M.P. O'Hare, and C. Muldoon. "Benchmarking latency effects on mobility tracking in WSNs", Proceedings of the Second International Workshop on Applications of Ad-hoc and Sensor Networks, Bradford, United Kingdom, May 26-29, IEEE, 2009, pp. 768–774.

54) W.R. Heinzelman, J. Kulik, and H. Balakrishnan. "Adaptive protocols for information dissemination in wireless sensor networks", Proceedings of the Fifth

ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, USA, August 15-19, IEEE, 1999, pp. 174–185.

55) C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. "Directed diffusion for wireless sensor networking", IEEE Transactions on Networking, 11 (1), IEEE, 2003, pp. 2–16.

56) D. Braginsky and D. Estrin. "Rumor routing algorithm for sensor networks", Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, USA, September 28, ACM, 2002, pp. 22–31.

57) Y. Liu and Z. Wang. "Maximizing energy utilization routing scheme in wireless sensor networks based on minimum hops algorithm", Computers & Electrical Engineering, 38(3), 2012, pp. 703-721.

58) A. Manjeshwar and D. Agrawal. "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks", Proceedings of the 15th International Parallel & Distributed Processing Symposium, San Francisco, USA, April 23-27, 2001, pp. 2009–2015.

59) W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, 2, USA, January 4-7, IEEE, 2000, pp. 3005–3014.

60) J. Xu, N. Jin, X. Lou, T. Peng, Q. Zhou, and Y. Chen. "Improvement of LEACH protocol for WSN", Ninth International Conference on Fuzzy Systems and Knowledge Discovery, Sichuan, China, May 29-31, IEEE, 2012, pp. 2174–2177.

61) H. Gou and Y. Yoo. "An energy balancing LEACH algorithm for wireless ensor networks", Seventh International Conference on Information Technology: New Generations, Las Vegas, Nevada, USA, April 12-14, IEEE, 2010, pp. 822–827.

62) X. Fan and Y. Song. "Improvement on LEACH protocol of wireless sensor network", International Conference on Sensor Technologies and Applications, pp.260–264, Valencia, Spain, October 14-20, IEEE, 2007.

63) H. Junping, J. Yuhui, and D. Liang. "A time-based cluster-head selection algorithm for LEACH", IEEE Symposium on Computers and Communications, Marrekech, Morocco, July 6-9, IEEE, 2008, pp. 1172–1176.

64) S.A. Awwad, C.K. Ng, N.K. Noordin and M.F.A. Rasid. "Cluster based routing protocol for mobile nodes in wireless sensor network", Wireless Personal Communications, 61(2), 2011, pp. 251-281.

65) B. Manzoor, N. Javaid, O. Rehman, M. Akbar, Q. Nadeem, A. Iqbal and M. Ishfaq. "Q-LEACH: A new routing protocol for WSNs", Procedia Computer Science, 19, 2013, pp. 926-931.

66) A.A. Kadhim and M.W. Abdulrazzaq. "Efficient Routing Techniques for Wireless Sensor Networks", Journal of Applied Sciences, 14(24), 2014, pp. 3479-3485.

67) T. Hou and V. Li. "Transmission range control in multihop packet radio networks", IEEE Transactions on Communications, 34, IEEE, 1986, pp. 38–44.

68) H. Frey, S. Rührup, and I. Stojmenović. "Routing in wireless sensor networks", Guide to Wireless Sensor Networks, Springer, 2009, pp. 81–111.

69) I. Stojmenovic and X. Lin. "Power-aware localized routing in wireless networks", IEEE Transactions on Parallel and Distributed Systems, 12 (11), IEEE, 2001, pp. 1122–1133.

70) S. Fedor and M. Collier. "On the problem of energy efficiency of multi-hop vs one-hop routing in Wireless Sensor Networks", Advanced Information Networking and Applications Workshops, 2, 2007, pp. 380-385.

71) P. Khurana and I. Aulakh. "Wireless Sensor Network Routing Protocols: A Survey", International Journal of Computer Applications, 75(15), 2013, pp. 17-25.

72) Y. Chen and Q. Zhao. "On the lifetime of wireless sensor networks", Communications Letters, 9(11), IEEE, 2005, pp. 976-978.

73) R. Nagpal, H. Shrobe and J. Bachrach. "Organizing a global coordinate system from local information on an ad hoc sensor network", Information Processing in Sensor networks, Springer Berlin Heidelberg, 2003, pp. 333-348.

74) P.Z. Zahariev, G.V. Hristov and T.B. Iliev. "Study on the impact of node density and sink location in WSN Technological Developments in Networking", Education and Automation, Springer Netherlands, 2010, pp. 539-542.

75) K. Xu, M. Gerla and S. Bae. "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks", Global Telecommunications Conference, 1, IEEE, 2002, pp. 72-76.

76) J. Caffery and G.L. Stuber. "Subscriber location in CDMA cellular networks", IEEE Transactions on Vehicular Technology, 47 (2), IEEE, 1998, pp. 406–416.

77) A.J. Viterbi. "CDMA: principles of spread spectrum communication", Addison-Wesley, Boston, USA, 1995.

78) A. Shah. "Code division multiple access: a tutorial", Rowan University, Wireless Communications, 1999, pp. 6–10.

79) H.L. Harter. "Least squares", Encyclopedia of statistical sciences, 1983.

80) S.S. Chiang, C.H. Huang, and K.C. Chang. "A minimum hop routing protocol for home security systems using wireless sensor networks", Electronics, 53 (4), IEEE, 2007, pp. 1483–1489.

Додаток А

Збірник наукових праць «Актуальні проблеми комп'ютерних наук АПКН-2019»

Міністерство освіти і науки України

Хмельницький національний університет

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XI всеукраїнської науково-практичної конференції

«Актуальні проблеми комп'ютерних наук АПКН-2019»

14-15 листопада 2019

Том 1

Роботи студентів та молодих вчених

Факультету програмування та комп'ютерних і телекомунікаційних систем ХНУ

Хмельницький 2019

Зміст

Додаток Б

Апробації наукових результатів

УДК 004

Жалюк А.І., Лужанський В.І.

