Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу
Назва теми

КРКБ 190121.19.01.01 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Шифр, назва

Виконав студент 4 курсу, група КБ-19-1 _____ Веремійчук В.Є.
Підпис Ініціали, прізвище

Керівник _____ Чешун В.М.
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ 15.06.23 Мостовий С.В.
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Кльоц Ю.П.
Підпис, дата Ініціали, прізвище

15 06 2023 р.

Хмельницький, 2023

Формат	Зона	Позиц	Позначення	Найменування	Кільк.листів	Прим.
А4		1	КРКБ 190121.19.01.01 ПЗ	Бездротова сенсорна мережа	72	
				військового призначення із		
				захистом від несанкціонованого		
				доступу та впливу		
				Пояснювальна записка		
А2		2	КРКБ 190121.19.01.01 Е8	Бездротова сенсорна мережа	1	
				військового призначення із		
				захистом від несанкціонованого		
				доступу та впливу		
				Схема додавання нового		
				вузла до мережі		
А2		3	КРКБ 190121.19.01.01 Е8	Бездротова сенсорна мережа	1	
				військового призначення із		
				захистом від несанкціонованого		
				доступу та впливу		
				Схема реакції мережі на		
				аномальну поведінку вузлів		
А2		4	КРКБ 190121.19.01.01 Е8	Бездротова сенсорна мережа	1	
				військового призначення із		
				захистом від несанкціонованого		
				доступу та впливу		
				Демонстрація роботи		
				механізму ізоляції вузлів		

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ 190121.19.01.01 ВП			
Розробив		Веремійчук В.С		7.06.23	Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу Відомість проєкту	Літера	Аркуш	Аркушів
Перев.		Чешун В.М.				н	1	2
Н. контр.		Мостовий С.В.		15.06.23		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		15.06.23				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Освітня програма Освітньо-професійна програма підготовки бакалаврів

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"01" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Веремійчук

В.С

Прізвище, ім'я, по батькові студента

1. Тема роботи Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу

Керівник роботи Чешун В.М.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023 р. №5 додаток №11

2. Строк подання студентом роботи на кафедру

3. Вихідні дані до проекту (роботи) створити програмну модель бездротової сенсорної мережі. Провести класифікацію мережі, що розробляється. Вибрати середовище розробки. Дослідити алгоритми та протоколи які використовуються в бездротових сенсорних мережах. Враховуючи особливості мережі, що розробляється, обрати протоколи та алгоритми для реалізації моделі мережі. Розробити програмну модель алгоритмів та протоколів і інтегрувати в єдину модель мережі. Дослідити алгоритми, методи та протоколи захисту безпровідних сенсорних мереж. Дослідити вразливості мережі. Визначити вразливості мережі, що розробляється. На основі аналізу вразливостей системи імплементувати алгоритми та протоколи захисту в програмну модель мережі. Провести тестування розробленої моделі мережі, механізмів захисту. Провести аналіз роботи мережі на основі даних, отриманих при тестуванні програмної моделі мережі.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз предметної області та постановка задачі. Проектування та реалізація системи. Тестування системи розгортання та захисту бездротової сенсорної мережі. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Схема додавання нового вузла до мережі», «Схема реакції мережі на аномальну поведінку вузлів», «Демонстрація роботи механізму ізоляції вузлів», «Реакція мережі на реалізацію атаки заглушення».

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 01 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір і погодження теми кваліфікаційної роботи	Січень	–
2	Пошук теоретичної інформації про безпровідні сенсорні мережі	Січень	–
3	Дослідження існуючих рішень	Лютий	–
4	Постановка задачі	Лютий	–
5	Побудова структури мережі	Березень	–
6	Розробка модулів мережі. Інтеграція модулів в єдину програмну модель мережі	Квітень	–
7	Тестування моделі мережі. Аналіз отриманих результатів	Квітень\Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Червень	–

Студент _____ Веремійчук В.Є.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Чешун В. М.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу.

Автор роботи: Веремійчук Віталій Свгенович.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 72 с., 1 додаток, 29 рис., 40 джерел.

Графічна частина: 8 презентаційних слайдів.

БЕЗДРОТОВА СЕНСОРНА МЕРЕЖА, КЛАСТЕРИЗАЦІЯ, ПОШУК МАРШРУТУ, ПЕРЕДАЧА ДАНИХ, ЗАХИСТ МЕРЕЖІ

Метою роботи є розробка моделі бездротової сенсорної мережі військового призначення з захистом від несанкціонованого доступу та впливу, що дозволить провести дослідження цієї мережі з метою розробити нову захищену систему моніторингу та збору даних, яка може бути ефективною для вирішення специфічних завдань в умовах високого рівня загрози нападу на мережу.

У роботі було досліджено і проаналізовано предметну область, протоколи та алгоритми роботи, протоколи та механізми захисту які використовуються в безпровідних сенсорних мережах, вразливості таких мереж, атаки та засоби протидії атакам на мережі такого типу. Створено модель безпровідної сенсорної мережі з випадковим розгортанням, яка може працювати в складних умовах, а також має вбудовані механізми захисту від зловмисного впливу та атак на систему. Проведено дослідження моделі мережі визначено її особливості, протестовані механізми роботи та захисту мережі. Визначена поведінка мережі у разі виявлення загроз безпеці та цілісності системи.

15.06.2023

ANNOTATION

Theme of the qualification work: Wireless sensor network for military purposes with protection against unauthorized access and influence.

Author of the work: Veremiichuk Vitalii Yevhenovych.

Supervisor: Cheshun Viktor Mykolaiovych.

Explanatory note: 72 p., 1 appendix, 29 figures, 40 sources.

Graphic part: 8 presentation slides.

WIRELESS SENSOR NETWORK, CLUSTERING, ROUTE FINDING, DATA COMMUNICATION, NETWORK SECURITY

The aim of the work is to develop a model of a wireless sensor network for military purposes with protection against unauthorized access and influence, which will allow to study this network in order to develop a new secure monitoring and data collection system that can be effective for solving specific problems in conditions of a high level of threat of attack on the network.

In this work, the subject area, protocols and algorithms, protocols and protection mechanisms used in wireless sensor networks, vulnerabilities of such networks, attacks and means of counteracting attacks on networks of this type were investigated and analyzed. A model of a wireless sensor network with random deployment is created, which can operate in difficult conditions and has built-in mechanisms to protect against malicious influence and attacks on the system. The network model is studied, its features are determined, and the mechanisms of network operation and protection are tested. The behavior of the network in case of detection of threats to the security and integrity of the system is determined.

15.06.2023

ЗМІСТ

ВСТУП

На фоні поточної ситуації в країні, а саме війни з росією, дуже актуальними стали галузі, які займаються розробкою та виробленням військової продукції, від простої, такої як сухпайків, стрілецької зброї тощо, до більш складної, наприклад, як стрілецькі, артилерійські, зенітні вогневі системи, системи РЕБ (радіоелектронної боротьби), системи керування БпЛА (безпілотними літальними апаратами) або дронами, та багато інших, які в умовах сучасних бойових конфліктів почали обладнувати електронним обладнанням та системами, що дозволяють підвищити ефективність роботи особового складу, зменшити ризики, покращити безпеку та ефективність зброї, захисних, розвідувальних, сигналізаційних систем.

Роль цих електронних систем може бути різна – від тих які збирають, обробляють та виводять дані оператору або корегують стрільбу, до тих, які можуть бути повністю або майже повністю автоматизовані і приймати рішення самостійно без втручання оператора.

Якщо розглянути статистику поранень від куль та осколків в війнах XX-XXI сторіччя то можемо прослідкувати що частота поранень від осколків як правило становить більш ніж 60%, а в окремих битвах може становити більше 90%. Це говорить про те, що провідну роль в сучасних війнах відіграють артилерія, авіація, флот, тобто важке озброєння, і чим воно потужніше, тим більш складні електронні системи, як правило, містить. Натомість, роль людини у таких конфліктах все більше схиляється до підтримки такої техніки, обслуговування та прийняття рішення.

Це означає актуальність електронних систем буде збільшуватися, все більше й більше засобів будуть модернізуватися, обладнуватися новими системами керування, стеження, наведення, інформування тощо.

Одним з перспективних напрямків розробки у даній сфері є БСМ (безпровідні сенсорні мережі). БСМ – це тип спеціальної мережевої технології,

яка виникла понад 20 років тому для моніторингу у військових програмах. БСМ, як правило, включають велику кількість сенсорних вузлів, обмежених в ресурсах, але які мають можливість з’єднуватися з іншими вузлами мережі для передачі отриманих даних. Головним завданням кожного вузла є моніторинг навколишнього середовища за допомогою датчиків, також вони можуть збирати отримані дані, діяти як ретранслятор або як голова кластера. Кожен вузол можна використовувати як маршрутизатор для пересилання даних від сусідів до приймача або базової станції (БС). БС може обробляти дані локально або діяти як шлюз мережі для передачі даних на віддалені сервери [1].

Завдяки динамічній інфраструктурі та ефективній передачі даних у мережах БСМ області їх застосування досить різноманітні. Протягом останніх двох десятиліть для БСМ були запропоновані різні програми, такі як моніторинг навколишнього середовища, охорона здоров'я, розумні будинки, розумні фабрики та управління стихійними лихами. Хоча БСМ вважаються високодинамічними спеціальними мережами, управління топологією мережі було фундаментальною проблемою в цих типах мереж, зокрема управління ресурсами, масштабованість, надійність та ефективність [2].

БСМ можуть використовуватися не тільки в військовій сфері, а й в інших сферах діяльності, але в кваліфікаційній роботі змодельовано конкретну модель мережі – це безпровідна мережа з випадковим розгортанням (Randomly Deployed Wireless Sensor Network), першочерговим призначенням якої є збір інформації та її передача на приймач, для чого потрібно реалізувати алгоритми передачі, збору даних, алгоритми захисту від несанкціонованого втручання та впливу на роботу мережі [3].

В кваліфікаційній роботі виконано такі етапи проєктних робіт:

– розглянуті моделі датчиків, які можуть бути використані для побудови обраної мережі, їхні технічні дані;

– розглянуто алгоритми передачі даних в мережі, здійснено порівняльний аналіз та проведена оцінка для обґрунтування вибору оптимального;

– здійснено розрахунки параметрів мережі;

– визначено топологію БСМ, її організаційні та функціональні особливості;

– розглянуто та змодельовано основні типи атак на БСМ.

– розглянуто існуючі та запропонувати нові способи захисту від атак на БСМ.

В кінцевому результаті розроблена модель БСМ, що реалізує обрані алгоритми передачі, збору даних і захисту від зловмисного впливу та втручання в роботу мережі шляхом імплементації обраних на основі дослідження протоколів та механізмів автентифікації, безпеки та шифрування в систему що проєктується.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд та аналіз існуючих рішень

Кваліфікаційна робота з розробки бездротової сенсорної мережі військового призначення із захистом від несанкціонованого доступу та впливу окреслює широкий ряд питань, серед яких варто розглянути такі:

– розгортання БСМ (безпровідних сенсорних мереж);

– алгоритми кластеризації, покриття БСМ;

– алгоритми маршрутизації;

– алгоритми передачі даних в БСМ, конфігурування БСМ.

Розгортання БСМ передбачає розгортання сенсорних вузлів і є критично важливим етапом, який суттєво впливає на функціонування та продуктивність мережі [4]. Часто датчики, що складають мережу, не можуть бути точно позиціоновані і тому розкидані хаотично. Для компенсації випадкового характеру їх розміщення, зазвичай, розгортається велика кількість датчиків, що також сприяє підвищенню відмовостійкості мережі. Стратегія розгортання та позиціонування сенсорних вузлів у БСМ використовується при визначенні кількості і розташування сенсорних вузлів та при визначенні топології мережі. Від топології мережі також залежить моніторинг, зв'язок та енергоспоживання мережі. Задача оптимального розміщення вузлів є NP-складною для більшості випадків розгортання.

Розгортання може бути:

– стаціонарним або мобільним;

– одноцільовим або багатоцільовим;

– детермінованим або стохастичним;

– статичним (випадковим або контрольованим) або динамічним.

Випадкове розгортання є результатом практичної реалізації розгортання датчиків на полях бою або в складних умовах, наприклад, датчики можуть бути скинуті з повітря або запущені за допомогою артилерії.

Діяльність з розгортання можна можна згрупувати у три основні етапи. Етап підготовки до розгортання та розгортання, яка стосується ручного розміщення вузлів вручну людиною або роботом, або запуск їх з літака (вертольота або дрона). Етап після розгортання є необхідним, якщо топологія мережі змінилася внаслідок переміщення вузлів або зміни умов поширення радіосигналу. Третя фаза – перерозгортання, яка полягає в додаванні нових вузлів до мережі для заміни деяких зламаних або пошкоджених вузлів. В статті [5] представлене дослідження методів розгортання в безпровідних сенсорних мережах, покриття та підключення, в якому автори привели класифікацію для методів покриття БСМ (рис. 1.1).

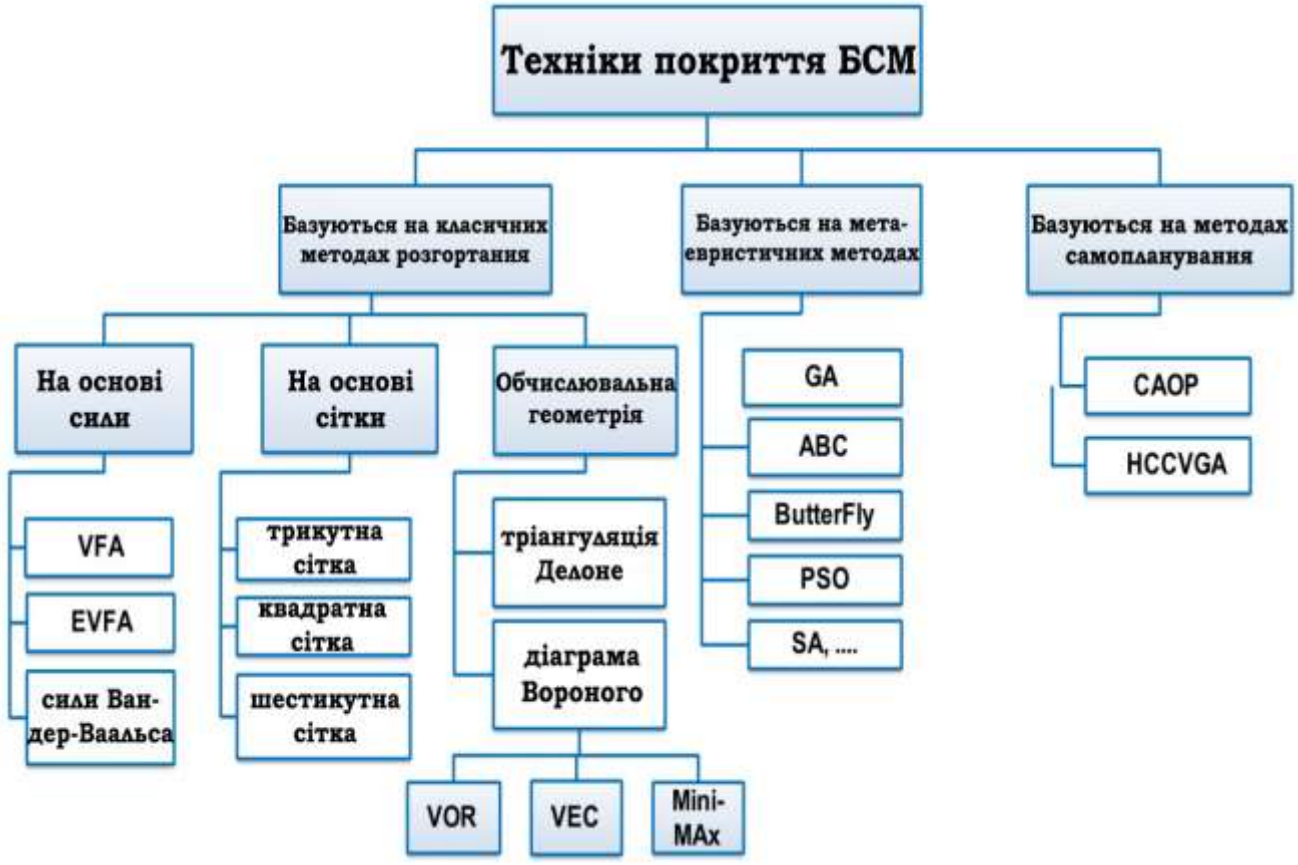


Рисунок 1.1 – Ілюстративна блок-схема таксономії методів покриття у БСМ

Наступне актуальне питання – алгоритми кластеризації [6]. Кластеризація є одним із найпопулярніших методів управління топологією БСМ [7]. Управління топологією використовується для забезпечення ефективної,

надійної та стабільної мережевої інфраструктури в мережах. Кластеризація розділяє вузли на набір груп, які називаються кластерами, на основі набору певних попередньо визначених критеріїв, таких як балансування мережевого навантаження, підтримка якості обслуговування, оптимізація споживання ресурсів, тощо. Кожен кластер може мати одну і більше головок кластера (CH - Cluster Head), які збирають дані з інших вузлів кластера. CH надсилають отримані дані до базової станції (BS - Base Station). Агрегація даних може виконуватися або на CH або безпосередньо на базовій станції. Варто зазначити, що агрегація даних на CH забезпечує стиснення даних перед передачею на BS, що дозволяє витрачати менше енергії та часу на передачу даних, з іншого боку, такий підхід створює додаткову небезпеку для мережі, а самі вузли потрібно доповнювати агрегаторами даних [8].

Використовуючи методи кластеризації, вузлам з обмеженими ресурсами не потрібно надсилати свої дані безпосередньо на шлюзи (приймач), що може спричинити виснаження енергії, неефективне споживання ресурсів і перешкоди.

В БСМ кластеризація є також способом вирішеніня проблеми оптимізації передачі даних в мережі. Передавати дані в таких мережах можливо і без кластеризації, наприклад так, як це дозволяють робити алгоритми затоплення (flooding). Хоч перевага таких алгоритмів в простоті їх реалізації та надійності, вони потребують великих затрат енергії на передачу. Навіть у випадку контрольованого чи вибіркового затоплення, ефективність роботи залишає бажати кращого. До цього слід додати ще й підвищений ризик перехоплення даних що передаються в мережі або реалізації атаки [9], яка може бути здійснена з використанням перехоплених пакетів. Це може бути атака на отримання доступу, фальсифікація маршрутної інформації [10], передача фейкових пакетів даних чи введення фальшивого вузла в мережу. Таким чином, не дивлячись на свою простоту та надійність, алгоритми затоплення негативно

впливають на безпеку мережі та вимагають високих затрат енергії, що дуже критично для вузлів з автономним живленням.

1.2 Класифікація бездротових сенсорних мереж та ідентифікація класу системи, що проєктується

Перед тим як провести класифікацію мережі, яка буде змодельована, розглянемо терміни за якими подібні мережі класифікують та їх визначення.

1.2.1 Класифікація за передачею сигналу та типом вузлів.

Бездротова мережа – тип комп'ютерної мережі, яка використовує бездротове з'єднання для передачі даних й підключення до мережевих вузлів.

БСМ відносяться до просторово розосереджених мереж датчиків, які фіксують певні фізичні умови навколишнього середовища та передають зібрані дані в центральне розташування. БСМ можуть вимірювати умови навколишнього середовища, такі як температура, шум, рівень забруднення, коливання, вологість і вітер. БСМ може містити від кількох до сотень або тисяч вузлів, де кожен вузол підключений до інших датчиків. Кожен такий вузол зазвичай складається з кількох частин: радіопередавача з внутрішньою антеною або з’єднанням із зовнішньою антеною, мікроконтролера, електронної схеми для взаємодії з датчиками та джерела енергії (як правило, батареї або вбудованої форми збору енергії). Топологія БСМ може варіюватися від простої зіркової топології мережі до розширеної бездротової сітчастої мережі з кількома переходами.

1.2.2 Класифікація за складом вузлів.

Вузли в БСМ можуть відрізнятися компонентами та характеристиками.

Гомогенна БСМ (Homogenous БСМ) – це мережа, у якої всі вузли мають однакові можливості зберігання, обробки, живлення від батареї, зондування і зв'язку (рис. 1.2) [11].

Гетерогенна БСМ (Heterogeneous БСМ) - це мережа, яка складається з сенсорних вузлів з різними можливостями, наприклад, різною обчислювальною потужністю і дальністю зондування. Крім того, зачасту вузли в таких мережах відрізняються ще й ієрархічно (рис. 1.2). Гетерогенні мережі містять від двох і більше типів вузлів. Як правило, це прості сенсорні вузли та базові станції (центри кластерів). У порівнянні з гомогенною БСМ, розгортання і управління топологією в гетерогенній БСМ є більш складним. В той же час, і гомогенна і гетерогенна мережа має свої позитивні і негативні сторони. В статті визначено дві бажані характеристики сенсорної мережі: менша вартість обладнання та рівномірне відведення енергії. В той час як гетерогенні мережі досягають першої характеристики, гомогенні мережі досягають другої. Однак обидві характеристики не можуть бути об'єднані в одній мережі. В кваліфікаційній роботі розглядатиметься гомогенна мережа, через те, що планується випадкове розгортання мережі, яке не може забезпечити ефективну гетерогенну модель роботи.

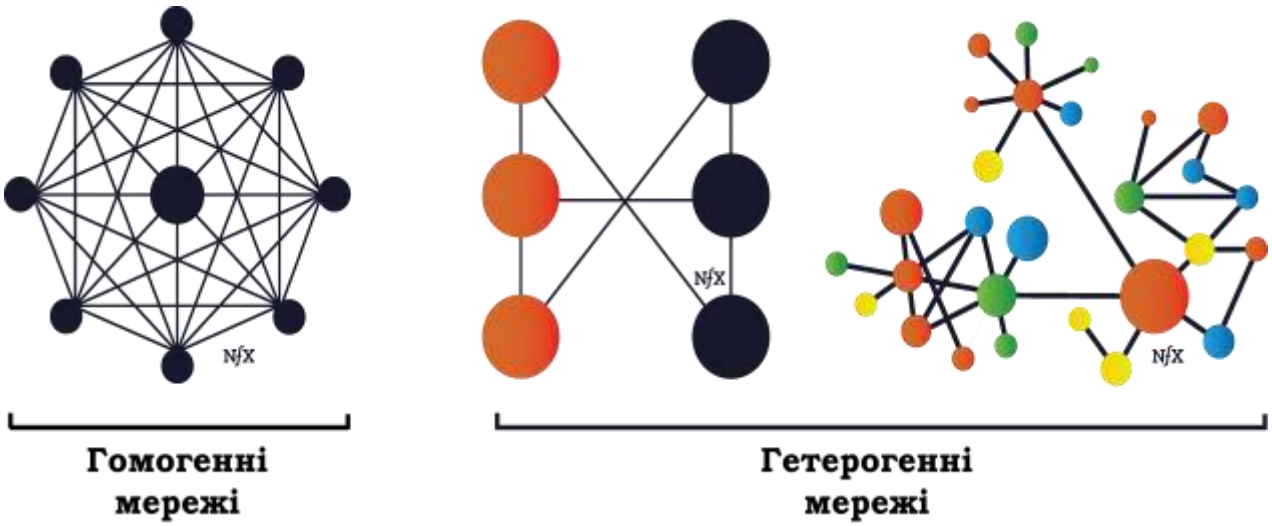


Рисунок 1.2 – Модель топології гомогенних та гетерогенних сенсорних мереж

1.2.3 Класифікація за типом розгортання мережі.

Типи розгортання було визначено в розділі 1.1. Досліджувана мережа класифікується як стаціонарна, багатоцільова, стохастична, статична з

випадковим розгортанням.

1.2.4 Класифікація за вимогами до оперативності передачі показань пристроїв апаратних та програмних датчиків:

– миттєвої передачі – передача показників ініціюється одразу після моменту їх фіксації;

– із низькою латентністю – передача показників відбувається із незначною затримкою у часі, яка складає одиниці або десятки секунд;

– із високою латентністю – передача одиничних показань або груп вибірок відбувається із значною затримкою у часі.

1.2.5 Класифікація за типом організації живлення мережі:

– стаціонарні. В таких мережах живлення всіх вузлів, незалежно від функціонального навантаження, здійснюється віз зовнішньої мережі живлення або від елементів живлення високої ємності;

– напівстаціонарні. Живлення вузлів, які піддаються найбільшому мережевому навантаженню, здійснюється від зовнішньої мережі живлення або від елементів живлення високої ємності, кінцеві вузли мають автономні елементи живлення;

– автономні. Ретранслятори та рядові вузли мережі мають особисті обмежені автономні джерела живлення.

1.2.6 Класифікація за розрахунком строку служби мережі:

– короткострокового функціонування: від кількох годин до кількох днів;

– середньострокового функціювання: до кількох місяців;

– довгострокового функціонування: до кількох років.

Класифікація мереж може бути проведена залежно від різних критеріїв, таких як масштаб, технології зв'язку, топологія, призначення та інші. Для того щоб робити дослідження або висновки, імплементувати алгоритми передачі даних, захисту та безпеки потрібно чітко провести класифікацію такої мережі.

В підсумку, визначено класифікацію досліджуваної мережі (табл. 1.1).

Таблиця 1.1 – Класифікація досліджуваної мережі

Предмет класифікації	Мережа
За передачею сигналу	бездротова
За типом вузлів	сенсорна
За складом вузлів	гомогенна (однорідна)
За типом розгортання мережі	стаціонарна, багатоцільова, стохастична, статична з випадковим розгортанням
За типом організації	самоорганізована
За оперативністю передачі даних	з високою латентністю
За типом живлення	автономна
За сроком служби мережі	середньострокового функціонування
За рівнем відмовостійкості	з високою відмовостійкістю
За здатністю до масштабування	масштабована

1.3 Огляд загроз для проєктованої системи, методів та засобів протидії

БСМ вразливі до різних загроз безпеки через свою розподілену природу, обмежені ресурси та відсутність фізичного захисту. Система, що проєктується, може мати як загальні, так і специфічні вразливості [12], зумовлені особливостями її структури, алгоритмами, що використовуються в БСМ, фізичним обладнанням структурних компонентів мережі. Окреслимо вразливості системи та, як наслідок, типи атак, до яких вразлива проєктована система.

Перелік потенційних вразливостей системи:

– відсутність механізмів автентифікації, або їх низька стійкість дозволяє неавторизованим вузлам приєднуватися до мережі або скомпрометованим вузлам маскуватися під легітимні;

– слабке шифрування може наражати конфіденційні дані, що передаються вузлами БСМ, на ризик перехоплення або несанкціонованого доступу;

– обмежені ресурси - вузли БСМ часто мають обмежену обчислювальну потужність, пам’ять та енергетичні ресурси, це обмеження робить їх уразливими до атак із виснаженням ресурсів і ставить під загрозу їх здатність впроваджувати складні заходи безпеки;

– фізичний вплив на вузли БСМ, розгорнуті в незахищеному середовищі, такі вузли вразливі до фізичних атак, втручання або крадіжки, що потенційно може поставити під загрозу безпеку мережі;

– слабка захищеність каналів зв’язку між вузлами БСМ наражає на ризик перехоплення, підслуховування або несанкціонованого доступу через слабке шифрування;

– вразливості мікропрограми або програмного забезпечення якими можуть скористатися зловмисники, щоб отримати неавторизований доступ або виконати шкідливий код, такі вузли можуть містити мікропрограму або програмне забезпечення з такими вразливими місцями, як переповнення буфера, ін’єкція коду або відсутність перевірки введення;

– відсутність оновлень і виправлень що робить вузли вразливими до нових вразливостей та атак;

– погано сплановане або небезпечне розгортання вузлів БСМ може наражати їх на фізичне втручання, несанкціонований доступ або компрометацію через недостатні фізичні або мережеві заходи безпеки;

– відсутність належних механізмів виявлення вторгнень, без даних механізмів вузли БСМ можуть бути не в змозі виявити або відповісти на зловмисну діяльність або спроби неавторизованого доступу, залишаючи мережу вразливою для атак;

– некоректні методи керування ключами, включаючи слабке створення, розповсюдження та зберігання ключів, можуть послабити загальну безпеку БСМ, роблячи його сприйнятливим до несанкціонованого доступу або маніпулювання даними;

Усунення цих вразливостей вимагає впровадження надійних заходів безпеки, включаючи надійні протоколи автентифікації та шифрування, регулярні оновлення та виправлення, фізичні заходи безпеки, захищені методи керування ключами та механізми виявлення вторгнень, адаптовані до унікальних вимог і обмежень БСМ.

Відповідно, зазначимо перелік основних атак до яких може бути вразливою система:

– глушіння (Jamming) – це атака, під час якої зловмисник заповнює бездротовий канал потужним сигналом, щоб запобігти законному зв'язку між датчиками. Це може спричинити відмову в обслуговуванні (DoS), коли сенсорна мережа не зможе функціонувати;

– спуфінг (Spoofing) або підміна передбачає, що зловмисник видає себе за легітимний датчик у мережі, надсилаючи неправдиву інформацію іншим датчикам. Це може призвести до потрапляння в мережу шкідливих даних, що може призвести до прийняття неправильних рішень на основі неправдивих даних;

– підслуховування (Eavesdropping) – це перехоплення даних, що передаються бездротовим каналом, несанкціонованими суб'єктами. Зловмисники можуть збирати конфіденційну інформацію, таку як паролі, ключі шифрування або інші конфіденційні дані, підслуховуючи бездротове з'єднання;

– несанкціоноване втручання (Tampering) передбачає, що зловмисники змінюють або маніпулюють даними, які передаються датчиками. Це може призвести до отримання мережею невірних або оманливих даних, що може спричинити прийняття мережею неправильних рішень;

– фізичні атаки передбачають фізичне втручання зловмисника в роботу датчиків або мережевої інфраструктури. Це може включати перерізання дротів, пошкодження датчиків або крадіжку датчиків, щоб отримати доступ до даних, які вони збирають;

– атака Сивілли (Sybil Attack) відбувається, коли зловмисник створює кілька фальшивих облікових записів у мережі, щоб отримати контроль над мережею. Це може дозволити зловмиснику впливати на рішення, що приймаються мережею, або навіть отримати контроль над мережею.

Серед даних атак окремо можна виділити такий клас атак, як DoS-атаки. В публікації [13] проаналізовано атаки даного типу направлені на БСМ з зазначенням їх класифікації відносно логічного рівня, на якому проводиться дана атака, по моделі OSI (табл. 1.2).

Таблиця 1.2 – Класифікація DoS-атак на БСМ відповідно до рівнів стеку протоколів OSI

Рівень OSI	DoS атака
Фізичний	Jamming, Interference, Node tampering and destruction
Канальний	Collision, Exhaustion, Unfairness
Мережевий	Sybil, Selective forwarding, Sinkhole, Hello flooding
Транспортний	Flooding, Desynchronization
Прикладний	Overwhelming sensors or sensor overload, Path based attack

Для захисту від таких атак важливо використовувати безпечні протоколи зв'язку, шифрування даних та механізми контролю доступу [14]. Крім того,

регулярний аудит безпеки та оновлення програмного забезпечення можуть допомогти захистити мережу від нових загроз.

1.4 Принцип роботи та функціональні можливості проєктованої системи. Тактико-технічні характеристики проєктованої системи та її аналогів

Ідея використання безпровідних датчиків з сенсорами на полі бою не нова. На сьогодні створено велику кількість моделей датчиків з різноманітними сенсорами та електронікою, розміри таких датчиків можуть коливатися від великих розмірів (польовий сенсорний пост системи BACH/BARRE - 33 х 33 х 33 см, 20 кг) до малих (сенсори iScout - 8,9 х 6,4 х 3,2 см, 0,2 кг), які відрізняються не тільки розмірами, дальністю зв'язку, терміном роботи та модулями, а й тактичним завданням. Власне, саме тактичне завдання та вартість є головними чинниками що визначають комплектацію датчиків.

Для прикладу, система BACH/BARRE (рис. 1.3) розгортається як повноцінний спостережний пост який з'єднується з командним пунктом (комп'ютером). Вона призначена для наземної та повітряної розвідки. Усього таких розгорнутих постів може бути від одного до восьми на один командний пункт. З опису зрозуміло, що система BACH/BARRE призначена для розвідки поблизу місць можливої дислокації противника [15]. Натомість, сенсорна система iScout (рис. 1.4) може бути використана безпосередньо в місцях дислокації противника. Як правило, вузли iScout застосовується для: захисту своїх військ; моніторингу об'єктів та периметру навколо них; моніторингу державного кордону. Сенсорні вузли дешеві, невеликі, мають невелику дальність зв'язку та виявлення і призначені для виявлення тільки наземних цілей, можуть працювати від сонячної батареї, мають вбудовані сейсмічні, акустичні, магнітні та інфрачервоні датчики. На таблиці (1.3) зазначено можливості сенсорної системи iScout з виявлення цілей.

Рисунок 1.3 – Сенсорна система BACH/BARRE та розгорнутий спостережний пост

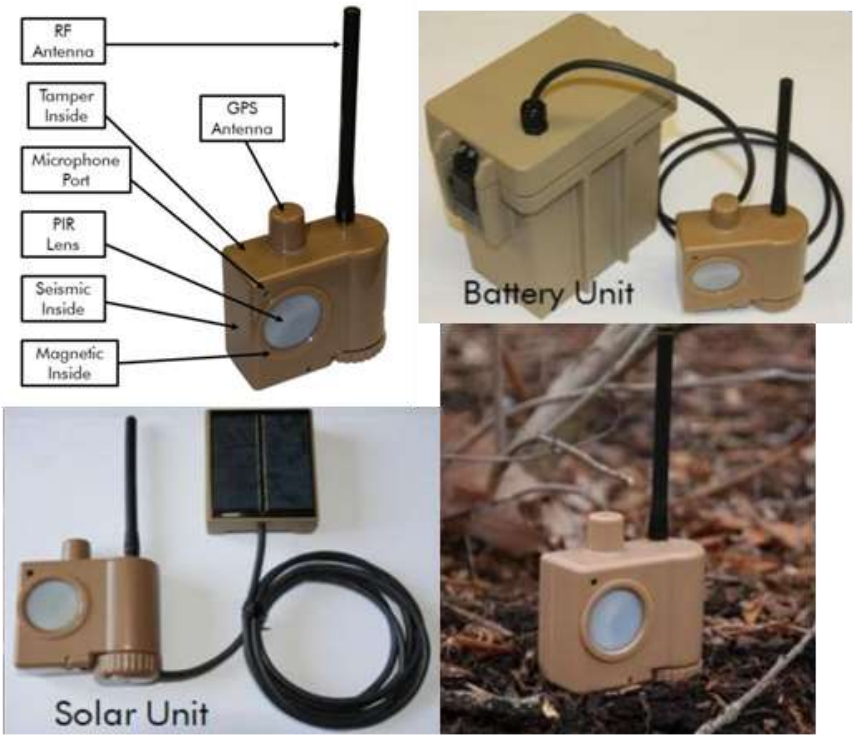


Рисунок 1.4 – Сенсорна система iScout та її компоненти

Таблиця 1.3 – Можливості сенсорної системи iScout з виявлення цілей

Тип цілі/сенсора	Радіус		
	Інфрачервоний	Сейсмічний	Магнітний
Жива сила	50 м	50 м	3 м
Колісна техніка	100 м	150 м	7 м
Гусенична техніка	200 м	300 м	30 м

Розглянуті сенсорні вузли не є еталоном. Сенсорні вузли можуть мати і більші, менші габарити, іншу комплектацію, що залежить від їх призначення. В кваліфікаційній роботі для мережі взято за зразок саме датчики типу iScout – такі датчики мають малі розміри, дешеві в виготовленні та малопомітні. Кількість та тип сенсорів що містить вузол принципіально не важливо – вони можуть комплектуватися або модифікуватися залежно від можливостей та тактичного завдання і це не впливатиме на алгоритми роботи мережі.

Параметри покриття датчика БСМ залежать від декількох факторів, включаючи тип датчика, його радіус дії та місце розташування. Ось деякі з ключових параметрів покриття для сенсорів БСМ:

– радіус дії або дальність дії датчика – це максимальна відстань, на якій він може виявити або виміряти фізичну величину, для моніторингу якої він призначений;

– поле зору датчика – це область, в якій він може виявити або виміряти фізичну величину, яку він призначений контролювати;

– точність зондування або точність вимірювання датчика – це ступінь, до якого він може точно виміряти фізичну величину, для моніторингу якої він призначений;

– частота дискретизації датчика – це частота, з якою він відбирає зразки навколишнього середовища і збирає дані;

– час автономної роботи датчика – це час, протягом якого він може працювати від одного заряду батареї. Час автономної роботи залежить від різних факторів, таких як енергоспоживання датчика, протокол зв'язку та частота передачі даних;

– щільність розміщення сенсорів у БСМ – це кількість сенсорів на одиницю площі. Вища щільність розгортання може забезпечити краще покриття і точніші дані, але вона також може збільшити вартість мережі і споживати більше енергії;

– топологія мережі БСМ – це розташування датчиків і спосіб, яким вони взаємодіють один з одним. Добре продумана топологія мережі може гарантувати, що датчики ефективно розподілені і з'єднані для забезпечення якісного покриття навколишнього середовища.

1.5 Постановка задачі

В даному розділі було проведено аналіз предметної області за темою кваліфікаційної роботи, проведено огляд існуючих рішень за темою кваліфікаційної роботи та їх аналіз, також було розглянуто існуючі класифікації таких систем, проаналізовано роботи дослідників на дану тематику. В розділі було проведено класифікацію проєктованої системи відповідно до різних критеріїв, таких як тип розгортання мережі, топологія мережі, модель передачі сигналу, тип мережевих вузлів, склад вузлів, тип живлення мережі, оперативність передачі даних мережею, строк служби мережі. Була визначена сфера застосування та призначення системи, розглянуто поширені загрози для систем даного типу та засоби протидії, захисту, які використовуються в таких системах. Зазначено принцип роботи та функціональні можливості проєктованої системи. Визначено тактико-технічні характеристики проєктованої системи та розглянуто характеристики її аналогів.

Узагальнюючи можна зазначити, що в даному розділі було розглянуто та проаналізовано матеріал, сформовано модель системи, що є підґрунтям для переходу до від етапу аналізу та підготовки до безпосереднього проєктування системи та в подальшому її реалізації.

Наступною задачею є вибір алгоритмів для реалізації системи, створення власних моделей на їх основі, з подальшим компонуванням модулів в цілісну модель системи. Після цього буде окреслено ряд проблем, вразливостей спроєктованої системи, атаки які можуть бути реалізовані та визначено способи і засоби які дозволяють зменшити ризик реалізації таких атак. Для цього буде змодельовано декілька сценаріїв проведення атаки на систему.

В підсумку, буде проведено тестування системи та її компонентів, та проаналізовано отримані результати.

2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ

2.1 Аналіз особливостей та побудова логічної моделі системи

Визначимо важливі для нас характеристики вузла та їх значення, створимо модель датчика що буде використовуватися в проєктуванні мережі (табл. 2.1).

Таблиця 2.1 - Параметри моделі сенсорного вузла

Параметр		Позначення	Значення
Підсилювач сигналу	поріг відстані для заміни моделей підсилення	d_0	87.7 м
	затрати енергії на передачу даних на відстань $<d_0$ (free space model)	E_{fs}	0.01 нДж/біт/м2
	затрати енергії на передачу даних на відстань $>d_0$ (multipath fading model)	E_{mp}	0.0000013 нДж/біт/м4
Енергія що витрачається при отриманні та відправленні повідомлення		*Eelec*	50 нДж/біт
Ємність акумулятора вузла		*C*	500000000 нДж

Ці параметри потрібні для розрахунку передачі даних.

2.2 Вибір засобів та алгоритмів для реалізації поставленого завдання

Даний розділ розбитий на підкроки відповідно до етапів реалізації [16].

Крок 1: Розгортання мережі.

На даному етапі завдання полягає в вибору оптимального алгоритму для моделювання випадкового розгортання мережі. Для початку розглянемо список таких алгоритмів:

– рівномірне випадкове розгортання – алгоритм передбачає випадкове розміщення датчиків у зоні розгортання з рівномірною ймовірністю.

– пуассонівське випадкове розгортання – алгоритм заснований на розподілі Пуассона, де датчики розміщуються випадковим чином з фіксованою щільністю датчиків на одиницю площі.

– розгортання за сіткою – в алгоритмі область розгортання розбивається на сітку комірок однакового розміру, і кожна комірка заселяється датчиком випадковим чином;

– кластерне розгортання – алгоритм передбачає групування датчиків у кластери, де кожен кластер містить певну кількість датчиків. Кластери розміщуються випадковим чином в межах області розгортання, а датчики в кожному кластері розміщуються рівномірно;

– гаусівське випадкове розміщення – алгоритм використовує гаусівський розподіл для випадкового розміщення датчиків у зоні розгортання, з більшою щільністю датчиків навколо центру і меншою щільністю до країв;

– розгортання Вороного – в алгоритмі область розгортання розбивається на комірки Вороного на основі розташування датчиків. Кожній комірці призначається датчик, і комірки випадковим чином розміщуються в межах зони розгортання;

– розгортання на основі покриття – алгоритм розміщує датчики на основі їхньої зони покриття таким чином, щоб кожна ділянка в регіоні розгортання була покрита принаймні одним датчиком.

Ці алгоритми можуть бути використані для створення різних сценаріїв розгортання для симуляції БСМ, вибір алгоритму залежить від вимог конкретного застосування. В даному конкретному випадку було вибране рівномірне випадкове розгортання, так як воно найкраще підходить для тестування проєктованої системи.

Крок 2: Алгоритми покриття (кластеризації).