Хмельницький національний університет

Розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах

Розглянуто параметри оцінки терміну служби, щільності, радіуса та надійності для застосувань бездротових сенсорних мереж. Було отримано низку результатів моделювання для протоколів маршрутизації Single-hop, LEACH та ближнього зв'язку, які були реалізовані в симуляційній платформі J-Sim. Результати моделювання були проаналізовані та запропоновано кілька моделей оцінки відповідно. Таким чином, моделювання може не знадобитися для того, щоб користувачі могли вибрати відповідний протокол маршрутизації.

Introduced the evaluation parameters of Lifetime, Density, Radius, and Reliability for the applications of wireless sensor networks. A series of simulation results have been obtained for the Single-hop, LEACH and Nearest Closer routing protocols which have been implemented in J-Sim simulation platform. Simulation results have been analyzed and several evaluation models have been proposed respectively. Thus, simulations may not be necessary for the users to choose a suitable routing protocol.

Бездротові сенсорні мережі складаються з багатьох вузлів (датчиків). Багато досліджень у цій галузі базуються на надто спрощеному аналізі, і тому лише обмежена впевненість може бути надана прогнозам, що випливають з таких експериментів, це все виявляється через обмежену кількість датчиків, які можна розподілити в реальній експериментальній мережі. Таким чином, моделювання стало звичним способом тестування нових додатків та нових протоколів перед реальним розгортанням [1].

Датчик [2] - це конвертер, який вимірює фізичну величину і перетворює її в сигнал, який може зчитувати електронний прилад. Наприклад, термоелемент перетворює температуру на вихідну напругу, яку можна зчитати вольтметром.

Як правило, вузли датчиків є дорогими і їх важко перевірити у великій кількості, тому інструменти моделювання стають необхідними для формування мереж. В даному випадку розглянуто декілька протоколів маршрутизації які інтегровані в інструмент моделювання J-Sim.

J-Sim [3] (раніше відомий як JavaSim) - це середовище симуляції композиційної мережі з відкритим вихідним кодом, що базується на компонентах. Також це платформа, заснована на Java. Датчики на основі Java в майбутньому можуть бути інтегровані з інструментами моделювання на основі Java.

Існує три основних типи протоколів маршрутизації в бездротових сенсорних мережах.:

- Плоскі протоколи;
- Ієрархічні протоколи;
- Протоколи, що базуються на розташуванні.

Single-hop, *LEACH* та протокол ближнього зв'язку є репрезентативними та базовими протоколами маршрутизації для кожного з цих типів відповідно. Отже, в рамках цієї роботи, Single-hop, LEACH та протоколи ближнього зв'язку інтегровані в інструмент моделювання J-Sim.

Далі наведено загальну модель інструменту моделювання [4]. Модель включає кілька сенсорних вузлів, радіоканалів, середовищ, факторів та приймальних вузлів.

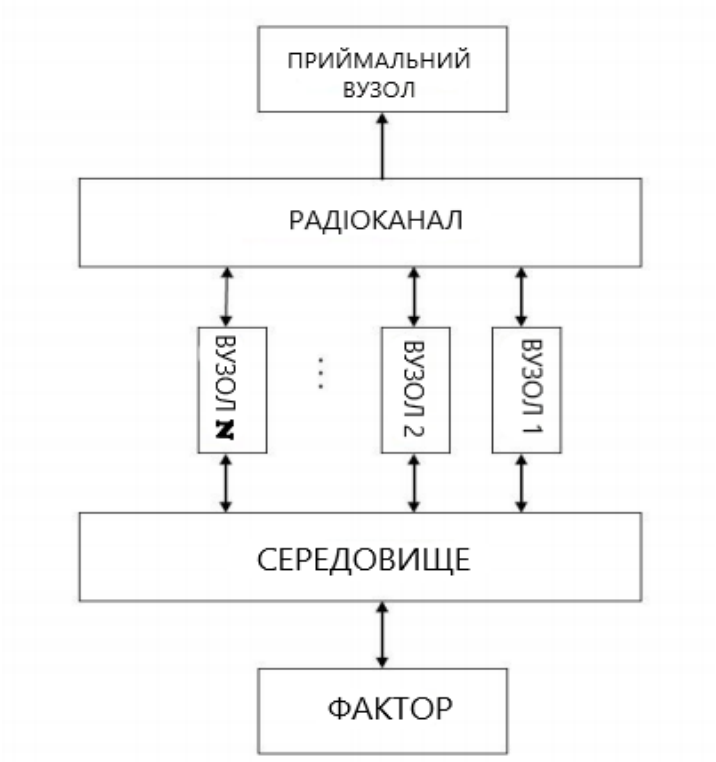


Рисунок 1.1 − Модель моделювання

Детальний опис компонентів на цьому рисунку такий:

а) *Вузли:* Вузли є базовими пристроями в цій моделі. Кожен вузол може зв'язуватись між собою через радіоканал. Існує також стек протоколів для управління цими комунікаціями.

б) *Навколишнє середовище:* Компонент навколишнього середовища моделює генерації та розповсюдження подій, які сприймаються вузлами датчика, і можуть призвести до інших дій датчика.

в) *Радіоканал:* Цей компонент характеризує поширення радіосигналів між вузлами в мережі.

г) *Приймальні вузли:* Приймальні вузли отримуватимуть дані із загальних сенсорних датчиків.

д) *Фактори:* Фактори відіграють роль генератора подій, що представляє запит для вузлів

У цій роботі представлена серія результатів моделювання. На основі результатів даною роботою розроблено деякі математичні моделі, що забезпечують дизайн більш ефективні бездротові сенсорні мережі без попереднього використання моделювання. Найважливішою формулою, яку було отримано, є наступна у LEACH:

$$\frac{\text{Надійність}}{\text{Термін служби}} \times \text{Кількість датчиків} = \text{Константа}$$

Це рівняння говорить, що швидкість успішного прийому пакетів даних за одиницю часу не залежить від кількості датчиків. Константа у наведеному вище рівнянні буде залежати від параметрів моделювання, і це розумна модель, якщо кількість головок кластера невелика. Кількість датчиків у кластері є одним із способів вимірювання отриманих пакетів, але знову ігнорує дані, втрачені від датчиків, перш ніж вони досягнуть головки кластера. Такі втрачені дані збільшуватимуться із збільшенням кількості датчиків, так що для невеликої, середньої чи великої кількості датчиків, можливо, доведеться знаходити константу в правій частині рівняння.

Проведена серія експериментів із інструментом моделювання J-Sim, і було зроблено кілька висновків:

1. Термін служби мережі збільшується із збільшенням кількості датчиків.
2. Існує лінійна залежність між кількістю пакетів даних, отриманих приймальним вузлом та терміном служби.
3. Вплив радіуса слабкий, що вказує на те, що цей параметр не є критичним.
4. Кількість кластерів впливає на зіткнення даних та енергію, а отже, на надійність та термін служби мережі.

Отже, запропонована система кодування та інтегрування Java протоколів Single-hop, ближнього зв’язку та LEACH в інструмент моделювання J-Sim для розробки моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах, забезпечує взаємозв’язок параметрів оцінки, таких як термін служби, надійність та радіус. Також дана система надає математичну модель для кожного протоколу. Ці математичні моделі фіксують взаємозв'язки між певними ключовими параметрами, які в більшості випадків є лінійними або кусочно-лінійними. Моделі також ілюструють, що в деяких випадках параметр, такий як радіус, як правило, не є критичним для значень, отриманих для інших параметрів, таких як термін служби та надійність, що дозволяє користувачам

ігнорувати такі надлишкові параметри. Після того, як додано більше протоколів та пов'язаних з ними моделей, можна безпосередньо передбачити більше параметрів. Моделі оцінки в рамках цієї роботи дозволяють здійснювати розгортання вузлів датчиків без моделювання, щоб задовольнити запити замовника, що призводить до значної економії часу та витрат.

Перелік посилань:

1. H.N. Pham, D. Pediaditakis and A. Boulis. "From simulation to real deployments in WSN and back", World of Wireless, Mobile and Multimedia Networks, c. 1-6, Espoo, Finland, IEEE, 2007.
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. "A survey on sensor networks", Communications magazine, 40(8), c.102-114 IEEE, 2002.
3. A. Sobeih, W. Chen, J.C. Hou, L. Kung, N. Li, H. Lim, H. Tyan, and H. Zhang. "J-Sim: a simulation environment for wireless sensor networks", Proceedings of the 38th Annual Symposium on Simulation, c. 175–187, Washington DC, April 4-6, IEEE, 2005.
4. E. Egea-Lopez, J. Vales-Alonso, A.S. Martinez-Sala, P. Pavón-Mariño, and J.García-Haro. "Simulation tools for wireless sensor networks", Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS05), Article 24, Philadelphia, USA, July 24-28, 2005.

Додаток В

Презентація дипломної роботи

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

КАФЕДРА АВТОМАТИЗАЦІЇ КОМПЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ І ТЕЛЕКОМУНІКАЦІЙ

ДИПЛОМНА РОБОТА

Розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах

Студент групи ТРм-19-1 Жалюк Андрій Іванович

Керівник роботи

к.в.н, доцент Лужанський Віктор Ігорович

Актуальність теми:

- Бездротові сенсорні мережі, як правило, використовуються в різних сферах застосування, включаючи промислові, військові та цивільні. Це призводить до популяризації досліджень маси протоколів маршрутизації. В умовах збільшення частки таких протоколів особливої актуальності набуває детальне вивчення основних параметрів оцінки для розробки моделей бездротових сенсорних мереж та засобів їх моделювання. Актуальність роботи обумовлена проблемами в галузі первинного дослідження, а саме енергоспоживання датчиків в бездротовій сенсорній мережі і поліпшення точності даних, сформованих на різноманітних параметрах оцінки.

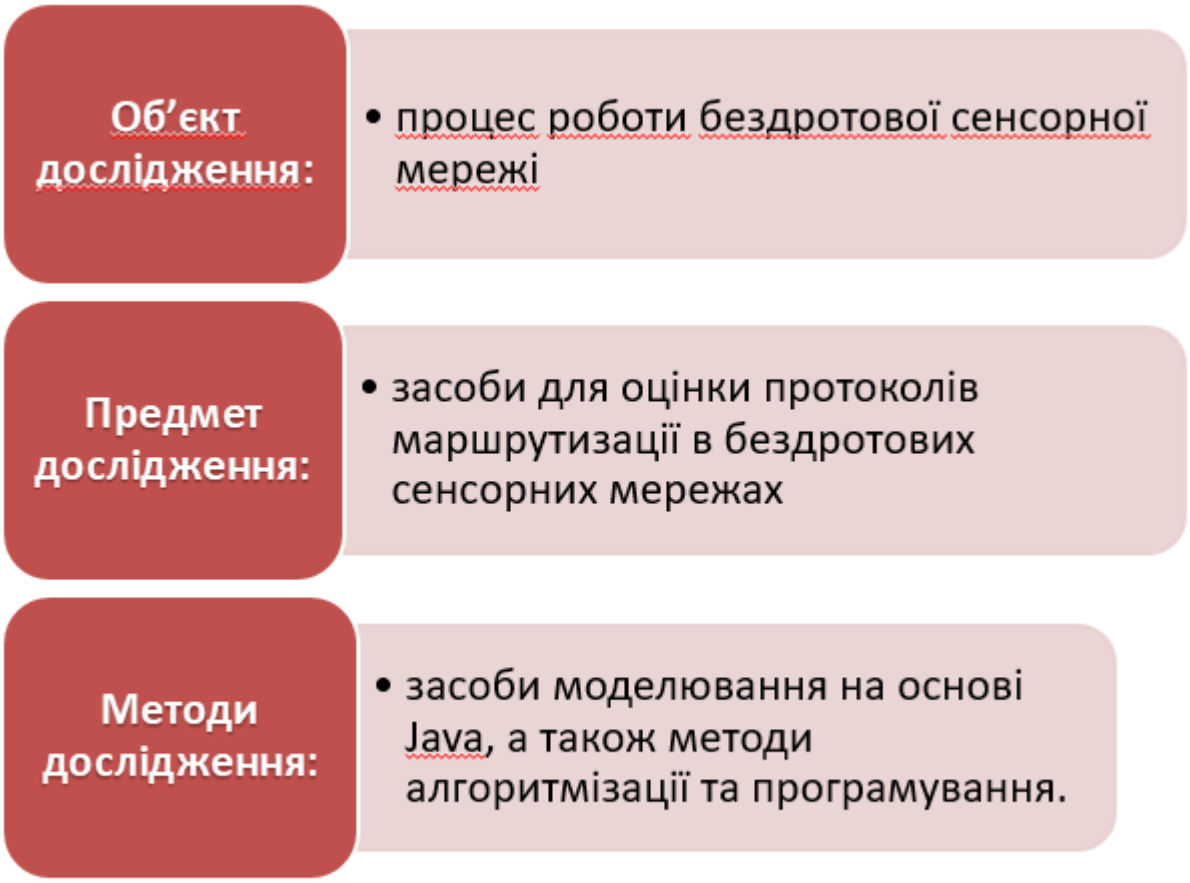
Мета дослідження:

- Детальне вивчення розробки моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах. Висвітлення взаємозв'язку між параметрами оцінки для визначення впливу кожного з них на певний протокол маршрутизації на основі інструменту моделювання J-Sim.

Задачі дослідження:

- 1. Аналіз інструментів моделювання;
- 2. Протоколи маршрутизації;
- 3. Моделі оцінки протоколу Single-hop.
- 4. Моделі оцінки протоколу Leach

3


Об’єкт дослідження:
• процес роботи бездротової сенсорної мережі
Предмет дослідження:
• засоби для оцінки протоколів маршрутизації в бездротових сенсорних мережах
Методи дослідження:
• засоби моделювання на основі Java, а також методи алгоритмізації та програмування.

4

Наукова новизна:

- Проведено розрахунок впливу внутрішньосистемних завад у мережі радіозв'язку під час руху мобільної станції у межах стільника при різних технічних характеристиках базових станцій.
- Отримали подальший розвиток методика «моніторинг завадової обстановки» у стільникових системах, яка дозволила визначати важливі параметри системи на етапі проектування мобільної мережі.
- Проведено розрахунок впливу внутрішньосистемних завад у мережі мобільного зв'язку при різних технічних характеристиках базових станцій. Це дозволило підвищити ефективність мережі мобільного зв'язку на 5,6% в умовах дії внутрішньосистемних завад.

Практичне значення:

- Проведено аналіз впливу внутрішньо системних завад на вході приймача мобільної станції при її русі за заданим маршрутом.
- Використана методика дозволяє здійснювати моніторинг реальної завадової обстановки та оцінювати якість зв'язку. Це дозволить виявити проблемні зони впевненого прийому сигналів, а також оперативно вирішувати питання щодо покращення роботи такої мережі.
- Сформульовані науково – обгрунтовані практичні рекомендації щодо раціонального використання стільникових мереж мобільного радіозв'язку з урахуванням переміщення мобільних станцій в умовах дії внутрішньосистемних завад.

5

1 Аналіз інструментів моделювання

1.1. Бездротові сенсорні мережі

Бездротова сенсорна мережа складається з просторово розподілених автономних датчиків для спільного моніторингу фізичних або екологічних умов, таких як температура, звук, тиск, рух. Наступний рисунок ілюструє типову модель передачі даних такої мережі.

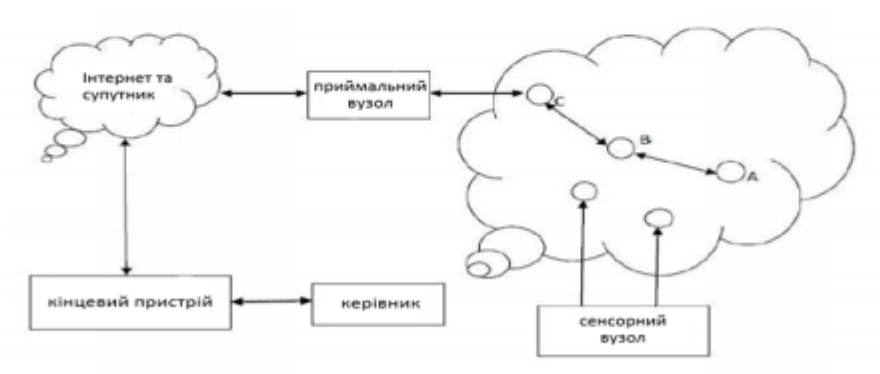


Рисунок 1– Модель передачі даних бездротової сенсорної мережі

6

1.2. Інструменти моделювання бездротової сенсорної мережі

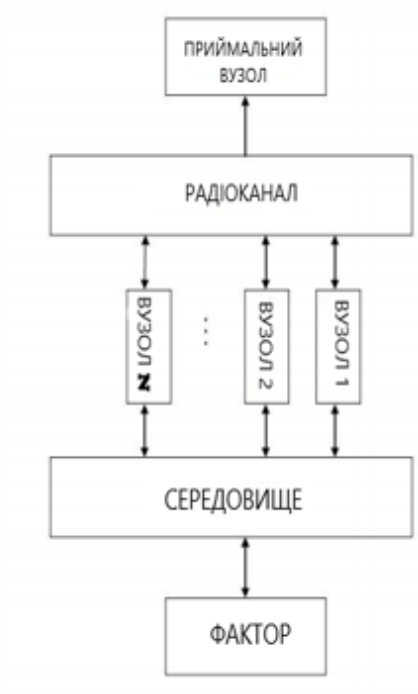


Рисунок 2 – Принцип моделювання

Детальний опис компонентів на цьому рисунку:

а) Вузли: Вузли є базовими пристроями в цій моделі. Кожен вузол може зв'язуватись між собою через радіоканал. Існує також стек протоколів для управління цими комунікаціями.

б) Навколишнє середовище: Компонент навколишнього середовища моделює генерації та розповсюдження подій, які сприймаються вузлами датчика, і можуть призвести до інших дій датчика.

в) Радіоканал: Цей компонент характеризує поширення радіосигналів між вузлами в мережі.