Список найпопулярніших алгоритмів для кластеризації БСМ:

– LEACH (Low-Energy Adaptive Clustering Hierarchy). Це популярний алгоритм кластеризації, який формує кластери динамічно на основі енергетичних рівнів датчиків. Він використовує рандомізовані ротації для рівномірного розподілу використання енергії між датчиками в мережі;

– HEED (Hybrid Energy-Efficient Distributed Clustering). Цей алгоритм спрямований на мінімізацію споживання енергії, забезпечуючи при цьому збалансоване споживання енергії кожним кластером. Він використовує імовірнісний підхід до вибору голів кластерів і враховує як фактор відстані, так і фактор енергії в процесі кластеризації.

– TEEN (Threshold-sensitive Energy Efficient sensor Network protocol). Цей алгоритм розділяє сенсорні вузли на дві групи на основі їх рівня енергії і використовує порогове значення для визначення того, коли вузол повинен приєднатися до кластера або стати головою кластера.

– PEGASIS (Power-Efficient Gathering in Sensor Information Systems). Цей алгоритм будує ланцюжок вузлів, де кожен вузол зв'язується зі своїми сусідами, щоб відправити дані на базову станцію. Він використовує жадібний алгоритм для вибору наступного вузла в ланцюжку, який має найкоротшу відстань до базової станції [17].

– SEP (Stable Election Protocol). Цей протокол використовує імовірнісний підхід для вибору голови кластера і гарантує, що процес вибору голови кластера є стабільним у часі [18].

– MC-LEACH (Multi-Cluster LEACH). Цей алгоритм розширює протокол LEACH для підтримки декількох кластерів, де голови кластерів вибираються на основі їх залишкової енергії та відстані від базової станції.

– EEC (Energy-Efficient Clustering). Цей алгоритм використовує підхід на основі нечіткої логіки для вибору голів кластерів на основі їхньої залишкової енергії, розташування та кількості сусідніх вузлів.

Ці алгоритми можна використовувати для формування кластерів у БСМ на основі різних критеріїв, таких як рівень енергії, відстань, розташування та вимоги до агрегації даних. Вибір алгоритму залежить від конкретного застосування і бажаних цілей кластеризації.

В проєктованій системі для покриття мережі буде використовуватися алгоритм PEGASIS. Алгоритм Power-Efficient Gathering in Sensor Information Systems (PEGASIS) – популярний алгоритм кластеризації в бездротових сенсорних мережах (БСМ), який має ряд переваг над іншими алгоритмами кластеризації, зокрема:

– енергоефективність. PEGASIS призначений для оптимізації споживання енергії в БСМ. Він будує ланцюжок вузлів, де кожен вузол взаємодіє зі своїми сусідами, щоб відправити дані на базову станцію. Це усуває необхідність у зв'язку на великі відстані та зменшує енергоспоживання мережі.

– масштабованість. PEGASIS масштабується і може використовуватися у великих мережах БСМ з сотнями і тисячами вузлів. Він утворює ланцюжок вузлів, які взаємодіють один з одним, а довжина ланцюжка може регулюватися в залежності від розміру мережі.

– балансування навантаження. PEGASIS гарантує, що енергетичне навантаження рівномірно розподіляється між вузлами мережі. Він використовує жадібний алгоритм для вибору наступного вузла в ланцюжку, який має найкоротшу відстань до базової станції. Це збалансовує споживання енергії між вузлами та подовжує термін служби мережі.

– надійність. PEGASIS надійна і може витримувати збої в роботі вузлів або зміни топології мережі. Він використовує механізм резервування, де кожен вузол має кілька сусідів, і якщо один з них виходить з ладу, вузол може зв'язатися з іншими сусідами, щоб забезпечити передачу даних.

– низька затримка. PEGASIS має низьку затримку, оскільки дані можуть швидко передаватися через ланцюжок вузлів. Це важливо для додатків, які вимагають передачі даних в режимі реального часу.

Підводячи підсумки, PEGASIS є перспективним алгоритмом кластеризації, який може покращити енергоефективність, масштабованість, балансування навантаження, надійність та затримку БСМ.

Крок 3: Вибір центрів кластерів.

Оскільки БСМ за топологією визначена як гомогенна, то постає питання вибору голів кластерів на які будуть передаватися дані з вузлів кластера, а голови кластерів в свою чергу, будуть передавати дані на базову станцію. Для цієї цілі було обрано алгоритм FOREL. FOREL - це алгоритм кластеризації з розбивкою, який розбиває дані на групи на основі їхньої близькості один до одного. Зазначимо головні причини, чому цей алгоритм підходить для вирішення поставлених задач:

1. Алгоритм FOREL простий і легкий у реалізації. Він вимагає лише одного параметра - радіуса кластера. Алгоритм є обчислювально ефективним і може працювати з великими наборами даних.

2. На відміну від деяких інших алгоритмів кластеризації, таких як k-середні, алгоритм FOREL не робить жодних припущень про розподіл даних. Він може працювати з наборами даних складної форми та ідентифікувати кластери будь-якої форми та розміру.

3. Алгоритм FOREL може обробляти викиди в наборі даних, призначаючи їх в окремий кластер.

4. Алгоритм FOREL є стійким до шуму в наборі даних. Він може визначити ядро кожного кластера і призначити зашумлені точки даних

окремим кластерам або повністю виключити їх.

5. Алгоритм FOREL можна адаптувати для роботи з різними типами даних, такими як числові та категоріальні дані. Його також можна модифікувати для обробки різних метрик відстані.

6. Алгоритм FOREL створює кластери, які легко інтерпретувати та візуалізувати. Центри та радіуси кластерів дають уявлення про структуру даних і можуть допомогти в аналізі даних та прийнятті рішень.

Також зазначимо причини вибору алгоритму FOREL, які випливають зі специфіки поставленої задачі:

1. FOREL в якості параметра він приймає радіус кластера. Оскільки збір даних передбачається з аероплатформи, зона видимості якої теж визначається радіусом, ці параметри легко узгодити при прямій передачі даних від вузлів до станції. Маніпулюючи радіусом як вхідним параметром алгоритму ми можемо легко змінювати розміри кластерів, відповідно і відстань польоту і час збору даних з мережі, що дозволяє в критичних ситуаціях збирати дані швидко – але з високими затратами енергії вузлів, або повільно, економлячи заряди вузлів. Тобто, це робить процес збору даних динамічним.

2. FOREL є швидким та легковісним алгоритмом, у разі виявлення змін в мережі перекластеризувати вибірку можна змінювати в поточному часі.

3. Так як в FOREL вартість обчислень низька, вибірку можна перекластеризовувати після кожного збору даних. Як наслідок – ротація голів кластерів, що забезпечує більш рівномірний розряд кластерів.

4. Зникнення чи поява датчика в мережі не вплине на роботу та ефективність мережі. Мережу просто буде перекластеризовано.

Загалом, алгоритм кластеризації FOREL - це простий і ефективний алгоритм, стійкий до шуму і здатний обробляти набори даних складної форми і розміру.

Крок 4: Збір даних, алгоритми маршрутизації

Алгоритм FOREL визначає центри кластерів. Ці точки простору є центрами масс кластерів. Центр масс може визначатися як просторовий центр масс, а може і корегуватися з урахуванням таких величин як заряд, потужність вузлів. Маршрутизація проєктованої мережі розраховується по центрам кластерів [19].

2.3 Розробка модулів системи. Компонування модулів проєктованої системи. Налагодження взаємодії між програмними модулями

Першочергово здійснимо моделювання розгортання системи.

2.3.1 Моделювання розгортання системи

При розгортанні системи не передбачається ніякої строгої моделі, проєктована система повинна працювати при будь-якій моделі розгортання, при виході з ладу датчиків чи їх розряджання. Саме тому для тестування такої моделі найкраще буде зупинитися на моделі рівномірного випадкового розгортання. Для моделювання такого розгортання використовуються функції з псевдовипадковим виходом. Однією з математичних моделей функції з псевдовипадковим виходом є генератор псевдовипадкових чисел (ГПВЧ). ГПВЧ – це детермінований алгоритм, який генерує послідовність чисел, що здається випадковою, але насправді генерується за допомогою детермінованого алгоритму. Одним з найпоширеніших алгоритмів ГПСЧ є лінійний конгруентний генератор (LCG), який генерує послідовність псевдовипадкових чисел за наступною формулою (1.1):

$$x_{n+1} = (ax_n + c) \bmod m \qquad (1.1)$$

де x_n - поточне число в послідовності, a, c і m - константи, а mod - операція за модулем.

Алгоритм LCG широко використовується в комп'ютерному програмуванні, він є простим у реалізації та відповідає поставленим вимогам, тому його було обрано серед інших алгоритмів для моделювання процесу розгортання. На (рис. 2.1) можемо бачити результат моделювання розгортання 100 вузлів на ділянці 600 х 600 метрів за результатами алгоритму LCG.

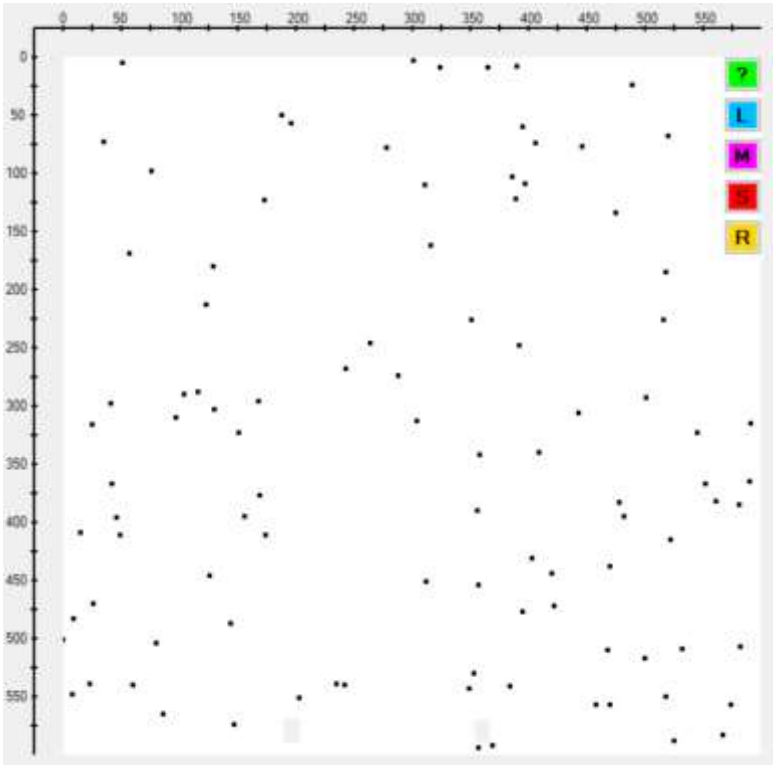


Рисунок 2.1 – Результат роботи алгоритму LCG: розміщення 100 вузлів на ділянці 600 х 600 м

Після розгортання перейдемо до етапу кластеризації мережі.

2.3.2 Кластеризація мережі

Для кластеризації мережі було обрано алгоритм FOREL. Алгоритм кластеризації FOREL - це алгоритм кластеризації з розбивкою, який розбиває дані на групи на основі їхньої близькості один до одного. Назва FOREL розшифровується як FORmula REpresentation of Objects in clusters (Формула представлення об'єктів у кластерах).

Алгоритм працює наступним чином:

1) обрати радіус R для кластера. Він може базуватися на попередніх знаннях або бути обраний емпірично;

2) обрати випадкову точку даних як початковий центроїд кластера;

3) для кожної точки даних, що залишилася, обчислити її відстань від центроїда. Якщо відстань менша або дорівнює R, додати точку даних до кластера;

4) обчислити новий центроїд для кластера на основі середнього значення точок даних у кластері;

5) повторити кроки 3 і 4, доки позиція центроїда не стане стабільною;

6) повторити з кроку 2 для точок що залишилися без кластера.

Результатом роботи алгоритму FOREL є набір кластерів, що не перетинаються, де кожен кластер представлений своїм центроїдом (рис. 2.2).

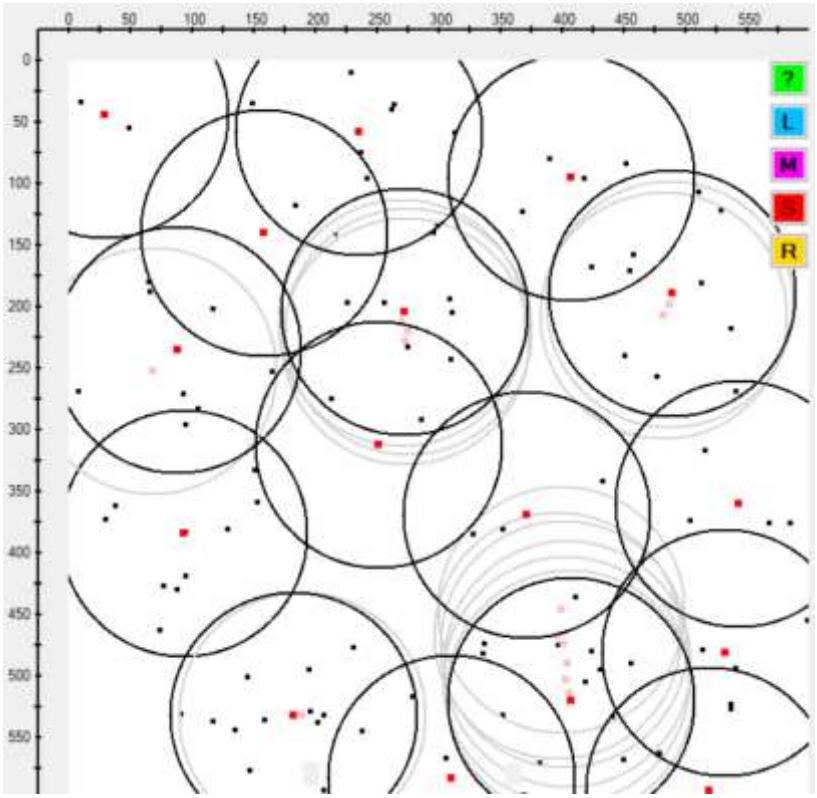


Рисунок 2.2 - Результат роботи алгоритму FOREL: покриття 100 вузлів на ділянці 600 х 600 м

Центроїди (геометричні центри кластерів або центри масс кластерів) позначені червоними точками, чорні кола – кластери, відповідно світло-червоними точками позначаються зміщення центроїдів, сірі кола – зміщення кластерів при обчисленні, чорними точками позначаються вузли.

Виконаємо побудову маршруту базової станції.

2.3.3 Побудова маршруту базової станції

Як базову станцію для збору планується використовувати безпілотну аероплатформу (БПЛА), адже дана мережа планується до розгортання в складних і важкодоступних місцях. Тому наступним кроком є побудова маршруту базової станції (БС). Така задача також відома як задача комівояжера (TSP - Traveling Salesman Problem).

TSP – це класична задача, яка полягає в знаходженні найкоротшого можливого маршруту, яким комівояжер може відвідати набір міст рівно один раз і повернутися в початкове місто. Це добре відома NP-важка задача, що означає, що її точне розв'язання для великих екземплярів вимагає значних обчислювальних витрат, і для її розв'язання було розроблено багато наближених алгоритмів. Я вважаю, що для повноти необхідно розглянути популярні способи вирішення даної задачі, вибрати серед них ті, які можна використати як еталонні, оптимальні та які можуть бути використані для збору даних з мереж такого типу. Зазначимо декілька полярних способів вирішення задачі TSP [20]:

– метод грубої сили (Brute force, прямий перебір) передбачає перевірку кожної можливої перестановки міст і вибір міста з найкоротшою відстанню. Цей метод не є практичним для великих вибірок, оскільки кількість можливих перестановок зростає в геометричній прогресії зі збільшенням кількості міст, відповідно, даний алгоритм обмежений розміром вибірки, часом який може бути витрачений на обчислення та потужністю обчислювального пристрою;

– найближчий сусід (Nearest Neighbor) - алгоритм найближчого сусіда починається з випадкового міста і повторно відвідує найближче невідвідане

місто, поки не будуть відвідані всі міста. Цей алгоритм швидкий і простий у реалізації, але він рідко дає оптимальне рішення;

– 2-opt: Алгоритм 2-opt - це ітераційний алгоритм покращення, який починається з початкового розв'язку і багаторазово міняє місцями пари ребер, намагаючись покращити розв'язок;

– алгоритм Христофідеса - це евристичний алгоритм, який гарантує розв'язок, що не більше ніж у 1,5 рази перевищує оптимальний розв'язок для будь-якого екземпляра TSP. Він полягає у знаходженні мінімального остовного дерева екземплярів вибірки, а потім побудові мінімальної вагової досконалої відповідності у вершинах дерева з непарними степенями;

– евристика Ліна-Кернігана - це ще один ітераційний алгоритм покращення, який починається з початкового рішення і використовує послідовність локальних оптимізацій для покращення рішення;

– генетичні алгоритми - це клас алгоритмів оптимізації, натхненних біологічною еволюцією. Вони передбачають створення популяції рішень-кандидатів і використання генетичних операторів, таких як мутація і кросинговер, для генерації нових рішень-кандидатів;

– оптимізація мурашиних колоній - це ще один метаевристичний алгоритм, натхненний поведінкою мурах, які шукають їжу. Він включає в себе моделювання поведінки мурах, які залишають феромони на шляхах між містами і використовують феромонні сліди для пошуку хорошого рішення.

Варто зазначити, що алгоритм маршрутизації може бути обраний залежно від параметрів системи та інших факторів. Так, наприклад, на невеликих вибірках доцільно використовувати алгоритм прямого перебору. Також можлива оптимізація результатів алгоритму, але дана тема не буде розглядатися в цій роботі, тому що завдання цієї роботи – оцінка можливостей та демонстрація ефективності роботи такої системи.

Провівши огляд різних способів вирішення задачі TSP та проаналізувавши їх, я вирішив що для демонстрації роботи проєктної системи буде розглянуто наступні алгоритми:

– алгоритм прямого перебору;

– алгоритм найближчого сусіда;

– алгоритм опуклої оболонки;

– спіральний маршрут [21];

– алгоритм FPPWR (Fast Path Planning with Rule).

Алгоритм прямого перебору можливо використовувати на малих вибірках. На (рис. 2.3) можна бачити результат роботи даного алгоритму на 10 точках маршруту. Маршрут для збору даних базовою станцією будується з нульової координати по центрам кластерів. В лівому нижньому кутку (рис. 2.3) можемо бачити загальну відстань побудованого маршруту.

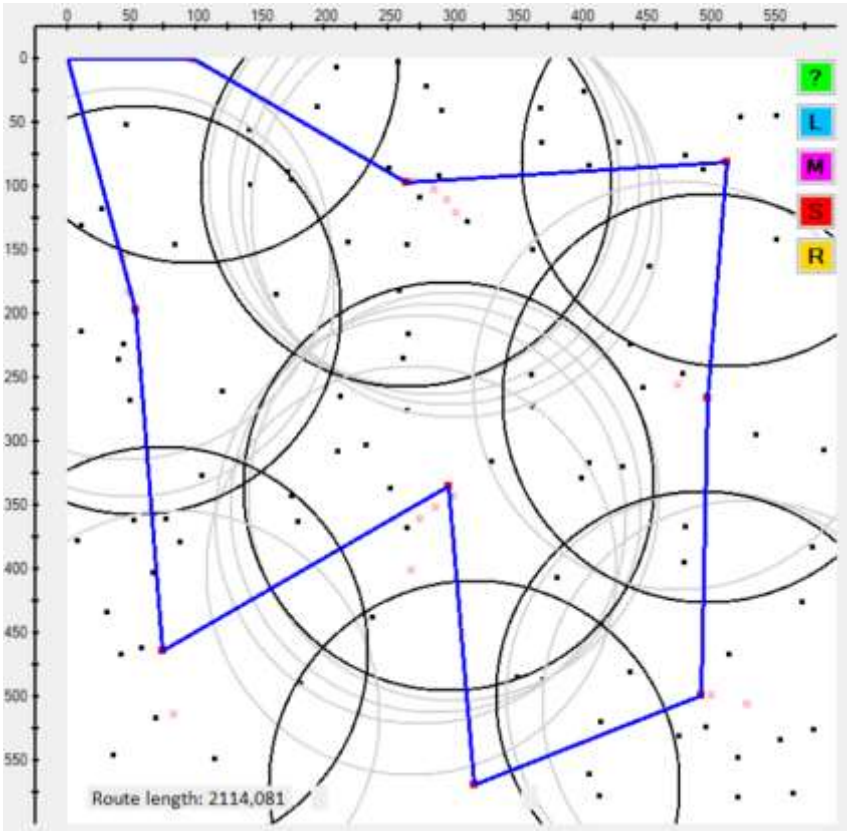


Рисунок 2.3 - Побудова маршруту на кластеризованій вибірці методом прямого перебору

На (рис. 2.4) виконана побудова маршруту за допомогою алгоритму найближчого сусіда. Цей алгоритм та алгоритм прямого перебору є еталонними алгоритмами, за допомогою яких можливо оцінити ефективність інших алгоритмів, які будуть використані при створенні моделі мережі.