г) Приймальні вузли: Приймальні вузли отримуватимуть дані із загальних сенсорних датчиків.

д) Фактори: Фактори відіграють роль генератора подій, що представляє запит для вузлів.

7

2. Моделі оцінки протоколу Single-hop

2.1. Надійність та термін служби моделей протоколу

1. Модель протоколу із фіксованим радіусом

Взаємозв'язок між кількістю датчиків і надійністю для фіксованого 15-метрового радіуса передачі проілюстровано у формулі:

$$100.014 – 0.0126857142857145n, \quad (1)$$

де n являє собою кількість датчиків. Значення 100 слід вживати, коли $n = 1$, тоді як рівняння 100,001343 вказує на те, що ця лінійна модель добре підходить для реальності. З іншого боку, надійність дорівнює 0 за цією моделлю, коли $n = 7884$. Термін служби мережі повинен моделюватися за формулою:

$$K/16/6\alpha, \quad (2)$$

де α – це константа. Тому $e = 16.6\alpha$ чи дорівнює $K = 258960\alpha$.

2. Модель протоколу із змінним радіусом

Оскільки радіус передачі змінюється, очікувана кількість датчиків в межах діапазону буде задаватися формулою:

$$20\pi r^2/100, \tag{3}$$

при чому 0 ≤ r ≤ 5.

Ця формула надає відповіді 0,62831853, 2,513274123, 5,654866776, 10,05309649 та 15,70796327 для r = 1, 2, 3, 4 та 5 метрів відповідно, і очевидно, що відповідь 20 при r≥5√2 метрів. При 5 < r < 5√2 деяка елементарна геометрія показує нам, що площа всередині квадрата, але поза колом, центром якого є приймальний вузол, визначається за формулою:

$$A = 2(5 - \sqrt{r^2 - 25})^2 + (50 - r^2) - 4(\tfrac{\pi}{4} - 0)r^2, \tag{4}$$

де $\theta = \tan^{-1}(\sqrt{r^2 - 25}/5)$. Таким чином, очікувана кількість датчиків у цьому випадку становить 20 – A/5, що означає 19,016 при r = 6 метрів.

9

Отримані дані усереднювали для постійних значень *s* для різних значень *r*, а потім за допомогою методу найменших квадратів загальна кількість переданих пакетів даних була приблизно

$$206230.002000859 - 9193.8288407016s.$$

при $0 \le r \le 5$. Також, використовуючи той самий метод, кількість пакетів даних, отриманих приймальним вузлом, становить приблизно

$$436.736796908544 + 1280.42582653499s$$

при $0 \le r \le 5$. Таким чином, в середньому надійність для 20 датчиків та $0 \le r \le 5$, може бути наближена наступною формулою:

$$\frac{436.736796908544 + 1280.42582653499\frac{\pi r^2}{5}}{206230.002000859 - 9193.8288407016\frac{\pi r^2}{5}}. \quad (5)$$

Ця формула загалом надмірно оцінює показники надійності, отримані в результаті проведених експериментів, але має правильну загальну форму. Графік функції, представленої наведеною вище формулою зображений червоною кривою на рисунку 3.

10

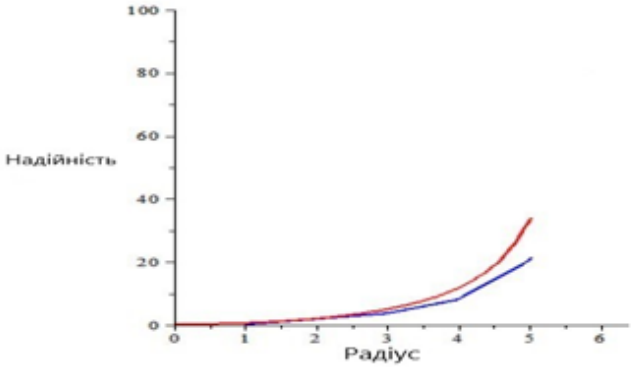


Рисунок 3 – Модель надійності

Тепер, якщо кількість датчиків зафіксовано на рівні 20 і $r \geq 5\sqrt{2}$ метрів, то основний показник надійності з лінійного рівняння становить 99,76%. Найкраща формула, яка може бути запропонована для $5 < r < 5\sqrt{2}$ полягає в тому, що надійність задається формулою:

$$\left(1 - \frac{A}{100}\right) \times (0.9976), \quad (6)$$

де *A* - площа, виявлена вище.

11

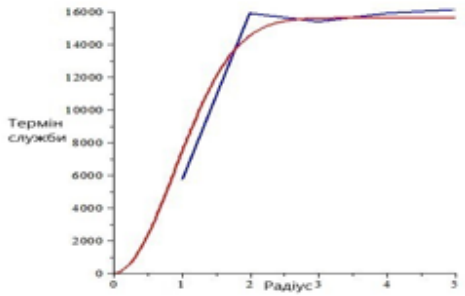


Рисунок 4 – Модель терміну служби

Швидкість передачі в рази, витрачена енергія на пакет даних, дає енергію, спожиту в секунду; ділення *K* (значення загальний час автономної роботи) на *e* формує термін служби).

Імовірність, *p*, що відсутні датчики в діапазоні передачі, задається значенням:

$$(1-\frac{E(s)}{20})^{20}, \quad (7)$$

де $E(s)$ очікувана кількість датчиків у діапазоні передачі, розрахована вище. Отже, очікуваний термін служби задається формулою: 15600(1-*p*) Ця формула дає значення (майже точно) 15600 при r≥3 і задається формулою:

$$15600\left(1-\left(1-\frac{\pi r^2}{100}\right)^{20}\right), \quad (8)$$

при $0 \le r < 3$. Зокрема, ця формула дає 7361 та 14537 при при $r = 1$ та 2 метри відповідно. Графік функції, представленої наведеною вище формулою зображений червоної кривою на рисунку 3.

12

3. Моделі оцінки протоколу Leach

У міру збільшення кількості вузлів датчиків у фіксованому просторі, більше датчиків може бути обрано головками кластера, і таким чином можна зберегти енергію для кожного датчика. Термін служби мережі повинен збільшуватися із збільшенням кількості датчиків. Рисунок 5 підтверджує, що термін служби мережі збільшується із збільшенням щільності. Іншими словами, взаємозв'язок між щільністю та терміном служби мережі є позитивною кореляцією.

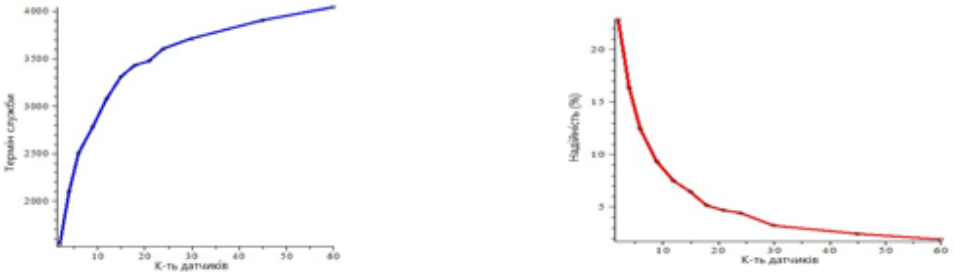


Рисунок 5 – а) Взаємозв’язок кількості датчиків та терміну служби б) Взаємозв’язок кількості датчиків та надійності.

Тривалість служби для цього експерименту на рисунку 5(а) збільшується з 1541 до 2097, 2503, 2779, 3077, 3307, 3427, 3475, 3601, 3707, 3903 і, нарешті, до 4043. На рисунку 5 а) показано взаємозв'язок між надійністю і кількість датчиків. Надійність для цього експерименту знизилася з 22,86% до 16,35%, 12,44%, 9,31%, 7,46%, 6,45%, 5,13%, 4,67%, 4,38%, 3,23%, 2,40% і, нарешті, до 1,89%.

Таким чином, взаємозв'язок між кількістю датчиків та надійністю пов'язаний з негативною кореляцією. Це можна пояснити наступним чином: зі збільшенням щільності головки кластера будуть споживати набагато більше енергії для зв'язку з вузлами датчиків.

Тоді енергія, що залишилася для кожної головки скупчення, буде швидко зменшуватися зі збільшенням щільності. Крім того, передача даних на приймальний вузол споживає багато енергії, і тоді все більше і більше обраних головок кластера не можуть передавати дані на приймальний вузол.

13

Щільність – термін служби – надійність

Таблиця 1 – Кількість датчиків, надійність, термін служби для протоколу ближнього зв'язку

К-ть датчиків	Надійність %	Термін служби
10	89.08	702
20	92.53	581
30	93.21	530
40	93.64	438
50	93.81	341
60	90.63	324
70	89.72	282
80	90.03	280
90	89.78	277
100	89.05	274
110	88.08	258
120	89.86	230
130	88.83	228
140	88.67	244
150	88.61	239
160	88.28	234
170	88.07	224
180	87.97	227
190	87.31	232
200	86.31	233
210	84.99	228
220	83.91	223
230	83.51	226
240	83.24	249
250	83.02	248
260	81.46	246
270	79.04	251
280	77.15	250
290	76.84	240
300	75.89	249.

Була проведена серія експериментів з кількістю датчиків, починаючи з 10, і збільшуючи з кроком від 10 до 300 датчиків.

Радіус передачі для кожного датчика був встановлений на рівні 15 метрів, оскільки він є достатньо великим для передачі даних в будь-яку точку площі. Надійність та термін служби для цього експерименту представлені в таблиці 1

14

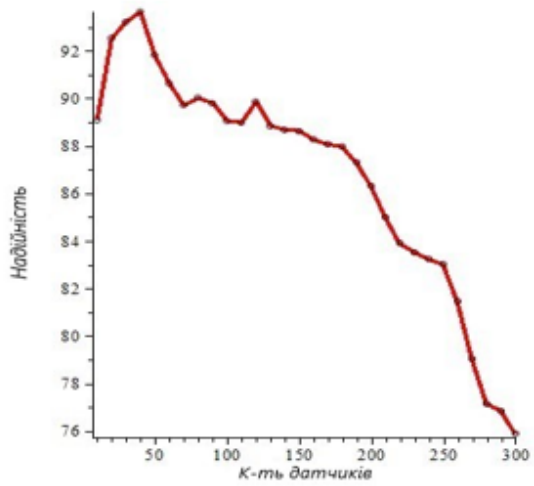


Рисунок 6 – Взаємозв’язок надійності та щільності для протоколу ближнього зв’язку

На рисунку 6 взаємозв'язок між кількістю датчиків та надійністю дуже чіткий. Надійність для цієї програми зросла, коли кількість датчиків зросла до 40, коли вона досягла найвищого значення. Потім воно суттєво зменшилось, оскільки кількість датчиків зросла з 40 до 300, коли досягло найнижчого значення. Це можна пояснити зауваженням, що зі збільшенням щільності вузлів все більше датчиків приєднується до процесу передачі даних і, зв'язок між датчиками стає все більш і більш складнішим. Втрачені дані через зіткнення та затримку даних не можна ігнорувати. Після того надійність зменшується із щільністю.

15

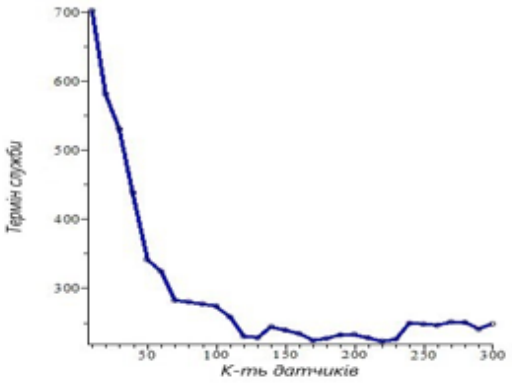


Рисунок 7 – Взаємозв’язок терміну служби та щільності для протоколу ближнього зв’язку

На рисунку 7 термін служби досяг найнижчого значення, коли кількість датчиків дорівнювало 220, тоді як найвище значення терміну служби було, коли було 10 датчиків.