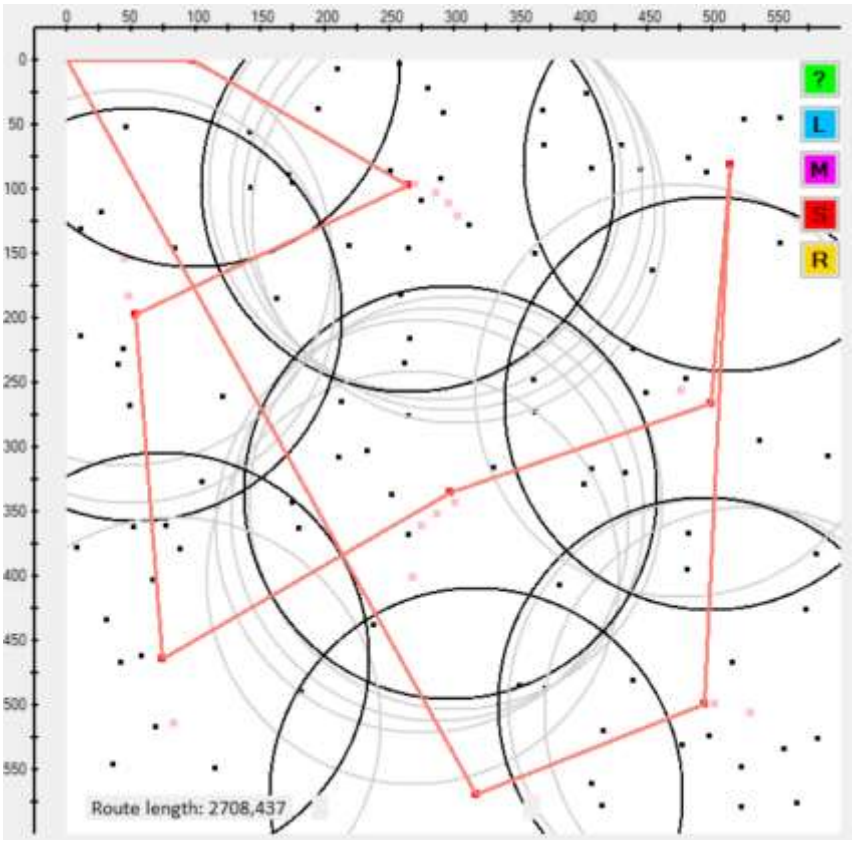


Рисунок 2.4 - Побудова маршруту на кластеризованій вибірці за алгоритмом найближчого сусіда

Алгоритм опуклої оболонки – евристичний алгоритм, результат роботи якого зображений на (рис. 2.5). Робота алгоритму розділена на 2 етапи: перший етап – це робота алгоритму упаковки подарунків (gift wrapping algorithm) або ще відомого як марш Джарвіса (Jarvis march), другий етап – це ітераційне згортання побудованого маршруту всередину. На кожному кроці перебираються ребра маршруту та шукається найближча точка до даного ребра, вона позначається як нова точка маршруту, утворюючи з одного ребра два, і так поки всі точки не будуть внесені до маршруту. Стандартний пошук

найближчої точки до маршруту виконується порівнянням сум відстаней крайніх двох точок ребра до обраної точки. Ту точку, в якої сума найменша буде внесено до маршруту. Натомість, я виконую обчислення не за відстанню, а за кутом між прямими, а точніше за косинусом кута. Таким чином, буде шукатися точка з найбільшим кутом відносно ребра (найменшим косинусом), що дає змогу запобігти гострим кутам в маршруті і цим зменшує кількість перехрещень. Різниця в роботі двох даних підходів була протестована на малих і середніх вибірках, де краще себе показав останній. Проте, в контексті даної роботи це питання не розглядається, так як потребує розгляду в форматі окремої роботи та більш детальної перевірки і тестування.

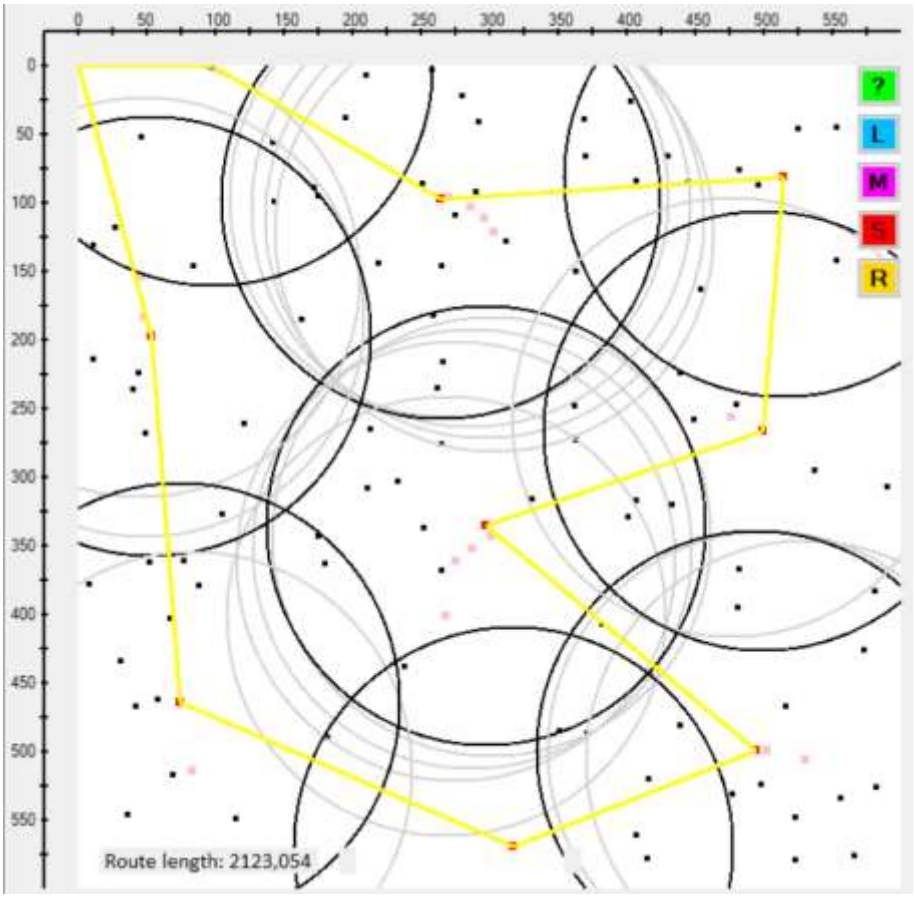


Рисунок 2.5 - Побудова маршруту на кластеризованій вибірці методом опуклої оболонки

В даній роботі показано результат роботи цього алгоритму на 10 точках маршруту (рис. 2.5). Варто зазначити, що на великих вибірках (близько 500 точок та більше) результати роботи такого алгоритму починають вирівнюватися з результатами алгоритму найближчого сусіда, але проте на малих та середніх вибірках цей алгоритм працює доволі успішно, та з зменшенням вибірки зменшує шанси утворення перехрещень маршруту (рис. 2.6).

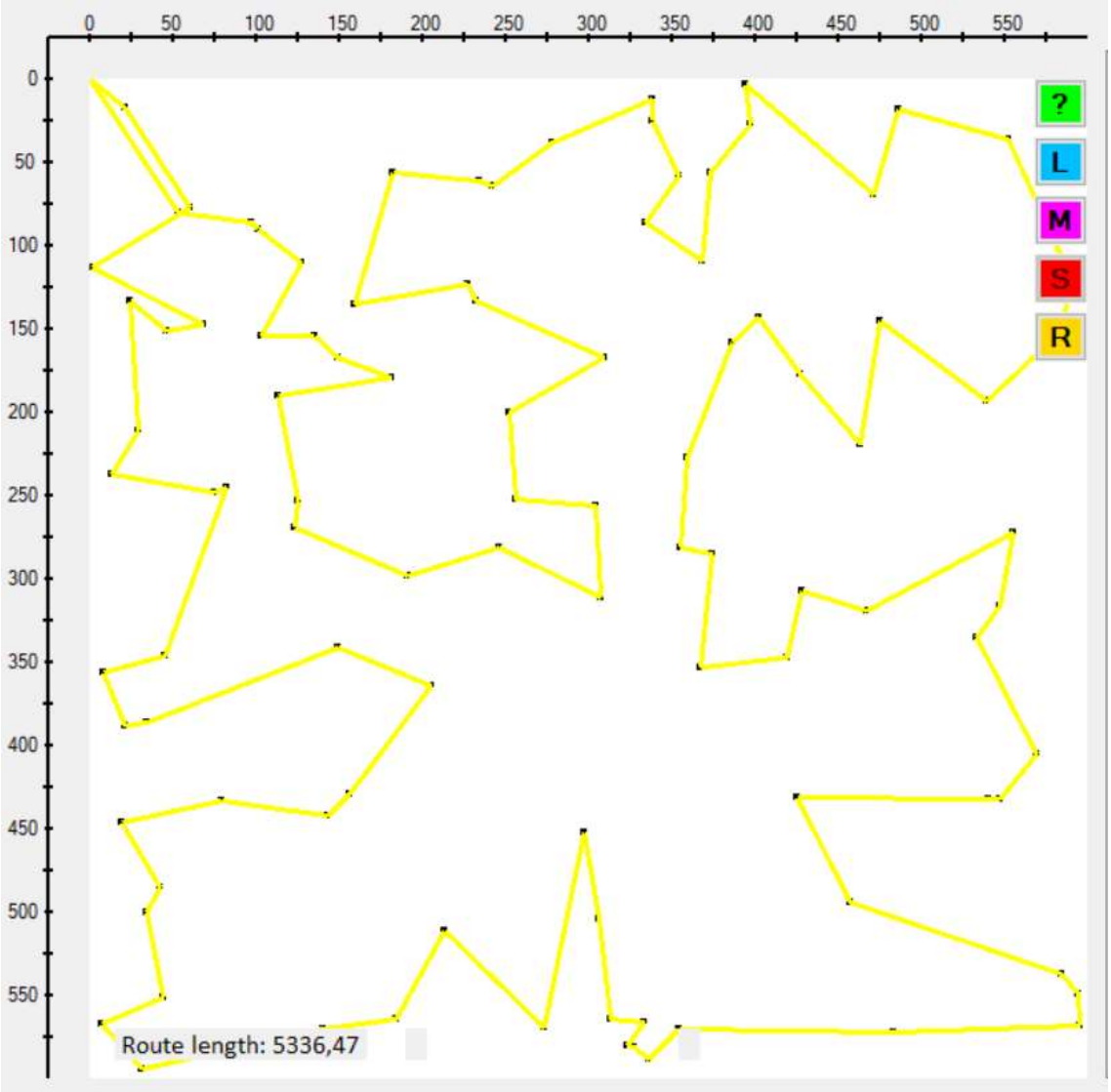


Рисунок 2.6 - Побудова маршруту на вибірці зі 100 точок методом опуклої оболонки

Після розгортання і першої кластеризації, перекластеризації мережі БС не має даних про точки маршруту, тому для визначення маршруту БС потрібно здійснити обліт території де розгорнута мережа для збору даних, які тільки після цього можуть бути оброблені і використані для побудови маршруту. Фактично, ми втрачаємо ресурси на один обліт тільки на збір даних про положення центрів кластерів, адже для алгоритму прямого перебору та опуклої оболонки для обчислення потрібна уся вибірка, а використання алгоритму найближчого сусіда наражає на ризик втратити з поля зору частину мережі. В такій ситуації для суміщення процесів збору даних про мережу та сенсорних даних можуть бути використані алгоритми, які зачасту будують маршрут довший ніж за алгоритмом найближчого сусіда, проте які не потребують цільної вибірки для побудови маршруту і гарантують збір усієї інформації [22]. До таких алгоритмів належать пошук спірального маршруту та FPPWR.

За основу для знаходження спірального маршруту, як і для алгоритму опуклої оболонки взято алгоритм Джарвіса, проте з деякою модифікацією – маршрут не замикається на першій точці, а продовжує свою роботу і рухається по точках, які ще не були внесені до маршруту, таким чином рухаючись по спіралі ззовні до середини вибірки (рис. 2.7). На рисунку рух починається з нульової координати вниз. Дійшовши до останньої точки в маршруті БС повертається в початкову.

Альтернативним способом вирішення вищезазначеної задачі є алгоритм FPPWR. FPPWR - це алгоритм, спеціально розроблений для планування маршруту в контексті збору даних з повітря за допомогою БпЛА або мобільних збирачів даних. Робота алгоритму полягає в розбитті ділянки обльоту на сітку, в якій для кожного сегменту оптимальне рішення шукається окремо, як правило, жадібним алгоритмом, а загальний рух по сітці здійснюється по визначеному правилу.

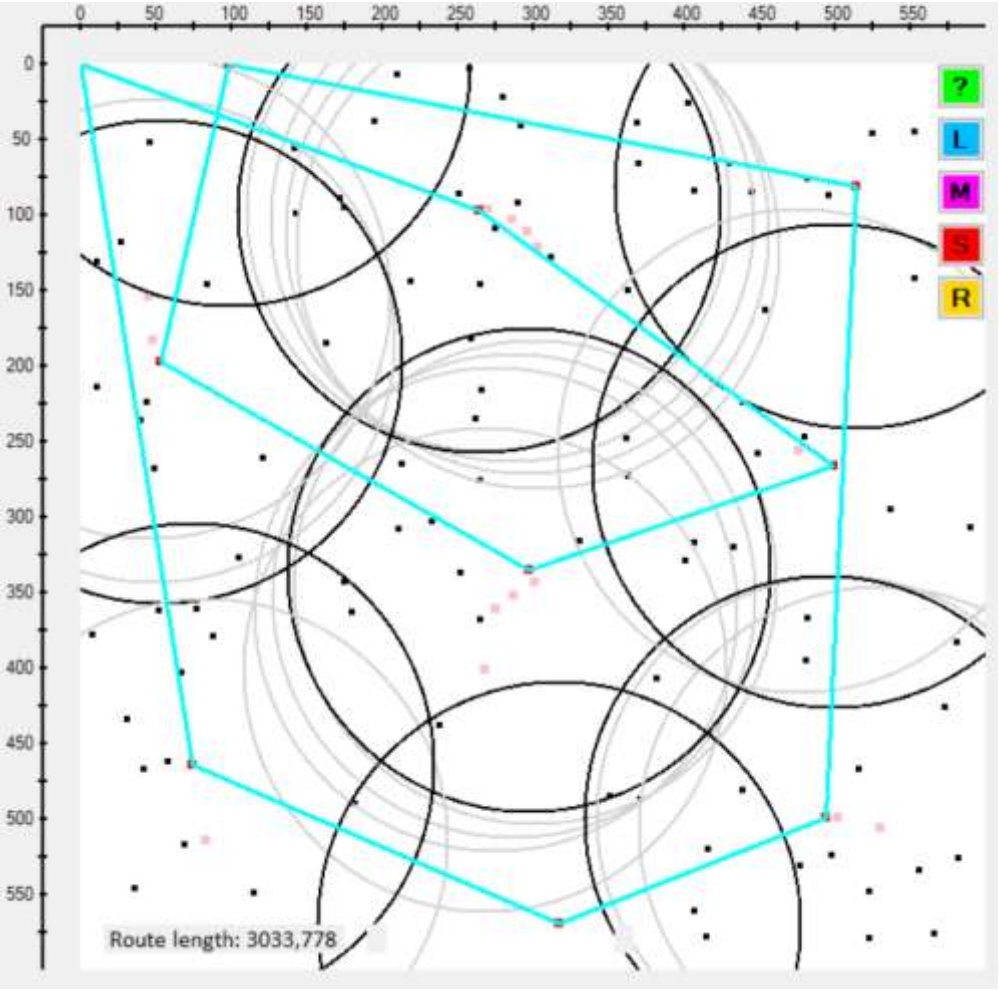


Рисунок 2.7 - Побудова маршруту на кластеризованій вибірці методом спіралі

Для клітинок це як правило рух змійкою по рядам. Таким чином, маршрут будується так що гарантовано один раз відвідується кожен сегмент мережі. Такий алгоритм об'єднує маршрути в межах кожного сегменту в основний маршрут польоту, що допомагає отримати глобальний маршрут польоту швидко і з дотриманням визначених правил (рис. 2.8). Загальна мета FPPWR полягає в тому, щоб забезпечити швидке і ефективне рішення для планування траєкторії в сценаріях збору повітряних даних, беручи до уваги обмеження і вимоги великомасштабних бездротових сенсорних мереж. Такий підхід дозволяє працювати з великомасштабними мережами датчиків і скоротити витрати часу в порівнянні з іншими алгоритмами (табл. 2.2).

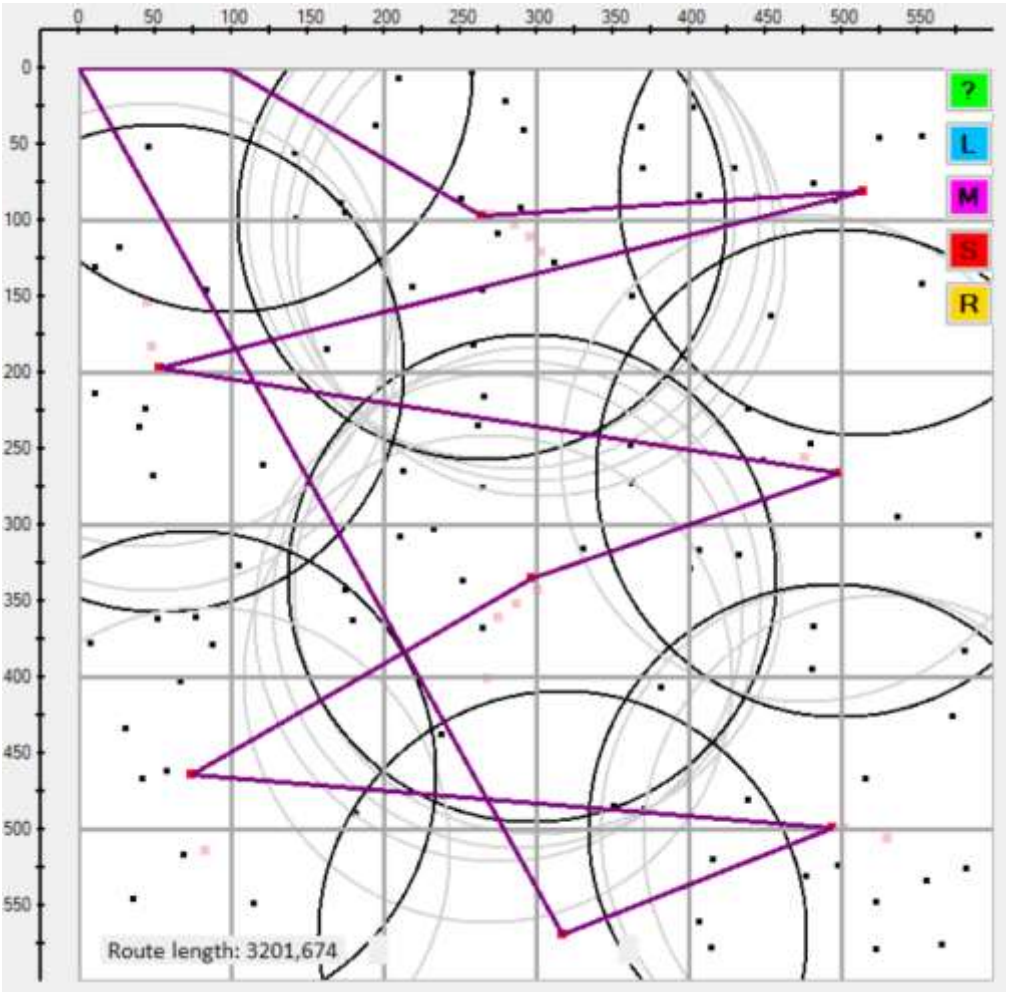


Рисунок 2.8 - Побудова маршруту на кластеризованій вибірці за допомогою алгоритму FPPWR

Таблиця 2.2 – Рекомендовані граничні значення для зміни алгоритму пошуку шляху.

Кількість точок шляху	Алгоритм пошуку шляху	Умовні розміри БСМ
< 12	Прямий перебір	Малі БСМ
12 - 5000	Опуклої оболонки	Середні БСМ
> 5000	FPPWR	Великомасштабні БСМ

2.4 Визначення вразливостей мережі. Розробка системи протидії від атак, збоїв в роботі мережі

На даному етапі проведено аналіз вимог та параметрів мережі, на основі якого вибрано протоколи безпеки та інтегровано в існуючу програмну модель мережі.