16

У протоколі ближнього зв’язку, відправка пакету на приймальний вузол вимагатиме від кожного датчика передачі своїх даних по шляхах передачі до найближчих датчиків до приймального вузла. Ці найближчі датчики (лише близько двох або трьох) будуть приймати всі дані в мережі і передавати їх у приймальний вузол, використовуючи велику кількість енергії.

Таким чином, мережа ближнього зв’язку, як правило, досить швидко відділяється від приймального вузлу. Якби мережа LEACH з двома або трьома кластерами працювала з фіксованими головками кластера, то можна було б очікувати, що її термін служби буде дуже коротким, оскільки кожна головка кластера повинна збирати та передавати всі дані в мережі (як мережа ближнього зв’язку на початку).

Однак найважливішою особливістю LEACH є те, що кластерні головки обертаються між датчиками, що дозволяє рівномірно розподілити цей енергетичний тягар між датчиками, що призводить до набагато більш тривалого терміну служби.

На рисунку 6 коли кількість датчиків дорівнює 40, надійність становила 93,64%, що є найвищим рівнем, але з цим числом термін служби досить короткий. Це ілюструє, що користувачі можуть вибрати оптимальне значення щільності для цього додатка залежно від необхідної надійності та терміну служби.

– Взаємозв’язок терміну служби та щільності для протоколу ближнього зв’язку

17

1. Радіус – термін служби – надійність

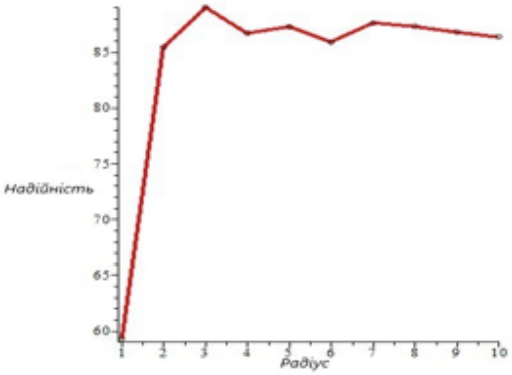


Рисунок 8 – Взаємозв'язок радіусу та надійності для протоколу ближнього зв'язку

На рисунку 8 показано взаємозв'язок між надійністю та радіусом передачі. Необхідно, щоб усі вузли датчиків застосовували найближчу техніку ближчого передавання для доставки повідомлень. Коли радіус дорівнює одному метру, надійність є найнижчою; однак, якщо радіус перевищує один метр, величина надійності залишається відносно стабільною і коливається менше ніж на 10%. Причину цього можна пояснити наступним чином:

- Для з'єднання радіусом в один метр багато даних буде втрачено в процесі передачі, а отже, надійність у системі негативно позначається. З іншого боку, із збільшенням радіуса відбуватиметься більше зіткнень даних, так що це впливатиме і на надійність.
- Значення надійності коливається в межах від 85 до 90% для радіуса, більшого або рівного двом метрам.

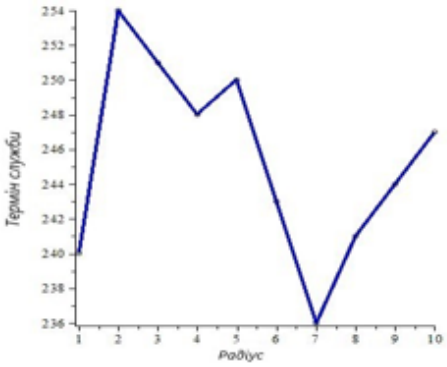


Рисунок 9 – Взаємозв’язок радіусу та терміну служби для протоколу ближнього зв’язку

На рисунку 9 показано взаємозв'язок між терміном служби та радіусом передачі. На цьому показнику немає чіткої тенденції, оскільки термін служби коливається лише від 236 до 254, і його можна вважати постійним для будь-якого радіуса від 1 до 10 метрів. Якщо кількість датчиків налаштовано на 20, результати будуть такими:

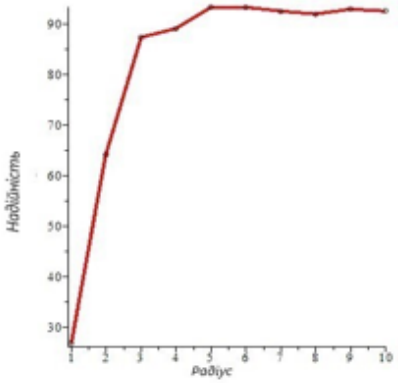


Рисунок 10 – Взаємозв’язок радіусу та надійності для протоколу ближнього зв’язку (20 датчиків)

На рисунку 10 показано взаємозв'язок між надійністю та радіусом передачі. Надійність для цієї програми зросла, оскільки радіус передачі збільшився з 1 до 5 метрів. Надійність досягла 93,28%, коли радіус становив 5 метрів. Коли радіус збільшився з 5 до 10 метрів, значення надійності дещо коливалось, оскільки радіус досить великий, щоб передавати дані для цього найближчого ближчого протоколу на приймальний вузол.

19

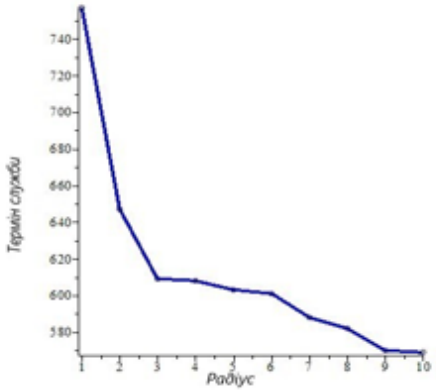


Рисунок 11– Взаємозв’язок радіусу та терміну служби для протоколу ближнього зв’язку (20 датчиків)

На рисунку 11 показано взаємозв'язок між терміном та радіусом передачі. Коли радіус збільшувався з 1 до 10 метрів з кроком в один метр, термін служби зменшився з 757 до 569. Причина цього падіння могла бути пов’язана з тим, що зі збільшенням радіуса зв'язок між датчиками ускладнювався, отже, набагато було витрачено більше енергії, що призвело до зменшення терміну служби.

20

ВИСНОВКИ

1. Проаналізовано та досліджено описи бездротових сенсорних мереж, а також надано деякі подробиці про J-Sim. Крім того, зроблено огляд роботи над параметрами оцінки WSN. Опрацьовано роботи дослідників, які виконали певні моделювання та отримали корисні результати із відповідними параметрами оцінки. Однак виходячи з їх досліджень не створено ані математичні моделі для відповідних параметрів, ані підходи для компромісу. Таким чином, інструменти моделювання не будуть необхідні для розгортання датчиків, що призводить до економії грошей і часу.

2. Розглянуто три різні категорії протоколів маршрутизації, для кожної категорії було розглянуто та описано ряд прикладів. Описано підмножину протоколів маршрутизації для аналізу, таких протоколів маршрутизації як: Single-hop, LEACH та Nerely Closer, які приймаються як представники плоских, ієрархічних та протоколів маршрутизації, які базуються на розташуванні відповідно.

3. Після аналізу найпростішого Single-hop протоколу запропоновано дві моделі оцінки серед параметрів терміну служби, надійності та щільності. На основі цих інтелектуальних моделей оцінки користувачі бездротової мережі датчиків можуть безпосередньо передбачити термін служби та надійність. Це означає, що вузли датчиків можуть бути розгорнуті в такій мережі без подальшого моделювання.

21

4. Проведена серія експериментів із інструментом моделювання J-Sim на основі протоколу LEACH. В результаті було виявлено, що:
термін служби мережі збільшується із збільшенням кількості датчиків;
існує лінійна залежність між кількістю пакетів даних, отриманих приймальним вузлом та терміном служби; кількість кластерів впливає на зіткнення даних та енергію, а отже, на надійність та термін служби мережі.

Також виходячи із серії експериментів, проведених в інструменті моделювання J-Sim, для протоколу ближнього зв'язку випливає, що надійність, термін служби та радіус напряму залежать від кількості датчиків.

Mon Dec 07 11:46:46 EET 2020, Федула Микола Васильович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

ID: 82701 Назва: Розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах Додано в БД: 2020-12-07 Автора: А. І. Жалюк Керівники: В. І. Лужанський Консультанти: Опоненти: Ю. М. Бойко	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	111921	863	1188 (1%)	15 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK

Ім'я користувача:
Кафедра АКІТІТК

ID перевірки:
1005387168

Дата перевірки:
07.12.2020 12:53:42 EET

Тип перевірки:
Doc vs Internet

Дата звіту:
07.12.2020 12:54:24 EET

ID користувача:
100005862

Назва документа: На_ПЛАГІАТ_Zhalyuk_diplom

Кількість сторінок: 92 Кількість слів: 17317 Кількість символів: 128014 Розмір файлу: 1.73 MB ID файлу: 1005679229

6.77%
Схожість

Найбільша схожість: 1.52% з Інтернет-джерелом (https://link.springer.com/chapter/10.1007/978-981-10-0412-4_6)

6.77% Джерела з Інтернету 306 Сторінка 94

Пошук збігів з Бібліотекою не проводився

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Заміжені символи 4

РЕЦЕНЗІЯ

на дипломну роботу

«Розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах»

студента групи ТРм-19-1 Жалюка Андрія Івановича

Дипломна робота та її зміст повністю відповідають завданню. Сформульовані мета, об'єкт та предмет дослідження свідчать про актуальність теми – розробка моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах.

Дипломна робота виконана відповідно до перспективних планів наукової роботи, кафедри автоматизації, комп'ютерно-інтегрованих технологій і телекомунікацій університету з тематики подальшого розвитку безпровідних сенсорних мереж та засобів їх моделювання.

Метою роботи є детальне вивчення розробки моделей та засобів для оцінки протоколів маршрутизації в бездротових сенсорних мережах. Висвітлення взаємозв'язку між параметрами оцінки для визначення впливу кожного з них на певний протокол маршрутизації на основі інструменту моделювання J-Sim.

Практичне значення одержаних результатів полягає у тому, що застосування такої системи дозволяє підвищити ефективність використання бездротових сенсорних мереж у ще більшій кількості галузей, окрім тих, що зазначені в даній магістерській роботі.

Результати дипломної роботи можуть бути використані для розробки системних методів оцінки протоколів маршрутизації в бездротових сенсорних мережах у реальному масштабі часу на основі використання ряду параметрів. В цілому зміст роботи відповідає темі, вся інформація подана у роботі є достовірною. До недоліків роботи можна віднести деякі стилістичні помилки, які суттєво не впливають на її наукову-технічну цінність.

Робота викладена науковою мовою, логічно й послідовно. Пояснювальна записка відповідає стандартам до її оформлення.

Робота Жалюка Андрія Івановича відповідає вимогам, які висуваються до дипломної роботи і може бути оцінена на оцінку «Відмінно».

Рецензент:
доктор технічних наук, професор **Бойко Ю.М.**

"9" 12 2020 р.

Завідувачу кафедри
проф. Мартинюку В. В.

здобувача вищої освіти (студента ПІБ, факультет, «курс», «група»)
Жалка А. І. ФІКТС, другий курс магістратури, ТРН-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

05.12.2020р
дата

підпис

РІШЕННЯ КАФЕДРИ

АВТОМАТИЗАЦІЇ, КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ ТА ТЕЛЕКОМУНІКАЦІЇ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Підвищення ефективності стільникових систем радіозв'язку з рухомими об'єктами в умовах дії внутрішньосистемних завад.

Автор: **Жалюк Андрій Іванович**

Спеціальність: **172 Телекомунікації та радіотехніка**

Освітня програма: Телекомунікації та радіотехніка

Науковий керівник: **д.т.н, проф. Лужанський Віктор Ігорович**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 6.77%, виявлені в роботі відповідають тексту стандартних бланків та списку літератури, решта запозичень є випадковими, або на них є посилання, тому ці запозичення не є плагіатом, бо вони не стосуються наукової новизни і практичної значущості роботи.

3.12.2020р.

Науковий керівник роботи: Лужанський В.І.

Зав. каф. АКІТіТК Мартинюк В.В.