2.4.1 Вибір протоколів безпеки

У бездротових сенсорних мережах (БСМ) механізми автентифікації вузлів мають вирішальне значення для забезпечення цілісності та безпеки мережі. Зазаначимо механізми автентифікації вузлів, які найчастіше використовуються в БСМ [23]:

– симетрична автентифікація ключа - передбачає використання спільного секретного ключа між вузлами та базовою станцією;

– інфраструктура відкритих ключів - використовує криптографію з асиметричним ключем. Кожен вузол має унікальну пару відкритий-приватний ключ. Вузли можуть автентифікувати себе, підписуючи повідомлення своїм закритим ключем і надаючи свій відкритий ключ для перевірки вузлом-одержувачем;

– автентифікація «запит-відповідь» - механізми автентифікації «запит-відповідь» передбачають обмін запитом від верифікатора (наприклад, базової станції або довіреного органу) до вузла. Вузол відповідає дійсною відповіддю, згенерованою за допомогою криптографічного алгоритму та його секретного ключа. Потім верифікатор перевіряє відповідь для автентифікації вузла;

– автентифікація на основі сертифіката - базується на використанні цифрових сертифікатів для автентифікації вузлів. Кожен вузол має унікальний сертифікат, що містить його ідентифікатор і відкритий ключ. Під час автентифікації вузол надає свій сертифікат верифікатору, який перевіряє автентичність сертифіката та перевіряє автентичність вузла [24];

– полегшені протоколи автентифікації - БСМ часто мають вузли з обмеженими ресурсами з обмеженою обчислювальною потужністю та пам’яттю. Щоб врахувати ці обмеження, спрощені протоколи автентифікації, такі як TinySec, LEAP або SPINS, розроблені для забезпечення ефективної та безпечної автентифікації, придатної для середовищ БСМ.

Для мережі що досліджується оптимальним варіантом буде вибір полегшених протоколів автентифікації. Полегшені протоколи автентифікації призначені для вирішення обмежень ресурсів сенсорних вузлів, одночасно забезпечуючи ефективну та безпечну автентифікацію. Зазначимо найпоширеніші з них:

– TinySec - це широко використовуваний легкий протокол безпеки для БСМ. Він забезпечує конфіденційність, цілісність даних і автентифікацію джерела. TinySec використовує криптографію з симетричним ключем і використовує алгоритм потокового шифрування для шифрування та автентифікації пакетів даних. Він розроблений, щоб бути ефективним з точки зору використання пам’яті та обчислювальних витрат;

– SPINS - це набір протоколів безпеки, спеціально розроблених для БСМ. Він включає кілька полегшених протоколів автентифікації, таких як SNEP (протокол шифрування мережі датчиків), TESLA (ефективна автентифікація потоку, стійка до втрат) і µTESLA (ефективна автентифікація потоку, стійка до втрат). Ці протоколи задовольняють різні вимоги безпеки, включаючи конфіденційність даних, цілісність і автентифікацію джерела, зводячи до мінімуму споживання ресурсів;

– LEAP (протокол локалізованого шифрування та автентифікації) - це легкий протокол автентифікації, який забезпечує безпечний зв’язок між сенсорними вузлами та базовою станцією. Він використовує криптографію з симетричним ключем і використовує код автентифікації повідомлення на основі хеш-функції (HMAC) для цілісності даних і автентифікації. LEAP має на

меті мінімізувати витрати на обчислення та зв’язок, пов’язані з механізмами безпеки;

– SPINS+, MiniSec: SPINS+ та MiniSec є удосконаленнями набору протоколів SPINS, призначені для підвищення безпеки та ефективності. Ці протоколи включають легкі криптографічні алгоритми та методи керування ключами, адаптовані для вузлів датчиків з обмеженими ресурсами;

– SEAL (Simple and Efficient Authenticated Link) - це легкий протокол автентифікації для захисту каналів зв’язку між вузлами датчиків. Він використовує код автентифікації повідомлення на основі хеш-функції (HMAC) і спільний секретний ключ для цілісності даних і автентифікації. SEAL розроблений як обчислювально ефективний і підходить для вузлів датчиків з обмеженими ресурсами.

Ці легкі протоколи автентифікації встановлюють баланс між вимогами безпеки та обмеженнями ресурсів у БСМ. Вони забезпечують важливі функції безпеки, мінімізуючи обчислювальну складність, використання пам’яті та енергоспоживання. Однак при виборі відповідного полегшеного протоколу автентифікації важливо враховувати конкретні вимоги та характеристики розгортання БСМ [25].

Вибір оптимального полегшеного протоколу автентифікації для БСМ залежить від кількох факторів, у тому числі конкретних вимог, обмежень і міркувань безпеки розгортання. Ось кілька факторів, які слід враховувати під час оцінки придатності спрощених протоколів автентифікації:

– вимоги безпеки;
– обмеження ресурсів;
– масштабованість;
– надійність;
– сумісність;
– наукові дослідження.

Для вибору протоколу призначимо оцінку для кожного фактору системи (табл. 2.3).

Таблиця 2.3 – Оцінка факторів системи

Фактор	Оцінка (1-5)
Вимоги безпеки	3
Обмеження ресурсів	2
Масштабованість	5
Надійність	4
Сумісність	1
Наукові дослідження	5

Враховуючи ці фактори, придатним полегшеним протоколом автентифікації для розгортання БСМ може бути SPINS або його вдосконалена версія SPINS+. SPINS та SPINS+ надають набір протоколів безпеки, спеціально розроблених для БСМ, що задовольняють різні вимоги безпеки, такі як конфіденційність даних, цілісність і автентифікація джерела.

Зазначу, як фактори узгоджуються із запропонованим протоколом:

– SPINS і SPINS+ пропонують повний набір функцій безпеки, що забезпечує задовільний рівень безпеки;

– незважаючи на те, що SPINS і SPINS+ відносно легкі порівняно з деякими іншими протоколами, вони все одно мають певні накладні витрати;

– SPINS і SPINS+ розроблені для масштабування та можуть ефективно обробляти велику кількість сенсорних вузлів. Вони можуть ефективно адаптуватися до зростання мережі;

– SPINS, і SPINS+ були розроблені з урахуванням міркувань безпеки, щоб забезпечити надійний захист від різних атак;

– SPINS і SPINS+ можуть вимагати деяких модифікацій для їх інтеграції в існуючі платформи або структури БСМ, що може вимагати додаткових

зусиль. Однак вони були широко впроваджені та досліджені за підтримки громадськості;

– ці протоколи були ретельно досліджені та пропонують надійні механізми безпеки.

Крім того, стек протоколів SPINS вирішує і інші задачі безпеки, він складається з кількох компонентів, які працюють разом, щоб забезпечити такі послуги безпеки, як конфіденційність даних, цілісність і автентифікація джерела. Основні компоненти набору протоколів SPINS:

– SNEP (Sensor Network Encryption Protocol) відповідає за забезпечення конфіденційності даних у БСМ. Він використовує методи шифрування симетричного ключа для шифрування даних датчика перед передачею. Ключ шифрування використовується між авторизованими вузлами в мережі;

– μTESLA (Micro Timed Efficient Stream Loss-tolerant Authentication) – це протокол синхронізації часу та автентифікації джерела. Він використовує цифрові підписи та мітки часу для забезпечення автентичності та цілісності даних датчика. Кожен вузол датчика підписує свої дані та містить мітку часу, що дозволяє одержувачу перевірити походження даних і виявити будь-які зміни;

– LITE (Localized Intrusion-Tolerant Encryption) – це ефективний і локалізований протокол керування ключами для БСМ. Він відповідає за встановлення та розподіл ключів шифрування між сенсорними вузлами. LITE мінімізує накладні витрати на керування ключами, забезпечуючи безпечні механізми розповсюдження та відкликання ключів;

Ці компоненти інтегровані в єдину систему, щоб забезпечити безпечний зв’язок, цілісність даних і автентифікацію джерела в БСМ. Використовуючи шифрування, автентифікацію, керування ключами та механізми безпеки маршрутизації, SPINS підвищує загальну безпеку мережі та захищає від різних атак, які можуть поставити під загрозу цілісність і конфіденційність даних датчиків.

2.4.2 Інтегрування протоколів безпеки та захисту в мережу

Інтеграція протоколів безпеки та захисту в систему безпеки БСМ необхідна для забезпечення конфіденційності, цілісності та доступності даних, а також захисту мережі від різних загроз і атак. При цьому, необхідно правильно узгодити роботу компонентів мережі з інтегрованими механізмами захисту. При правильному компонуванні інтегровані модулі не повинні порушувати роботу системи, а механізми реагування на зміни в мережі мати в основі чітку послідовність реакцій відповідних компонентів мережі, при цьому не повинно відбуватись ніяких конфліктів: передчасного доступу до певного компоненту системи до даних, конкурування між компонентами системи за ресурси, колізій [26].

Для забезпечення сумісності модулів системи з протоколами безпеки і захисту, визначено порядок доступу компонентів системи при реагуванні на зміни в системі, події безпеки (рис. 2.9).

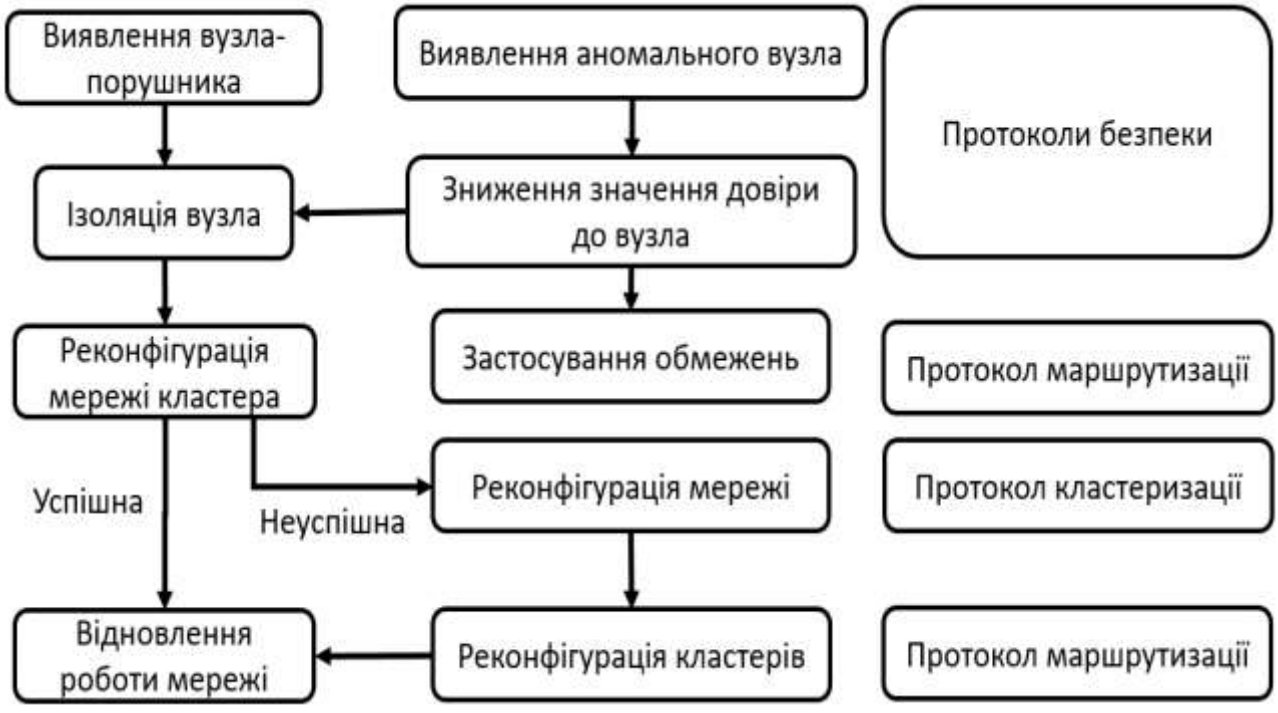


Рисунок 2.9 - Логічна модель реагування мережі на аномальну поведінку вузлів та порушення системи безпеки

Визначення аномального вузла може відбуватися на основі:

– аномалій – проводиться моніторинг поведінки вузлів у мережі та порівняння її з базовою або очікуваною поведінкою. Відхилення від норми можуть свідчити про наявність стороннього або скомпрометованого вузла;

– некорректної поведінки – вузли поводяться таким чином, що порушує очікувану поведінку мережі;

– механізмів довіри – такі механізми встановлюють довірчі відносини між вузлами на основі їхньої минулої поведінки та взаємодії. Вузли з низьким рівнем довіри або вузли, які демонструють неочікувану поведінку, можуть бути позначені як потенційні сторонні вузли.

На основі логічної моделі системи (рис. 2.9) інтегровано рішення безпеки в програмну модель мережі (рис. 2.10, 2.11) [27].

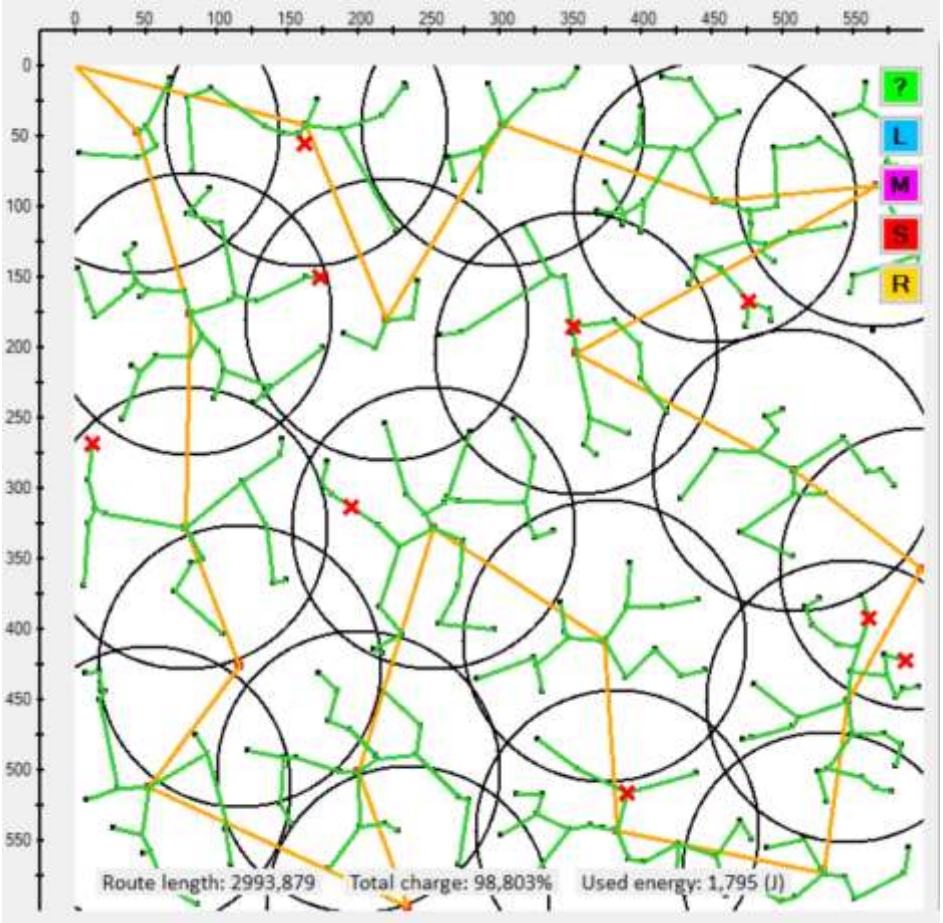


Рисунок 2.10 – Виявлення аномальних вузлів, вузлів-порушників в мережі

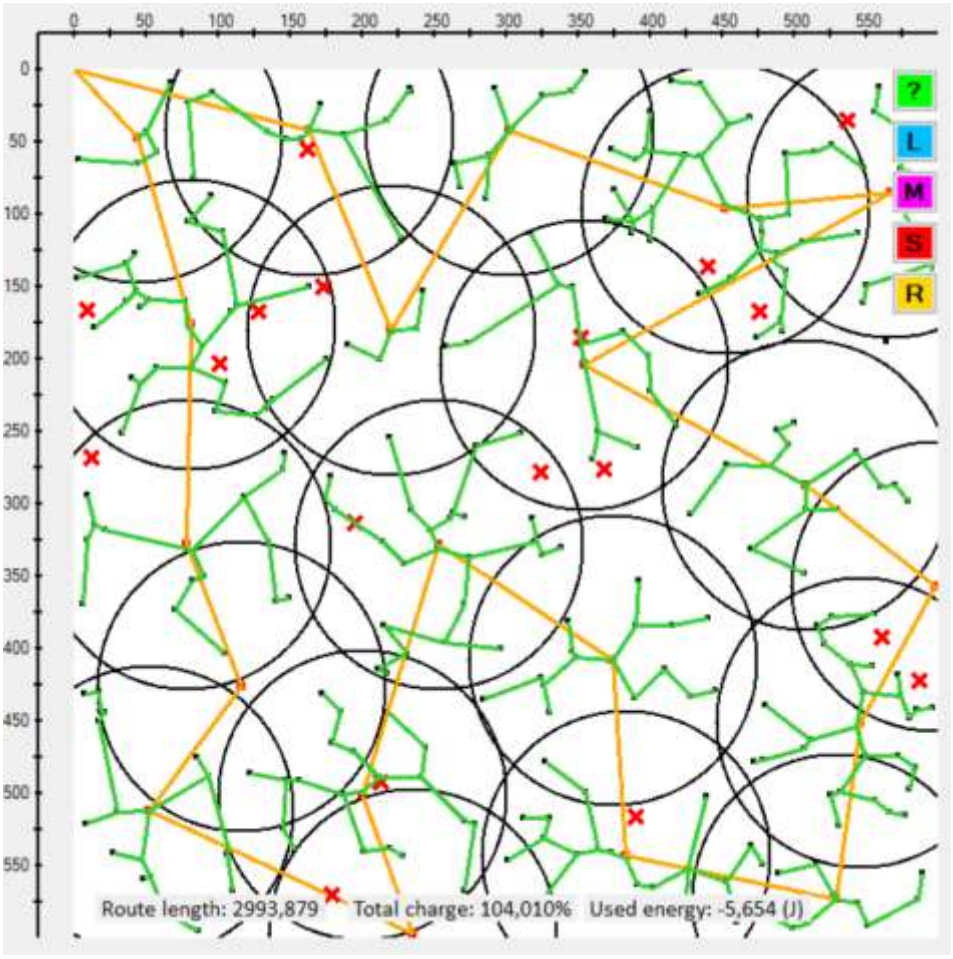


Рисунок 2.11 – Ізолювання аномальних вузлів, вузлів-порушників, реконфігурація кластерів

Пошкоджені вузли з часом можуть відновлювати свою роботу, крім того до мережа може бути розширена, можуть бути додані нові вузли. Розширення мережі – це складний процес, який включає в себе автентифікацію, перевірку надійності, авторизацію вузла і вносить зміни до структури мережі (рис. 2.12). Після проходження автентифікації вузла, виконується пошук вузла у списку довіри, і залежно від результату пошуку приймається рішення. Якщо вузла немає в списку, додається новий запис і визначається коефіцієнт довіри. На основі параметрів в списку довіри приймається рішення про дозвіл на авторизацію вузла в мережі [28].

Рисунок 2.12 – Порядок включення вузлів до мережі

2.5 Висновок

В розділі розроблені складові для мережі, що проєктується, ці окремі модулі були зкомпоновані в єдину систему, в яку згодом було імплементовано механізми та протоколи захисту, визначено порядок дії компонентів системи та їх повноваження в системі; визначено порядок виключення пошкоджених, аномальних, зловмисних вузлів з системи та порядок включення нових вузлів до мережі, продемонстрована робота цих механізмів; проведено оцінку критичних факторів для системи та на її основі обрано протоколи безпеки які будуть використовуватися в мережі. Після даного етапу необхідно провести тестування програмного продукту та проаналізувати отримані результати, визначити відповідність досягнених результатів поставленим завданням та ступінь їх виконання.

3 ТЕСТУВАННЯ СИСТЕМИ РОЗГОРТАННЯ ТА ЗАХИСТУ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Протягом процесу розробки програмної складової системи розгортання та захисту бездротової сенсорної мережі, як і будь-якого програмного продукту, постійно необхідно було проводити її тестування щоб виявити помилки до того, як окремий компонент буде інтегрований в загальну систему. Таким чином, процес тестування, що було проведено, можна розділити на окремі етапи (рис. 3.1).

Рисунок 3.1 – Порядок проведення тестування моделі мережі

Загальний етап тестування можна розділити на 2 етапи: тестування на етапі розробки та фінальні тестування. Розробка мережі починається з розробки окремих модулів, після цього проводиться тестування. Тестування дає можливість визначити правильність роботи логічного модуля, визначити помилки, що були допущені при проєктуванні. Після проведення тестування, залежно від його результатів вносяться зміни до коду алгоритму або модуль визначається як завершений та готовий до інтеграції в загальну модель мережі.

3.1 Тестування на етапі розробки системи

Тестування на етапі розробки дозволяє виявити помилки ще на етапі проєктування. Так, при генерації випадкового розгортання мережі (рис. 3.2) візуально все виглядало правильно, проте після перевірки даних вручну, виявилось що засоби візуалізації які використовуються в проєкті використовують інверсну координатну вісь, яку було вирішено графічно позначити для кращої інформативності (рис. 3.2).

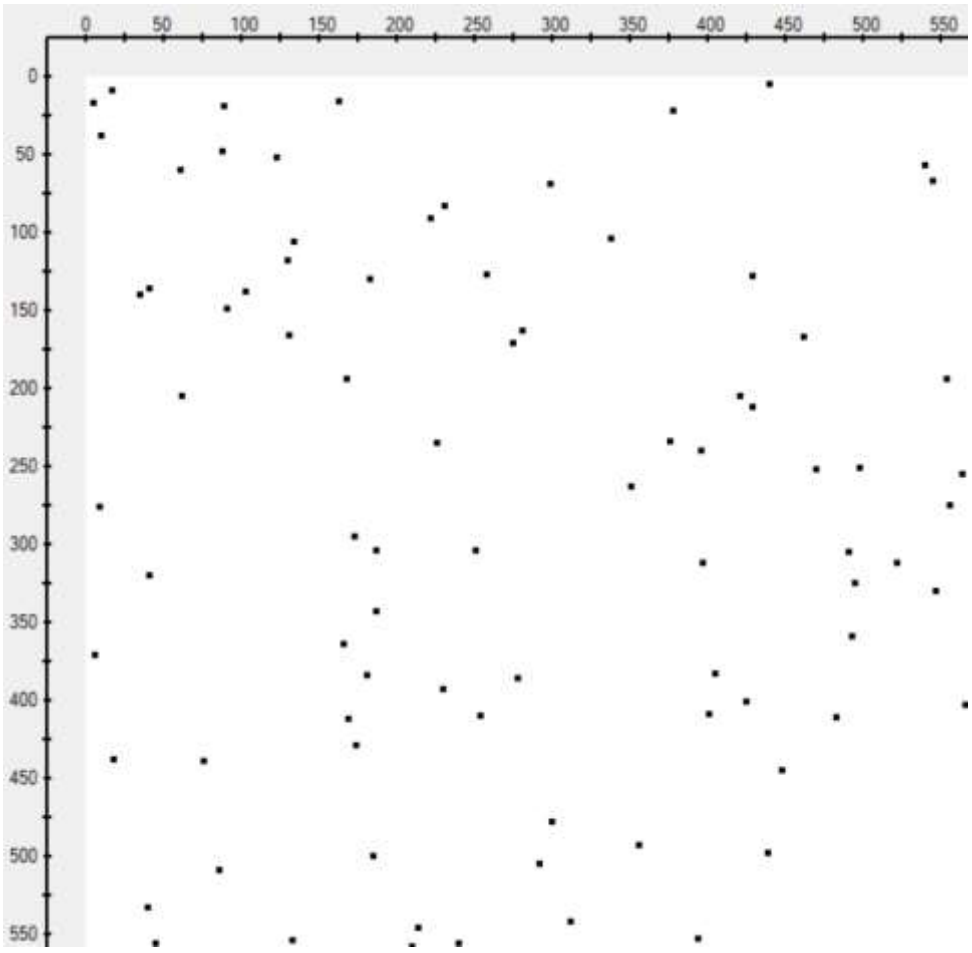


Рисунок 3.2 – Візуалізація випадкового розгортання мережі

Перевірка алгоритмів виконувалась візуально та за допомогою обчислень вручну. Етап проєктування супроводжувався постійними тестами, правками, корегуваннями (рис. 3.3).

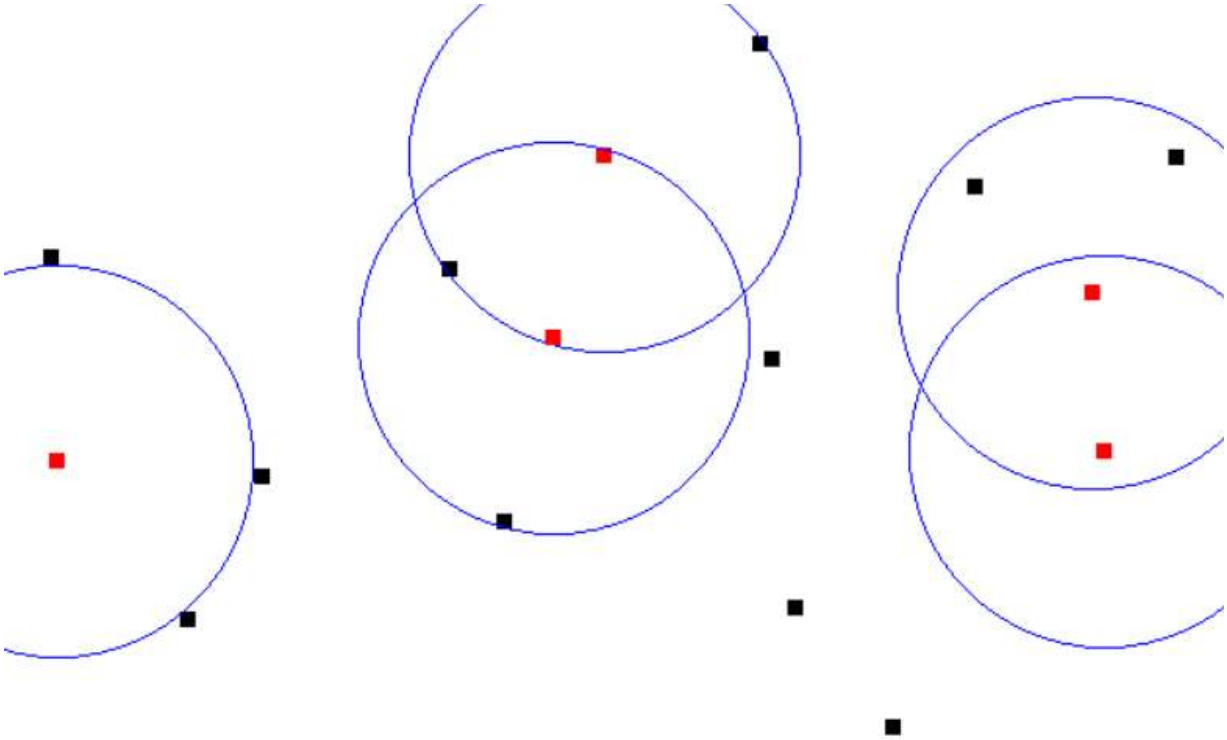


Рисунок 3.3 – Тестування алгоритму FOREL на етапі розробки

В ході проєктування та проведення тестів також може бути виявлено неповноту інформацій що необхідна для моделі, або навіть неправильність таких даних. Так, при моделюванні енергетичної моделі мережі, довелося зрівнювати дані з різних джерел, так як дані з одного джерела зачасту не мали повноти, а іноді і відрізнялись формули, що напряму було видно на роботі моделі – датчики розряджались надто швидко, довго, результати відхилялися від допустимих норм. Таким чином, методом порівняння джерел та перебору варіантів, було підібрано такі вхідні дані, за яких вихідні дані системи відповідають очікуваним. На (рис. 3.4) можемо бачити результати обчислень цієї моделі – загальний заряд вузлів, середня енергія що використовується за один цикл збору даних, використана енергія вузлів за останній цикл, розряд вузлів, суму використаної енергії [29].

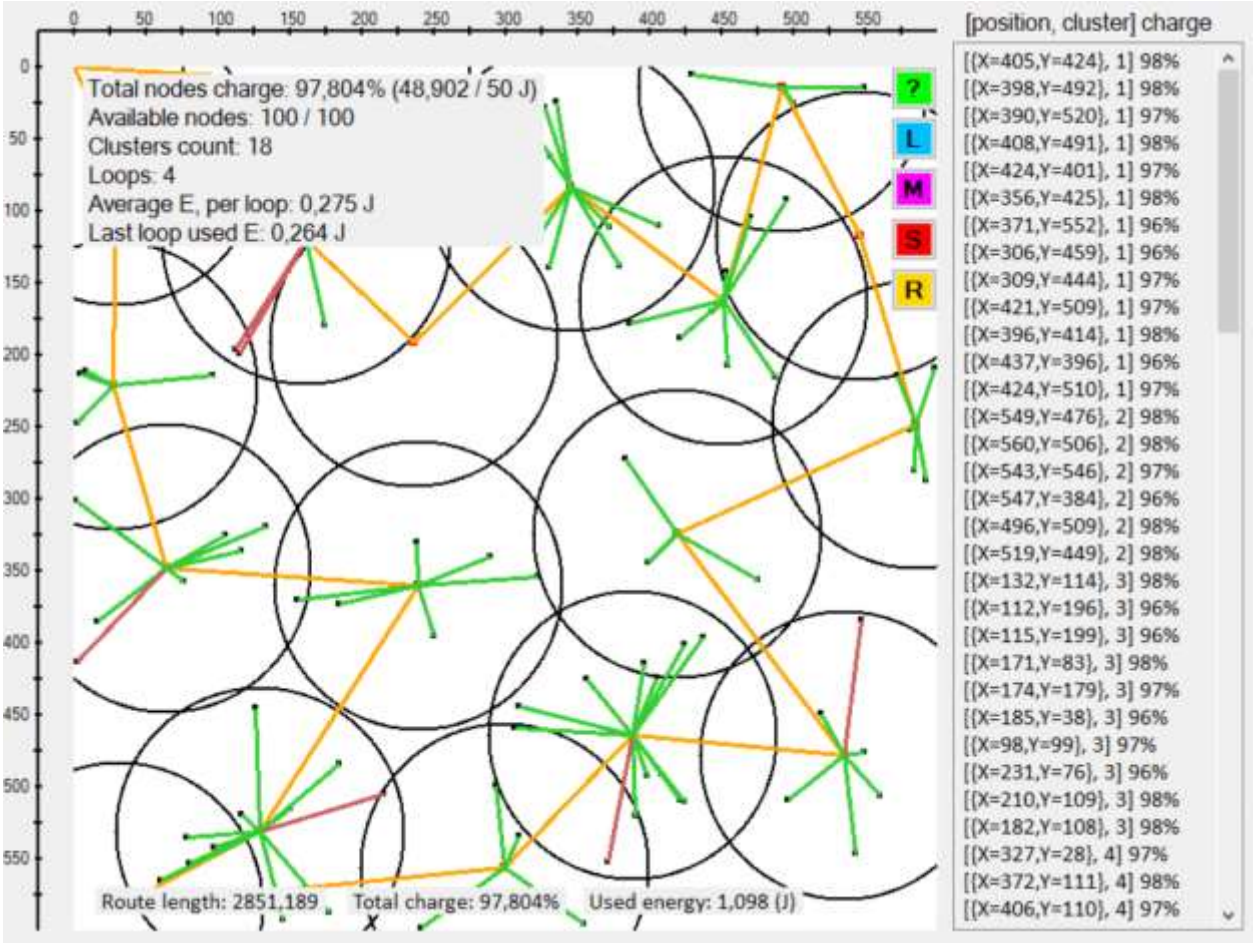


Рисунок 3.4 – Вивід розрахунків енергетичної моделі мережі

3.2 Випробувальне тестування розробленої системи

Кінцеве тестування дозволяє провести глибоке тестування роботи продукту та роботи його компонентів, внести додаткові корективи, оцінити ступінь досягнення поставлених задач. На цьому етапі також визначаються інші дані, які можуть бути критичними, розробляються інструкції. Фінальне тестування дозволяє виявити особливості системи, взаємодії програмних модулів шляхом аналізу результатів тестування. Фінальне тестування включає тестування компонентів мережі з метою виявлення помилок та проведення аналізу. Так, були протестовані алгоритми передачі даних. На (рис. 3.5) можемо бачити роботу алгоритму прямої передачі в варіанті коли для збору

даних як БС може бути використаний коптер, він підлітає в центр кластеру і зависає над ним, поки дані не будуть зібрані з мережевого кластера. Круги – це кластери, червоні та зелені лінії позначають передачу даних в центр кластера до БС, зелені лінії – це модель передачі даних без підсилювача сигналу, червоні відповідно з підсилювачем, оранжевим кольором позначений маршрут БС.

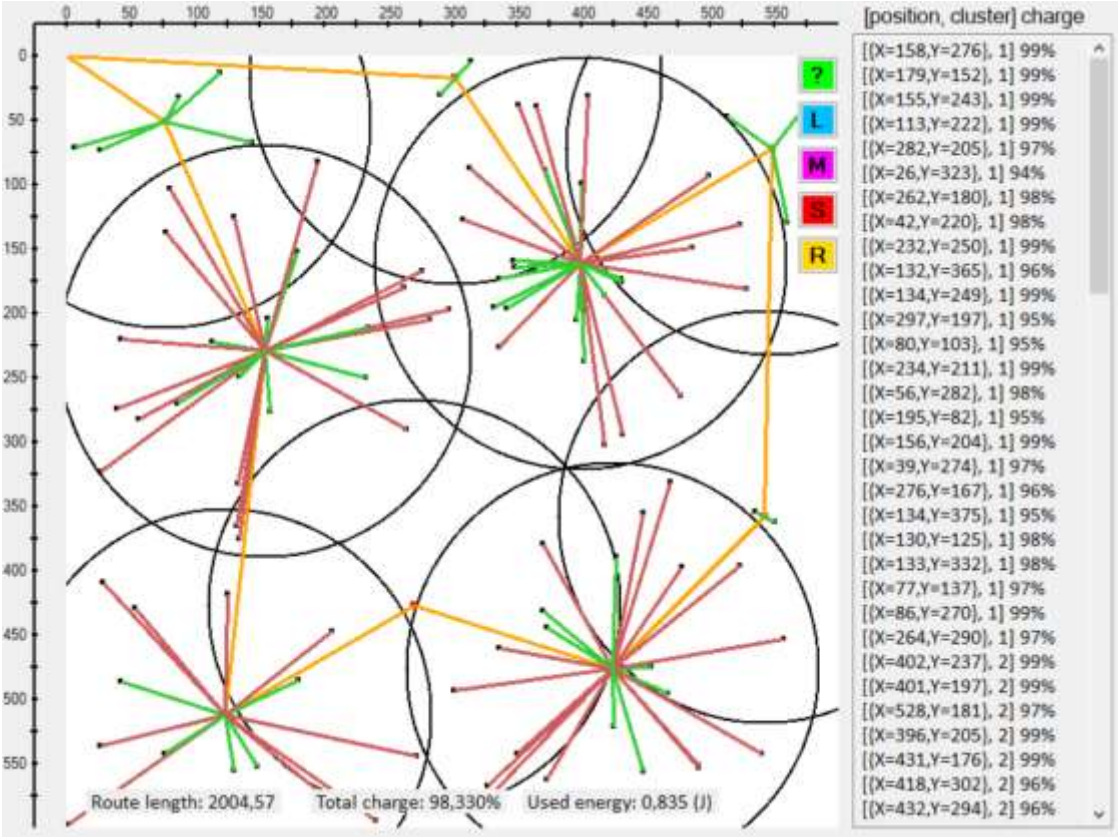


Рисунок 3.5 - Пряма передача даних напряму до станції в центрі кластеру

На (рис. 3.6) зображено алгоритм передачі даних напряму по маршруту слідування БС, що може бути використано як для БпЛА типу коптер так і для БпЛА планерного типу. Передача даних по маршруту слідування здійснюється в момент проходження БС точки на маршруті, найближчої до вузла, що здійснює передачу, а точніше – в момент проходження БС в певних межах від перпендикуляра опущеного з точки на пряму маршруту, розмір такого проміжку для передачі залежить від швидкості руху БС та кількості даних що потрібно передати (рис. 3.7) [30].

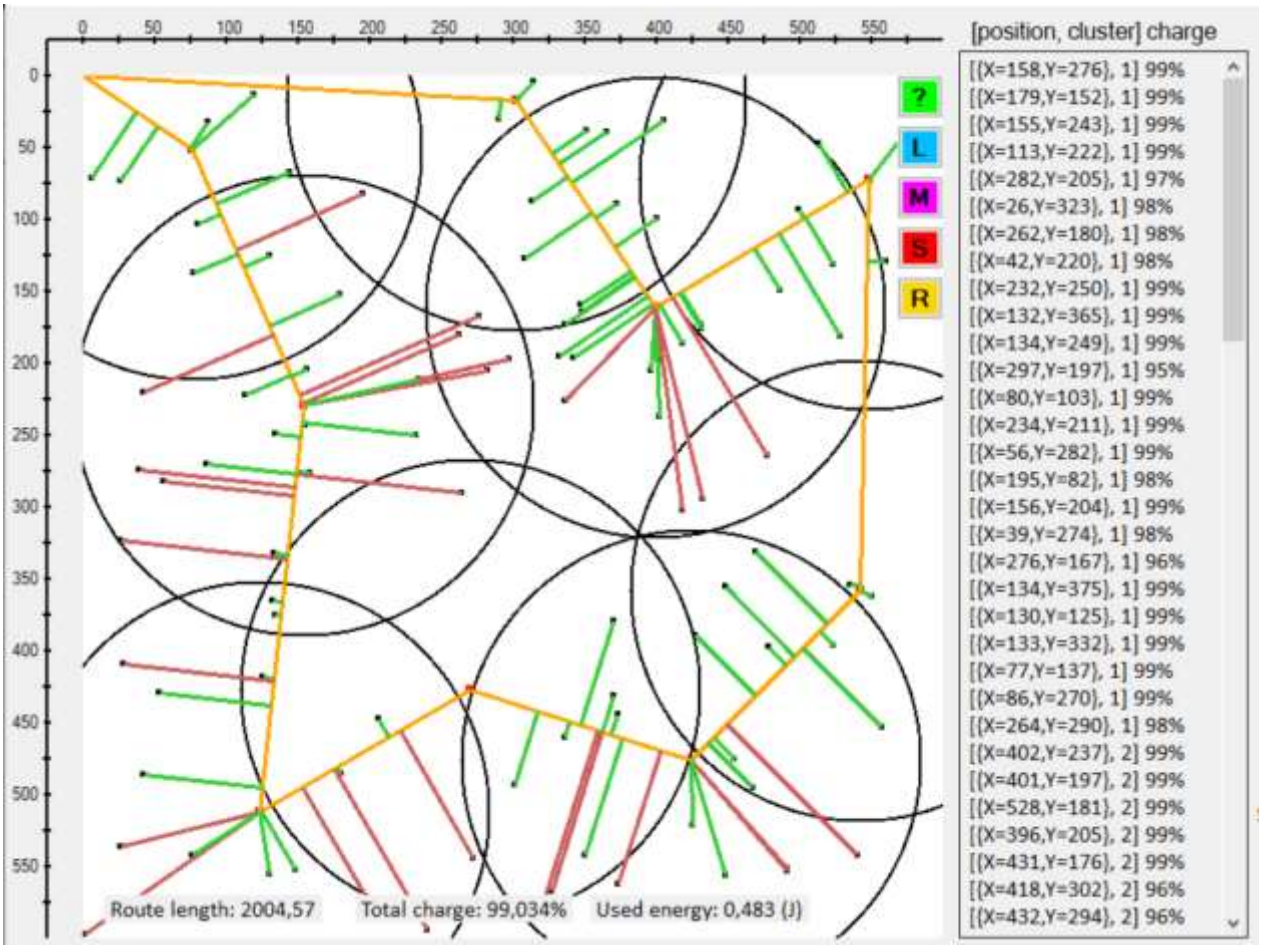


Рисунок 3.6 - Передача даних по маршруту слідування станції

Рисунок 3.7 – Схема передачі даних вузлом по маршруту слідування БС

На рисунку (3.8) зображена передача даних з використанням алгоритму PEGASIS до центру кластеру. Передача даних алгоритмом PEGASIS це передача даних типу “точка-точка” жадібним алгоритмом, в якому вузол передає дані найближчому до нього вузлу в напрямку БС.

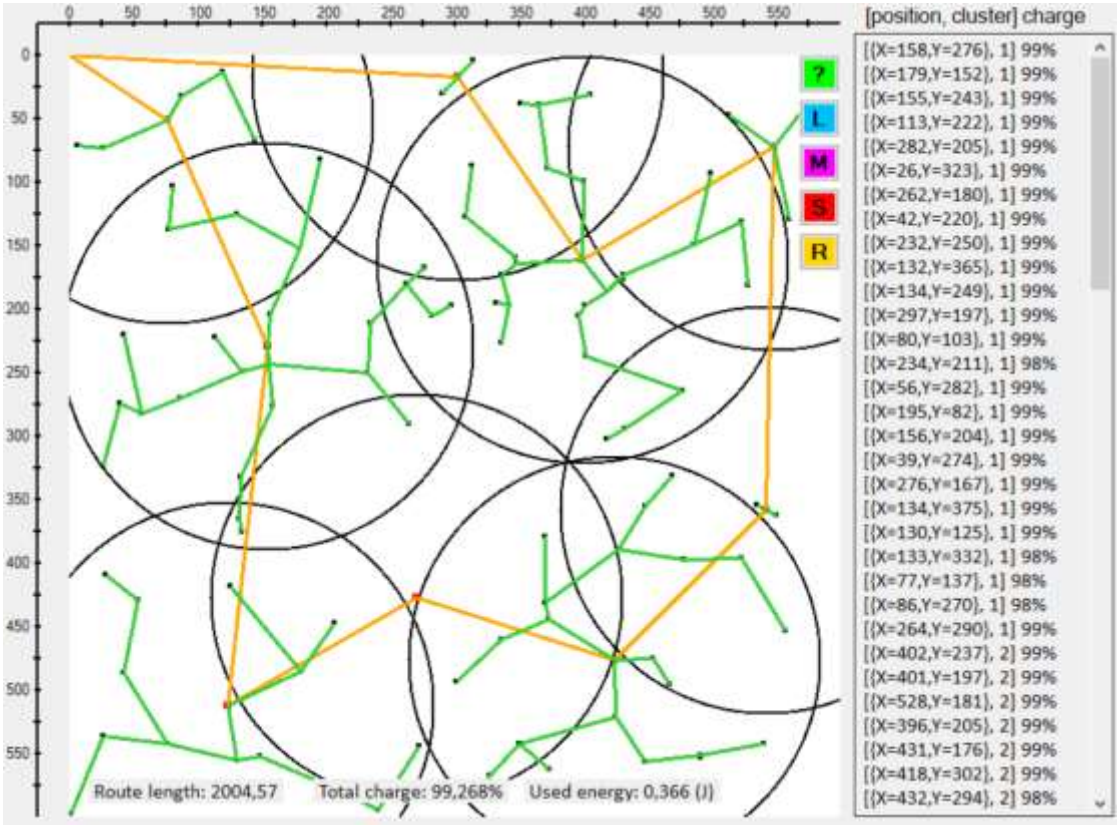


Рисунок 3.8 - Передача даних до центру кластеру за допомогою алгоритму PEGASIS

На (рис. 3.9) зображена передача даних алгоритмом PEGASIS по маршруту слідування станції.

В результаті проведення тестування алгоритмів передачі даних, було отримано цікаві результати їх роботи, а саме, те, як швидко розряджалися вузли при використанні різних алгоритмів для передачі даних, що буде детально розглянуто при аналізі отриманих результатів [31].

Також було проведене тестування механізмів захисту мережі. Так, виявлено, що зазначений на (рис. 2.9) механізм ізоляції вузлів дозволяє реагувати на досить широкий спектр інцидентів та атак. Як приклад, реагування мережі на атаку “Глушіння” (Jamming) по даному алгоритму (рис. 3.10). В результаті глушіння отримані пакети даних містять аномальну кількість спотворень [32].

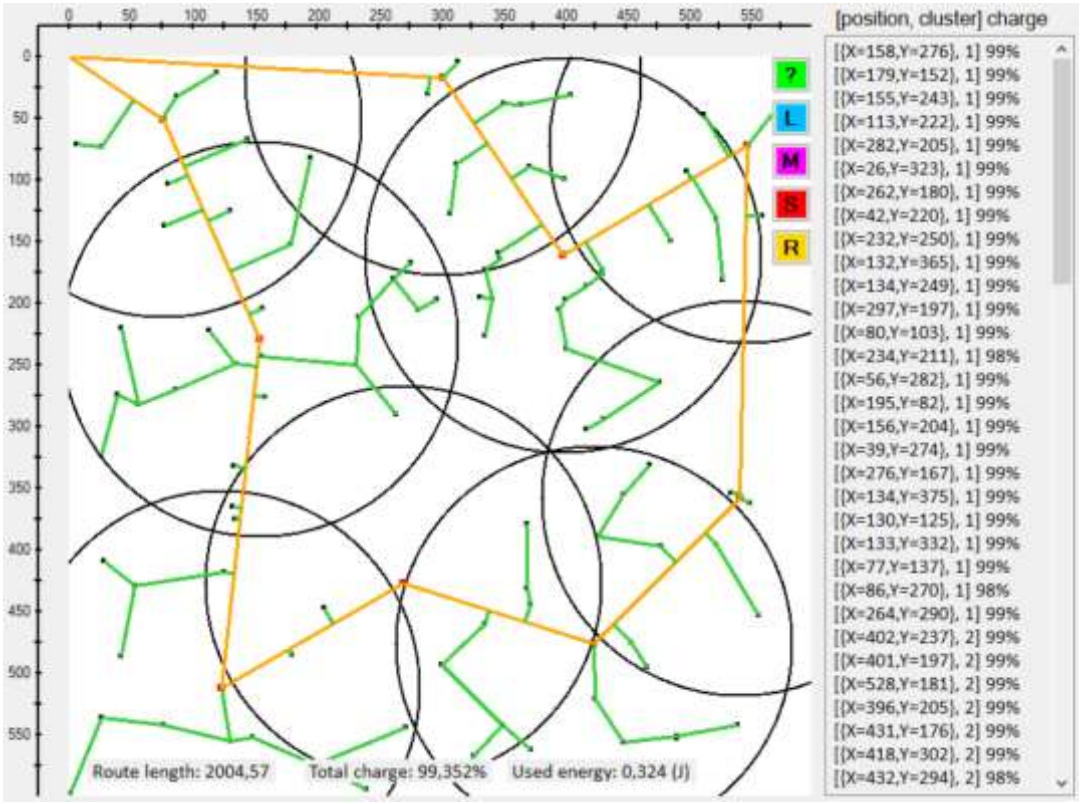
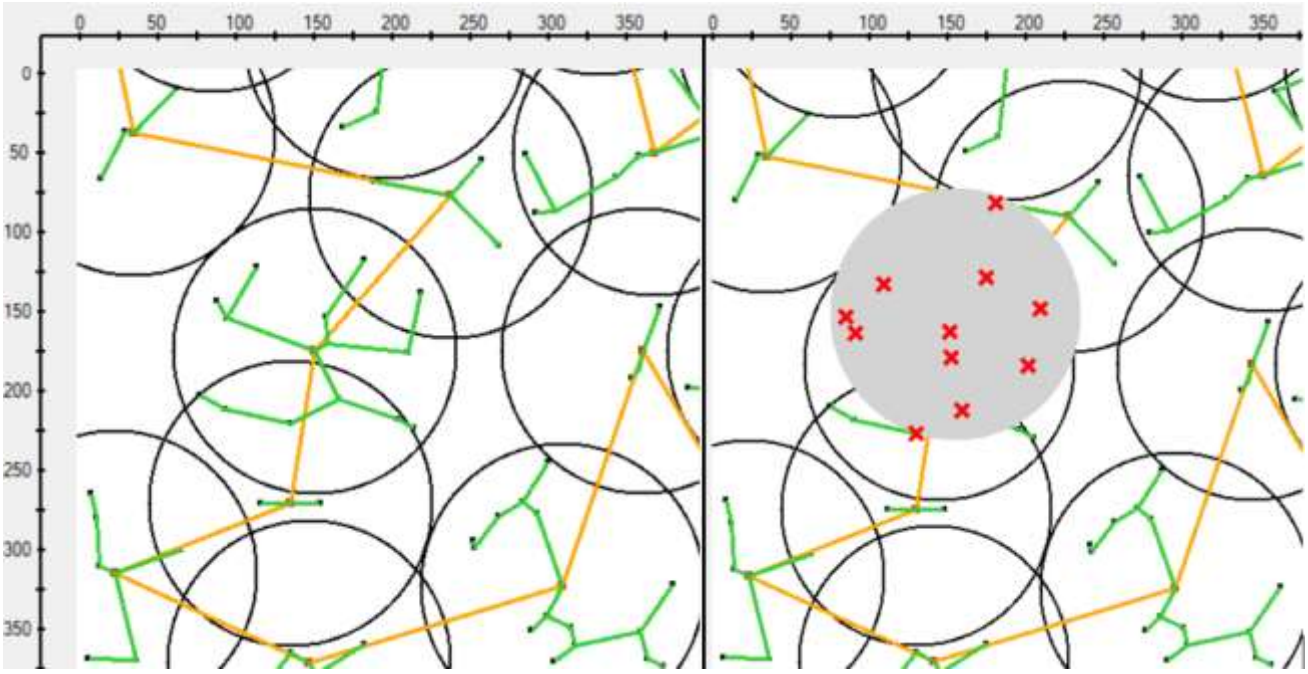


Рисунок 3.9 - Передача даних за маршрутом слідування станції за допомогою алгоритму PEGASIS



а) б)

Рисунок 3.10 – Модель мережі: а) фрагмент мережі; б) зона глушіння сигналу

Згідно логічної моделі (рис 2.9) ізолюємо ці вузли (рис. 3.11). Вузли, що знаходяться в зоні глушіння переходять в “сплячий” режим. При зникненні завад, вузли знову включаються в мережу [33].

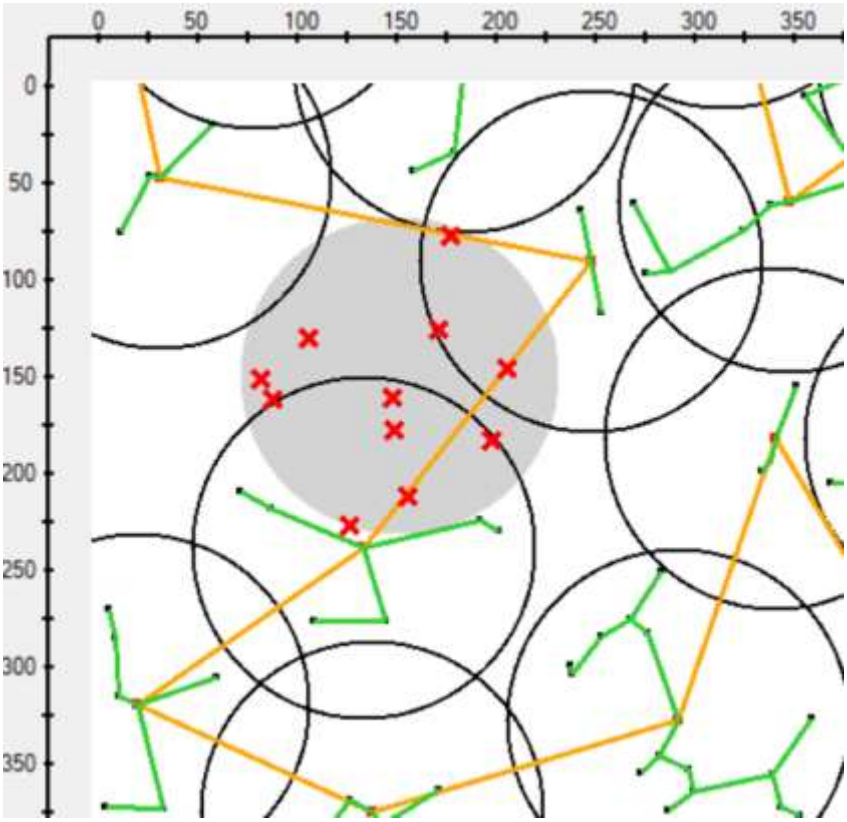


Рисунок 3.11 – Виключення вузлів в зоні глушіння з мережі

На (рис. 3.10 а) зображено початковий стан мережі, (рис. 3.10 б) створення зони глушіння, (рис. 3.11) виключення датчиків в зоні глушіння з мережі. Як можна побачити з (рис. 3.10) та (рис. 3.11) в даному випадку зона глушіння була досить велика, що призвело до видалення мережевого кластеру, а точки, що залишилися, були розподілені між сусідніми. Після зникнення завад кластер може знову відновитися а вузли продовжити свою роботу

При передачі даних алгоритмом PEGASIS може знижуватися стійкість мережі до атак на фальсифікацію маршрутної інформації. Найефективніше використання такої атаки – це зациклення пакетів в мережі [34]. Для запобігання атак такого типу, використаний дуже простий механізм побітового

додавання унікальних ідентифікаторів вузлів. Так як, ідентифікація вузлів здійснюється за їх MAC-адресою, буде доречно використати її для цього. Механізм роботи такого алгоритму наступний, при отриманні пакету, вузол зчитує MAC-адресу зазначену в пакеті та додає до MAC-адресу наступного вузла шляхом побітового додавання. Якщо результатом операції став нуль, значить наступний вузол став причиною зациклювання пакету, тоді визначається новий маршрут, а значення довіри вузла знижується (рис. 3.12).

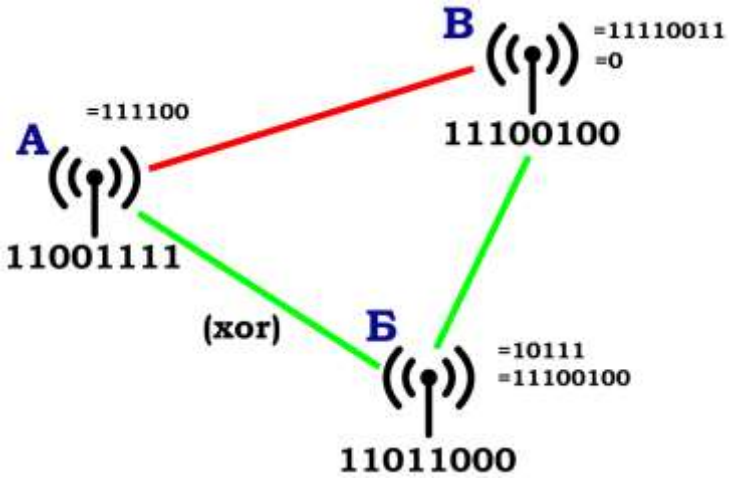


Рисунок 3.12 – Спрощена візуалізація методу запобігання зациклень

На (рис. 3.12) передача відбувається від вузла А до Б до В. Ініціатор передачі вузол А виконує її побітове додавання своєї MAC-адреси (11001111) та MAC-адресу вузла Б (11011000) і отримує результат (10111) який надсилає на вузол Б, який також виконує операцію побітового додавання з MAC-адресою вузла В (11100100) і надсилає на вузол В результат (11110011), далі така ж операція проводиться для вузла В, А і на вузлу Б ми отримуємо нульовий результат – отже пакет було зациклено вузлом В [35].

В гомогенній БСМ всі сенсорні вузли мають однакові можливості та ролі, а тому перевага такої системи може бути в тому, що концепція «списку довірених вузлів» може не застосовуватися безпосередньо. Однак управління довірою та репутацією може бути важливим для забезпечення загальної надійності та безпеки мережі. Для мереж такого типу список довірених вузлів

може бути заміщений механізмами довіри. Принцип роботи механізмів довіри полягає в тому що вузли можуть встановлювати довірчі відносини на основі їх взаємодії та спостережень за поведінкою один одного. Це може включати оцінку таких факторів, як надійність, коефіцієнт доставки пакетів і швидкість реагування. Вузли з вищими значеннями прямої довіри вважаються більш надійними. При цьому, перевага гомогенної мережі в тому, що вузлам не потрібно зберігати дані з базовими параметрами поведінки вузла, вузол просто може порівняти поведінку сусідніх вузлів зі своєю [36]. Таким чином, замість підтримки таблиць довіри кожен вузол встановлює рівні довіри для своїх безпосередніх сусідів. При зниженні значення довіри до певного рівня можуть бути задіяні механізми спільного прийняття рішень – в даному випадку це агрегація значень довіри, на основі якої приймається рішення про ізоляцію вузла (табл. 3.1).

Таблиця 3.1 – Таблиця довіри сусідніх вузлів

ID вузлів	Значення довіри до вузла
02:1A:6B:EF:8C:51	0.85
A7:9D:3F:62:E8:05	0.70
C9:BB:4F:26:13:FA	0.92
5E:83:D6:91:07:B2	0.45
F1:AC:2E:C8:9D:34	0.78
79:0F:BA:47:E6:58	0.63
Агреговане значення	0.7217

В (табл. 3.1) значення довіри до вузла були утворені при моделюванні слабкого зашумлення датчика, відповідно аномальна кількість помилок в пакетах даних призвела до зниження значення довіри цього датчика у сусідніх

вузлів. На практиці рекомендовані коефіцієнти довіри для прийняття рішення про ізоляцію вузла можуть відрізнятися залежно від конкретних системних вимог, характеристик мережі та бажаного рівня надійності. Через це, визначення граничних значень при яких до датчиків можуть бути застосовані ті чи інші обмеження слід визначати експериментально для кожної окремої фізичної моделі.

Вузли з низьким рівнем довіри можуть не тільки ізолюватися, при деяких допустимих значеннях довіри можна вживати певних заходів, обмежень щодо вузла, це може бути заборона участі в процесі передачі даних як проміжного вузла, оскільки це може наражати на небезпеку втрати пакетів, проте вузол все ще може бути джерелом інформації, також може бути застосоване обмеження в формі заборони на участь у механізмах спільного прийняття рішень, яке також може бути застосоване якщо таблиця довіри такого вузла містить дані що сильно відрізняються від тих що спостерігаються іншими датчиками [37].

3.3 Оцінка результатів тестування

При тестуванні фінальної моделі були виявлені досить цікаві результати в роботі різних моделей передачі даних. При передачі даних напряму найшвидше розряджалися ті вузли, що були далі від станції, що цілком логічно, натомість при роботі алгоритму PEGASIS, що представляє собою передачу даних через сусідні точки до станції жадібним алгоритмом розряджалися швидше вузли ті що були ближче до станції. Як вияснилося згодом при аналізі отриманих результатів, причина такої поведінки – велика кількість даних, яка передається через точки близькі до станції. Тобто, в алгоритмах з прямою передачею даних найбільші втрати енергії визначав такий показник як відстань між вузлом та станцією, натомість у алгоритмі PEGASIS цим показником є кількість даних що передається через вузол. В підсумку, такий результат може

бути дуже цікавим з точки зору балансування розряджання мережі за допомогою комбінування декількох моделей передачі. Це може бути не критичним для вузлів зі стаціонарним живленням, натомість таке балансування навантаження може бути важливим для мереж з автономним живленням, щоб не допустити перевищення швидкості розряджання вузлів над швидкістю відновлення їх заряду, як наслідок - повного розряджання таких вузлів. Цікаво зазначити, що балансування навантаження може забезпечити перекластеризація мережі, але тут грають роль декілька факторів: по-перше, процес перекластеризації мережі вимагає часу та додаткових затрат енергії для реконфігурації мережі, по-друге він не гарантує що вузли які мали велике навантаження знову не опиняться в точках найбільшого навантаження, він лише рандомізує цей процес, тому можливі втрати окремих вузлів, тоді як розглянута вище модель балансування навантаження за допомогою алгоритмів передачі дозволяє гарантовано обернути напрямок найбільшого навантаження в прямо протилежну сторону.

Також було проведено аналіз ефективності алгоритмів передачі даних на різних розмірах кластерів. Так, отримані дані були приведені до середніх значень та переведено в коефіцієнтні значення для зручності, по значенням яких побудовано графік (рис. 3.13).

На графіку (рис. 3.13) вертикальна вісь визначає коефіцієнт енергозатрат, чим він менший тим менші витрати енергії на передачу даних. За одиницю взяті енерговитрати на пряму передачу даних до центру кластеру. Нижня вісь позначає радіус кластера в метрах. Як видно з графіку, відслідковується цікава залежність в енергозатратах кожного алгоритму. Перед початком роботи очікувалось строге розходження в ефективності роботи алгоритмів, тобто такі дані, які ми маємо на графіку на радіусах кластера 150 м та більше. Натомість, отримані результати показали, що на радіусах кластера менше 150 м поведінка не така, як очікувалася, а на малих радіусах кластера (близько 50 м та менше) ефективність прямої передачі вища ніж алгоритму PEGASIS [38].

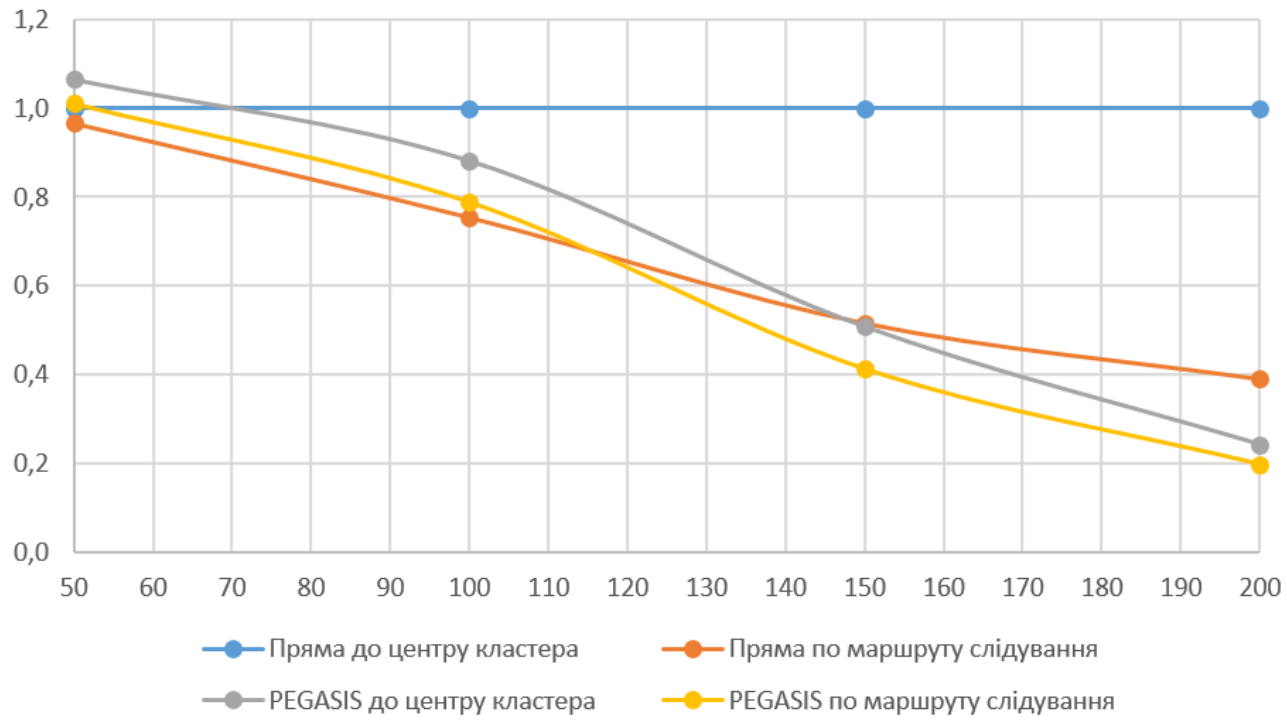


Рисунок 3.13 – Графік енергозатрат алгоритмів в залежності від розміру кластеру

Варто додати, що сенсорні вузли мають дві моделі передачі сигналу: передача без та з підсилювачем сигналу (free space model, multipath fading model), і остання модель споживає колосальну кількість енергії, настільки що датчик може розрядитися за кілька ітерацій. Датчики можуть мати різну межу переходу моделі передачі сигналу, це залежить від їх комплектації, в даній роботі я використав стандартне значення таких датчиків: 87,7 м. Тобто, на певних розмірах кластера (залежить від моделі передачі) в мережі починають з'являтися вузли, які розряджаються значно швидше через те що дальність передачі даних може бути більшою за граничне значення.

Підсумовуючи вищесказане, можна зробити висновок, що енергоспоживання мережі залежить від двох взаємопов'язаних факторів – щільності покриття мережі та радіусу кластера. Так, чим щільніше покриття, тим доцільніше використовувати алгоритм PEGASIS та збільшувати розмір кластера, і навпаки, чим менша щільність тим ефективніша пряма передача даних і тим менші кластери слід робити, щоб запобігти повному розряджанні

окремих датчиків. Це означає, що від процесу розгортання мережі, відповідно її щільності, залежить те які алгоритми і параметри будуть більш ефективними в даній конкретній ситуації. Провівши дослідження даного питання експериментальним шляхом, я рекомендую використовувати наступні параметри:

– при прямій передачі одразу враховуйте на якій висоті буде рухатися базова станція;

– при прямій передачі дальність передачі даних від крайніх точок кластера до базової станції на повинна перевищувати значення переходу датчиків на модель передачі з підсилювачем, це значення можна розрахувати за теоремою Піфагора, взявши за катети значення висоту польоту станції та граничні значення передачі сигналу без підсилювача;

– в моделі передачі PEGASIS при нерівномірній щільності покриття мережі, значення краще розраховувати як в попередньому пункті. Натомість, якщо щільність покриття такої мережі рівномірна, то можливо розрахувати ці параметри експериментально і таким чином збільшити радіуси кластерів.

Підводячи підсумки, модель мережі, що було спроєктована, є досить гнучкою так як вона може адаптуватись під щільність мережі шляхом регулювання радіусу мережевих кластерів.

3.4 Висновок

Отже, результатом даного розділу є те, що програмний продукт пройшов тестування в процесі розробки для виявлення помилок перед інтеграцією окремих компонентів у загальну систему. Тестування було поділено на два етапи: тестування розробки та фінальне тестування. Тестування на етапі розробки передбачало візуальну перевірку розгортання мережі, алгоритмів і ручних розрахунків. На цьому етапі проводилося постійне тестування,

редагування та виправлення алгоритмів. Фінальне тестування дозволило провести поглиблене тестування продукту та його компонентів, внести коригування та оцінити досягнення цілей. Також були виипробовувані алгоритми передачі даних і механізми захисту мережі. Результати показали роботу різних алгоритмів передачі даних і реакцію мережі на інциденти та атаки. Були протестовано механізми довіри мережі.

Також було проведено аналіз отриманих при тестуванні даних, зроблені висновки щодо роботи та ефективності різних моделей передачі даних. Пряма передача даних показала більш високу швидкість розряду для вузлів, розташованих далі від станції, тоді як алгоритм PEGASIS розряджав вузли, розташовані ближче до станції, швидше через велику кількість даних, що передаються через них. Було запропоновано балансування навантаження за допомогою комбінації моделей передачі даних, щоб запобігти розрядці вузла. Ефективність алгоритмів передачі даних була проаналізована на основі розмірів кластерів, і несподівані результати спостерігалися при менших радіусах кластерів.

Пряма передача показала вищу ефективність, ніж алгоритм PEGASIS при малих радіусах кластера, всупереч початковим очікуванням. Визначено що енергоспоживання мережі, що була розроблена, залежить від щільності покриття мережі та радіуса кластера.

Загалом даний розділ був зосереджений на тестуванні програмного забезпечення, механізмів довіри, аналізу алгоритмів передачі даних, алгоритмів захисту мережі та споживанні енергії в контексті моделі гомогенної мережі.

На завершення результати проведеного аналізу показали важливість тестування під час розробки програмного забезпечення, характеристики продуктивності різних алгоритмів передачі даних, роль механізмів довіри в однорідних мережах і вплив енергоспоживання мережі на розмір кластера та щільність покриття.

ВИСНОВКИ

Підводячи підсумки, можемо сказати, що в кожна з моделей БСМ має свої унікальні характеристики та комплектацію. Вибір певної моделі БСМ залежить від поставлених завдань, можливостей та вимог до такого продукту. Дана кваліфікаційна робота, в комплексі має за мету запропонувати новий варіант БСМ з унікальними характеристиками та набором компонентів, алгоритмів, систем безпеки та захисту яка може бути ефективною для вирішення специфічних завдань моніторингу та розвідки; ефективно вирішувати проблеми та поставлені задачі за певного набору вимог [39].

Дана кваліфікаційна робота пропонує новий технологічний продукт, та охоплює такі етапи його розробки, як:

1) визначення потреб і можливості розробки нового технологічного продукту;

2) проведення досліджень, пошук ідей та концепцій;

3) створення та тестування програмних моделей.

Дана робота є основою для подальшої розробки мережі, вона пропонує варіант компонування такої системи, досліджує її переваги та недоліки, особливості, проте потребує подальшого глибшого дослідження та тестування макетів, прототипів мережі; проведення аналізу на основі цих досліджень та можливо, внесення певних модифікацій чи змін у свою структуру. Саме тому в цій роботі компоненти мережі розглядаються як набір підходів, алгоритмів, що можуть бути використані та досліджується ефективність кожного з цих підходів, алгоритмів залежно від поставлених задач та вимог до мережі, ці підходи можуть бути імплементовані в систему як одиночно, так і комплексно, що дає можливість мережі динамічно змінювати свою поведінку, пристосовуючись до змін умов навколишнього середовища і збільшуючи ефективність мережі.

Підсумовуючи, цей проєкт успішно досяг своїх цілей у розробці та впровадженні рішень проблем та завдань безпеки мережі на основі дослідження та тестування алгоритмів та механізмів захисту. Шляхом ретельного тестування та оцінювання були надані конкретні докази ефективності та актуальності отриманих результатів, демонструючи їх цінність у вирішенні завдання роботи та відповідності вимогам часу. Детальні описи та супровідні графічні матеріали проілюстрували функціональність і можливості впроваджених програмних рішень і методів захисту інформації. Завдяки комплексному аналізу було продемонстровано, що розроблені рішення ефективно протидіють раніше ідентифікованим загрозам і виконують поставлені завдання, підтверджуючи їх стійкість і надійність. Цей аналіз підтверджує актуальність і практичну цінність результатів, гарантуючи їхній внесок у загальний стан науки та кібербезпеки. Крім того, була проведена ретельна оцінка ризиків безпеки, пов’язаних із самою розробкою. Ця оцінка дозволила нам виявити вразливі місця та запропонувати відповідні заходи щодо зменшення ризиків, що ще більше підвищить безпеку та стійкість реалізованих рішень [40].

На завершення, отримані результати цього проєкту є дуже актуальними, ефективними та цінними у сфері науки та безпеки безпровідних мереж, захисту інформації в безпровідних мережах. Дотримуючись вимог завдання, враховуючи та розглядаючи критичні аспекти безпеки, були розроблені рішення, що значно сприяють підвищенню загальної безпеки мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Жук О. В. Методологія управління неоднорідними безпровідними сенсорними мережами військового призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку*: Доп. та тези доп., м. Київ, 25–26 листоп. 2021 р. С. 224-225.

2. Жук О. В., Романюк В. А., Сова О. Я. Методологічні основи управління перспективними неоднорідними безпроводовими сенсорними мережами тактичної ланки управління військами. *Тези доповідей та виступів учасників IX науково-практичної конференції „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"*. Київ, 2016 р. С. 34-44.

3. Романюк А. В. Задачі управління збором даних моніторингу БПЛА в безпровідних сенсорних мережах. *Збірник наукових праць ВІТІ*, 2018, №2. С. 103-112.

4. Mohammed F., Mostafa A. Elhosseini, Mahmoud B., Hesham A. A., Hanaa Z. E.. Deployment Techniques in Wireless Sensor Networks, Coverage and Connectivity: A Survey. *IEEE Access.* 2019. Т. 7. С. 28940–28954.

5. Amin Shahraki, Amir Taherkordi, Øystein Haugen, Frank Eliassen. Clustering objectives in wireless sensor networks: A survey and research direction analysis. *ScienceDirect.* 2020. Т. 180, № 107376.

6. Wang C. Efficient Aerial Data Collection with UAV in Large-Scale Wireless Sensor Networks. *International Journal of Distributed Sensor Networks.* 2020. Т. 11, № 11. С. 28. URL: https://doi.org/10.1155/2015/286080 (дата звернення: 05.06.2023).

7. Гримуд А. Г., Романюк В. А., Степаненко Є. О. Модель тимчасової кластеризації безпроводової сенсорної мережі телекомунікаційною аероплатформою для збору даних моніторингу. *Системи і технології зв'язку,*

інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: Доп. та тези доп., м. Київ, 25-26 лист. 2021 р. С. 118-119.

8. Bharti D., Nainta N., Monga H. Performance Analysis of Wireless Sensor Networks Under Adverse Scenario of Attack. *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, м. Noida, India, 7–8 берез. 2019 р. 2019. URL: https://doi.org/10.1109/spin.2019.8711688 (дата звернення: 02.03.2023).

9. Choudhary S., Kesswani N. Detection and Prevention of Routing Attacks in Internet of Things. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications. 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, м. New York, NY, USA, 1–3 серп. 2018 р.

10. The Network Effects Bible. *Guides.co*. URL: https://guides.co/g/the-network-effects-bible/121732 (дата звернення: 16.02.2023).

11. Собчук А. В., Барабаш А. О., Кравченко Ю. В., Коваль М. О. Проблеми безпеки у функціонально стійких бездротових сенсорних мережах. *Science and Education a New Dimension. Natural and Technical Sciences*. 2019. Т. 23, № 193. С. 42-46.

12. Noman R. M., Buriro A., Mahboob A. Classification of Attacks on Wireless Sensor Networks: A Survey. *International Journal of Wireless and Microwave Technologies*. 2018. Т. 8, № 6. С. 15–39.

13. Keerthika M., Shanmugapriya D. A Systematic Survey on Various Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks (WSN). *2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, м. MANGALORE, India, 1–3 груд. 2022 р.

14. Sharma S. Classification of Security Attacks in WSNs and Possible Countermeasures: A Survey. *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, м. GOA, India, 16–19 груд. 2019 р. 2019.

15. Olivieri de Souza B. J., Endler M. Evaluating flight coordination approaches of UAV squads for WSN data collection enhancing the internet range on WSN data collection. *Journal of Internet Services and Applications.* 2020. Т. 11, № 1. URL: https://doi.org/10.1186/s13174-020-00125-4 (дата звернення: 05.06.2023).

16. Verma R., Bharti S. A Survey of Network Attacks in Wireless Sensor Networks. *Communications in Computer and Information Science.* Singapore, 2020. С. 50–63. URL: https://doi.org/10.1007/978-981-15-9671-1_4 (дата звернення: 05.03.2023).

17. Mahakud R.. Energy Management in Wireless Sensor Network Using PEGASIS. *Procedia Computer Science*. 2020. Т. 92. С. 207–212. URL: https://doi.org/10.1016/j.procs.2016.07.347 (дата звернення: 05.06.2023).

18. Heinzelman W. R. Energy-scalable algorithms and protocols for wireless microsensor networks. *International Conference on Acoustics, Speech and Signal Processing*, 2019 м. Istanbul, Turkey.

19. Гримуд А. Г. Аналіз алгоритмів пошуку найкоротшого маршруту обльоту телекомунікаційною аероплатформою кластеризованих вузлів наземної безпроводової сенсорної мережі: *І міжнародна науково-технічна конференція "Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку"* Доп. та тези доп., м. Київ, 25-26 лист. 2021 р. С. 117-118.

20. Weihuang Huang, Jeffrey Xu Yu. Investigating TSP Heuristics for Location-Based Services. *Data Sci*. Eng. March 2017. Т. 2. С. 71–93.

21. Yue W., Jiang Z. Path Planning for UAV to Collect Sensors Data Based on Spiral Decomposition. *Procedia Computer Science*. 2018. Т. 131. С. 873–879. URL: https://doi.org/10.1016/j.procs.2018.04.291 (дата звернення: 04.16.2023).

22. Xie H., Yan Z., Yao Z., Atiquzzaman M. Data collection for security measurement in wireless sensor networks: a survey. *IEEE Internet of Things Journal*. 2019 р. Т. 6, № 2. С. 2205–2224.

23. Turakulovich K. Z., Tokhirovich S. L. Analysis of Security Protocols in Wireless Sensor Networks. *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, 4–6 листоп. 2019 р.

24. Karakaya A., Akleylek S. A survey on security threats and authentication approaches in wireless sensor networks. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, м. Antalya, 22–25 берез. 2018 р.

25. Chen X. Point coverage analysis. Randomly Deployed Wireless Sensor Networks. 2020. С. 15–33. URL: https://doi.org/10.1016/b978-0-12-819624-3.00007-0 (дата звернення: 19.03.2023).

26. O'Mahony G.D., Curran J.T., Harris P.J., Murphy C.C. Interference and intrusion in wireless sensor networks. *IEEE Aerospace and Electronic Systems Magazine*. 2020. Т. 35, № 2. С. 4–16.

27. Jilani S. A., Koner C., Nandi S. Security in Wireless Sensor Networks: Attacks and Evasion. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, м. Durgapur, India, 7–8 лют. 2020 р. URL: https://doi.org/10.1109/ncetstea48365.2020.9119947 (дата звернення: 12.05.2023).

28. Dewal P., Narula G.S., Jain V., Baliyan A. Security attacks in wireless sensor networks: a survey. 2018.

29. Rault T., Bouabdallah A., Challal Y. Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*. 2014. Т. 67. С. 104–122. URL: https://doi.org/10.1016/j.comnet.2014.03.027 (дата звернення: 03.23.2023).

30. Романюк В. А., Романюк А. В., Лисенко О. І., Спаравало М. К., Жук О. В. Синтез методів збору даних телекомунікаційними аероплатформами в бездротових сенсорних мережа. *Інформаційні та телекомунікаційні науки*. 2020. № 2. С. 63–73.

31. Романюк В. А., Лисенко О. І., Романюк А. В., Жук О. В. Підвищення ефективності збору даних у кластерних бездротових сенсорних мережах з

використанням БПЛА. *Інформаційні та телекомунікаційні науки.* 2020. Вип. 11, № 1. С. 102–107.

32. AL-Shaihk N. F. A., Hassanpour R. Active Defense Strategy against Jamming Attack in Wireless Sensor Networks. *International Journal of Computer Network and Information Security.* 2019. Т. 11, № 11. С. 1–13. URL: https://doi.org/10.5815/ijcnis.2019.11.01 (дата звернення: 04.04.2023).

33. Verma R.. Countermeasures Against Jamming Attack in Sensor Networks with Timing and Power Constraints. *11th International Conference on Communication Systems & Networks (COMSNETS)*, м. Bengaluru, India, 7–11 січ. 2019 р. URL: https://doi.org/10.1109/comsnets.2019.8711437 (дата звернення: 12.03.2023).

34. Abidin S., Izhar M. Attacks on WSN and its Limitations. *International Journal of Computer Sciences and Engineering.* 2017. Т. 5, № 11. С. 158–161. URL: https://doi.org/10.26438/ijcse/v5i11.158161 (дата звернення: 07.06.2023).

35. Daniel A. D., Emalda R. S. WSN Security: An Asymmetric Encryption and Hash Function based Approach. *International Journal of Engineering Research and.* 2021. Т. V5, № 02.

36. Zhou H. A Security Mechanism for Cluster-Based WSN against Selective Forwarding. *Sensors.* 2019. Т. 16, № 9. С. 1537.

37. Johnson A. Security in Wireless Sensors Networks, *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, м. Farmingdale, NY, USA, 3 трав. 2019 р. 2019. URL: https://doi.org/10.1109/lisat.2019.8817338 (дата звернення: 27.03.2023).

38. El Ouadi M. R., Hasbi A. Comparison of LEACH and PEGASIS Hierarchical Routing Protocols in WSN. *International Journal of Online and Biomedical Engineering (iJOE).* 2020. Т. 16, № 09. С. 159. URL: https://doi.org/10.3991/ijoe.v16i09.14691 (дата звернення: 07.05.2023).

39. Zhuk O.V., Romaniuk V.A., Tkachenko D.V., Romaniuk A.V. Monitoring and telecommunications subsystems integration in the wireless

sensor networks: *Report of 4th International Scientific and Practical Conference „Problems of Infocommunications. Science and Technology / PIC S&T-2018”* Kharkiv, 2018 p. C. 334 – 338.

40. Butun I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials.* 2020. T. 22, № 1. C. 616–644.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Веремійчук Віталій Євгенович

Тема Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4; кількість сторінок записки 72.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена модель безпровідної сенсорної мережі. Ця система має вбудований захист від несанкціонованого доступу та впливу. У процесі проєктування були розроблені такі компоненти: модулі датчиків, протоколи безпеки, передачі, збору даних, модулі захисту від атак.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи наведена загальна характеристика задачі, визначені об'єкт, предмет та методи дослідження, а також сформульована мета. Зазначені задачі, що потрібно виконати для досягнення поставленої мети, проведений аналіз досліджуваної проблеми та обгрунтований підхід до її вирішення. У першому розділі проводиться аналіз предметної області та відбувається постановка задачі на створення модулі захищеної мережі. Наступні розділи присвячені проєктуванню моделі мережі, інтеграції рішень безпеки в існуючу модуль мережі, а також аналізу отриманих результатів.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у розробці моделі мережі, що має вбудований захист від несанкціонованого доступу та впливу на мережі. Результати дослідження цієї моделі можуть бути використані для створення нової системи моніторингу, яка може бути ефективною за певного набору факторів та умов, а також може мати кращу ефективність вирішення деяких завдань моніторингу, охорони та розвідки в умовах постійної загрози нападу ніж інші існуючі аналоги.

5. Негативні сторони роботи Пропонвані в роботі варіант компонування безпровідної сенсорної мережі та механізми безпеки ще потребують глибшого дослідження та тестування макетів, прототипів мережі; проведення аналізу на основі цих досліджень та можливо, внесення певних модифікацій чи змін у структуру мережі з метою покращення безпеки. Самі механізми безпеки в роботі недостатньо деталізовано.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження -

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім’я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович,
завідувач кафедри ТМІТ, доктор технічних наук, професор

«7» 06 2023. (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ
КАФЕДРИ КІБЕРБЕЗПЕКИ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу

Автор: Веремійчук Віталій Євгенович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. 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 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.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 93,12%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 6.88%, з яких 1.5% є збігами з одним джерелом, зумовленими наявністю типових шаблонів титульної сторінки і рамок пояснювальної записки.

2. Інші збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань, складових стандартних фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.

Керівник роботи  В. М. Чешун

Завідувач кафедри кібербезпеки Ю. П. Кльоц

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015535605

Дата перевірки:
09.06.2023 16:39:19 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.06.2023 16:42:43 EEST

ID користувача:
100008300

Назва документа: **Веремійчук**

Кількість сторінок: **72** Кількість слів: **12986** Кількість символів: **98904** Розмір файлу: **1.67 MB** ID файлу: **1015188645**

6.88%
Схожість

Найбільша схожість: **1.5%** з джерелом з Бібліотеки (ID файлу: **1015188646**)

6.27% Джерела з Інтернету	384	Сторінка 74
3.04% Джерела з Бібліотеки	50	Сторінка 77

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0.05%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за **8 слів** та **0%**)

0% Вилучення з Інтернету	20	Сторінка 78
0.05% Вилученого тексту з Бібліотеки	44	Сторінка 78

Модифікації

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

Замінені символи	2

Fri Jun 09 15:34:24 EEST 2023, Мостовий Сергій Володимирович, 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: 9%**

ID: 115474 Назва: Бездротова сенсорна мережа військового призначення із захистом від несанкціонованого доступу та впливу Додано в БД: 2023-06-09 Автора: Веремійчук В.Є. Керівники: Чешун В.М. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	74920	1173	1102 (1%)	17 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми