ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНИХ ГЕТЕРОГЕННИХ СЕНСОРНИХ МЕРЕЖ»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»

(шифр і назва спеціальності)

Довгалюк М.О.

(прізвище та ініціали)

Керівник Довженко Н.М.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтролер Чумак Н.С.

(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Безпроводові сенсорні мережі (БСМ) розглядають як один із найважливіших сучасних напрямів розвитку технологій у двадцять першому столітті. У минулому десятилітті ідея безпроводових сенсорних мереж здобула велике визнання в науковому світі та промисловості. Базова ідея БСМ - це відмова від безпосередньої участі людини в зборі інформації, наприклад, у зв'язку з неможливістю присутності людей у конкретному місці або за реалізації технологічного процесу.

Концепція безпроводових сенсорних мереж привертає увагу вчених, науково-дослідних інститутів та комерційних організацій, що зумовлено широкими можливостями застосування сенсорних мереж. Безпроводові сенсорні мережі, зокрема, можуть використовуватися для контролю відмови обладнання в аерокосмічних системах та в системах автоматизації будівель. Через свою здатність до самоорганізації, автономності та високої відмовостійкості такі мережі активно застосовуються в системах безпеки та військових додатках. Успішне застосування безпроводових сенсорних мереж у медицині для моніторингу здоров'я пов'язане з розробкою біологічних сенсорів, сумісних з інтегральними схемами сенсорних вузлів. Але найбільшого поширення безпроводові сенсорні мережі набули у сфері моніторингу довкілля та живих істот.

Об’єкт дослідження – безпроводові сенсорні мережі.

Предмет дослідження – методи побудови захищених гетерогенних сенсорних мереж

Мета роботи – розроблення рекомендацій щодо побудови захищених гетерогенних сенсорних мереж із використаням симуляторів

Завдання бакалаврської роботи:

– проаналізувати сучасний стан в галузі досліджень БСМ;

– визначити найважливіші характеристики та структури безпроводових сенсорних мереж;

– дослідити існуючі алгоритми маршрутизації, самоорганізації та вибору головного вузла кластера в БСМ;

– виокремити характеристики моделей довіри та репутації БСМ з використанням програми TRMSim –WSN 5.0;

– розробити рекомендації щодо протидій атакам на БСМ.

Методи дослідження – опрацювання технічної літератури за даною темою, аналіз експлуатаційної документації інструментів, порівняльний аналіз сервісів.

Практичне значення одержаних результатів: рекомендації щодо побудови захищених гетерогенних сенсорних мереж можуть бути використані у сфері забезпечення кібербезпеки у персональних та корпоративних інформаційних системах.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ СТРУКТУРИ ТА ФУНКЦІОНУВАННЯ БСМ

1.1 Основні поняття та принципи сенсорних мереж

Безпроводова сенсорна мережа (БСМ) – це мережа розгорнутих у великій кількості безпроводових вузлів, яка використовується для моніторингу систем Визначено основні поняття сенсорних мереж:

- Сенсор - пристрій, який виявляє та вимірює фізичні чи хімічні властивості навколишнього середовища чи системи та перетворює їх на електричний сигнал або інший вихідний сигнал, що можна зчитувати.
- Актуатор - це компонент, який відповідає за перетворення цифрових сигналів, отриманих від сенсорних вузлів, у фізичну дію чи рух.
- Сенсорний вузол - це пристрій, оснащений датчиками, які можуть виявляти різні типи параметрів навколишнього середовища, такі як температура, вологість, світло, тиск і звук.

Сенсорні вузли використовуються в БСМ із вбудованим процесором, який керує та контролює середовище в певній зоні. Вони підключені до базової станції, яка діє як блок обробки в системі БСМ. Базова станція в системі підключена через Інтернет для обміну даними.

Кожен сенсорний вузол зазвичай містить датчик, мікроконтролер, модуль безпроводового зв’язку та джерело живлення. Датчики збирають дані з навколишнього середовища, мікроконтролер обробляє та аналізує дані, модуль бездротового зв’язку передає дані на інші вузли або на базову станцію, а джерело живлення забезпечує енергією вузол [1].

На рисунку 1.1 представлено основні дії, що виконуються при роботі сенсорних мереж.

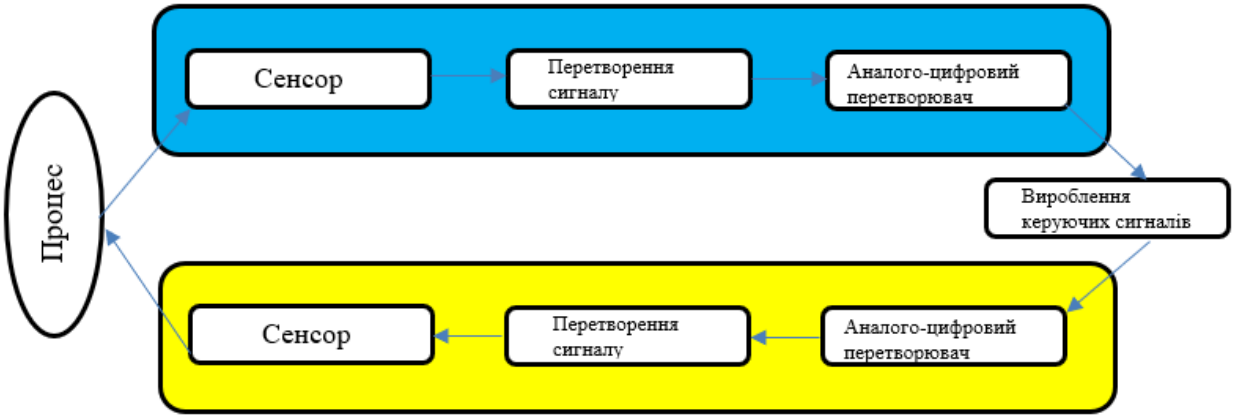

Рис. 1.1. Збір даних і управління в сенсорних мережах

Сама мережа визначає оптимальний маршрут руху інформаційних потоків, що зображено на рисунку 1.2

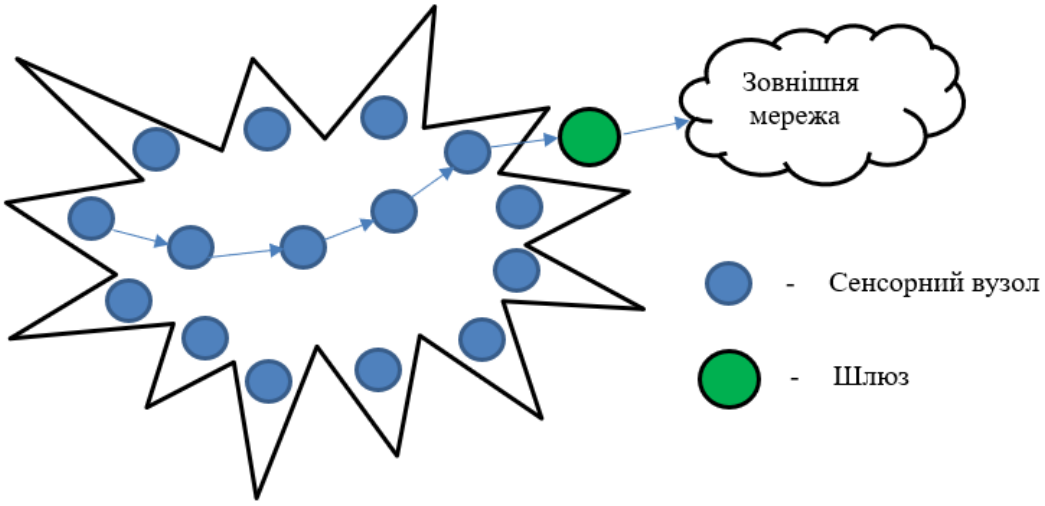

Рис. 1.2. Маршрутизація інформації в сенсорній мережі

Сенсорні мережі використовують протоколи маршрутизації, щоб визначити, як дані передаються між вузлами в мережі. Також ці мережі використовують методи агрегації даних, щоб об’єднати дані з кількох вузлів і зменшити обсяг даних, які необхідно передати. Це може допомогти зберегти енергію та зменшити мережевий трафік. Ці концепції є ключовими для проектування та роботи сенсорних мереж, і вони мають вирішальне значення для забезпечення

ефективності сенсорних мереж у моніторингу та зборі даних із фізичного середовища [1].

1.2 Характеристика вузлів БСМ

У БСМ вузли [2] є основою мережі, які відповідають за визначення, обробку та передачу даних безпроводовим способом. Вузли, як правило, є невеликими та малопотужними пристроями, призначеними для роботи в жорстких і віддалених середовищах. Габаритні розміри сенсорного вузла кілька квадратних сантиметрів.

Кожен сенсорний вузол у безпроводовій сенсорній мережі зазвичай містить кілька компонентів:

- Сенсорний блок: цей блок відповідає за вимірювання фізичних або екологічних умов. Наприклад, датчик температури, датчик вологості або датчик освітленості.
- Блок обробки: цей блок відповідає за обробку даних, зібраних датчиком, і виконання деяких локальних обчислень, таких як стиснення даних, вилучення функцій або виявлення подій.
- Комунікаційний блок: цей блок відповідає за передачу та прийом даних між сенсорними вузлами та базовою станцією чи шлюзом. Безпроводові сенсорні вузли зазвичай використовують технології безпроводового зв’язку малого радіусу дії, такі як Wi-Fi, Bluetooth, Zigbee або LoRa.
- Блок живлення: цей блок відповідає за забезпечення необхідного живлення інших компонентів сенсорного вузла. Безпроводові сенсорні вузли зазвичай використовують батареї або методи збору енергії для генерування або зберігання енергії.
- Блок пам’яті: цей блок відповідає за зберігання даних, зібраних датчиком, і результатів блоку обробки. БСМ зазвичай мають обмежений обсяг пам’яті, тому керування даними та оптимізація зберігання є важливими питаннями в таких мережах.

Сенсорні вузли складаються з двох основних областей: програмна платформа і апаратна архітектура. Програмна платформа складається здебільшого з операційної системи, яка керує сенсорним вузлом. З іншого боку, апаратна архітектура підтримує процедури вимірювання.

Таким чином, апаратна частина вузла безпроводової мережі може бути розділена на чотири основні підсистеми [2], що зображені на рисунку 1.3

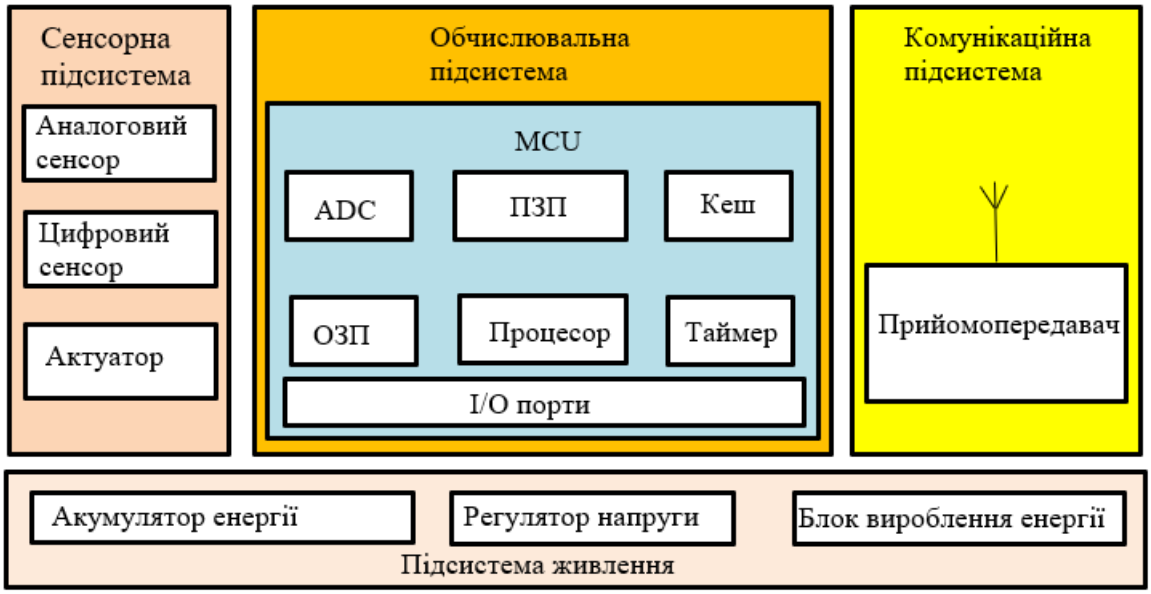

Рис. 1.3. Вузол БСМ

Ці підсистеми включають:

- Сенсорна підсистема: відповідає за збір даних із навколишнього середовища за допомогою одного або кількох сенсорів. Підсистема датчиків може включати аналого-цифрові перетворювачі, схеми обробки сигналів та інші компоненти, необхідні для взаємодії з датчиками.
- Обчислювальна підсистема: відповідає за обробку даних, зібраних сенсорною підсистемою. Може включати мікроконтролер або інший процесор, а також пам’ять і накопичувач для зберігання даних і виконання алгоритмів.
- Комунікаційна підсистема: відповідає за передачу даних між вузлами в мережі та з базовою станцією. Може включати радіопередавач, антени та протоколи для безпроводового зв’язку.

- Підсистема живлення: відповідає за живлення вузла. Може включати батарею, схеми збору енергії та схеми керування живленням для оптимізації енергоспоживання.

Також окрім основних є три додаткові підсистеми:

- Підсистема локалізації: відповідає за визначення розташування вузла в мережі.
- Підсистема безпеки: відповідає за забезпечення безпеки та конфіденційності даних, що передаються вузлом.
- Підсистема інтерфейсу користувача: Ця підсистема відповідає за надання інтерфейсу користувача для взаємодії з вузлом.

Вузли безпроводової сенсорної мережі часто використовують спеціалізовані операційні системи [3], які розроблені як легкі та ефективні, щоб зберегти обмежені обчислювальні ресурси та джерело живлення вузла. Деякі поширені ОС, які використовуються для вузлів БСМ, включають:

TinyOS — це ОС з відкритим кодом, спеціально розроблена для вузлів WSN. Дуже модульна і легка, містить набір стандартизованих компонентів і бібліотек для програмування сенсорних мереж.

Contiki — ще одна ОС з відкритим вихідним кодом, розроблена для систем з низьким енергоспоживанням і обмеженою пам’яттю. Включає підтримку кількох протоколів зв’язку та пропонує різноманітні мережеві функції.

RIOT — це легка операційна система реального часу, розроблена для Інтернету речей (IoT) і БСМ. Забезпечує підтримку широкого спектру мікроконтролерів і пропонує кілька мережевих і комунікаційних протоколів.

FreeRTOS — це ОС реального часу, яка забезпечує невелике ефективне ядро для вбудованих систем. Включає підтримку кількох мікроконтролерів і надає широкий спектр функцій, включаючи комунікаційні та мережеві протоколи.

mbed OS — це модульна ОС з відкритим кодом, розроблена для пристроїв IoT, включаючи вузли БСМ. Вона пропонує підтримку кількох протоколів зв’язку та містить низку функцій для керування енергоспоживанням і підключенням до мережі.

Ці ОС надають особливості і функціональні можливості, спеціально розроблені для вузлів БСМ, включаючи підтримку режимів низького споживання, ефективних протоколів зв’язку, а також спеціалізованих бібліотек і компонентів для керування даними датчиків.

У БСМ є кілька видів вузлів, які виконують різні функції та мають різні можливості. Ось деякі з найпоширеніших видів вузлів:

- Вузли шлюзу: використовуються для підключення БСМ до інших мереж або Інтернету. Зазвичай вони мають потужніші процесори та комунікаційні модулі, ніж сенсорні вузли, і вони відповідають за маршрутизацію даних між БСМ і зовнішніми мережами.
- Голови кластера: відповідають за агрегування та обробку даних з інших вузлів у кластері.
- Вузли-приймачі: використовуються для збору даних із БСМ і надсилання їх до зовнішніх мереж або пристроїв зберігання.
- Вузли ретрансляції: використовуються для розширення діапазону БСМ шляхом пересилання даних між вузлами. Вони також можуть використовуватися для забезпечення резервування та підвищення надійності мережі.
- Вузли виконавчих механізмів:можуть активувати або контролювати фізичні пристрої на основі даних, зібраних вузлами датчиків.

Кожен вид вузла має свої власні унікальні можливості та обов’язки в рамках БСМ. Вибір виду вузла залежить від вимог програми, топології мережі та обмежень ресурсів. Тому є три типи обов’язкових вузлів в будь-якій сенсорній мережі. Типова архітектура БСМ включає три типи вузлів що зображено на рисунку 1.4.

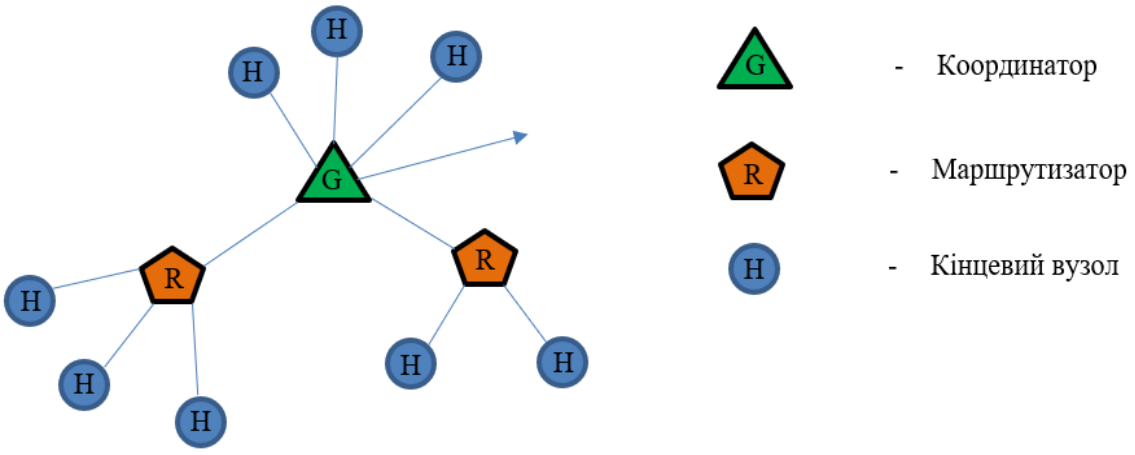

Рис. 1.4. Типова архітектура БСМ

Вузол-координатор - відповідає за керування загальною роботою мережі, включаючи контроль доступу до мережі, маршрутизацію даних між вузлами та забезпечення надійного зв’язку.

Маршрутизатор - це пристрій, який діє як міст між кількома вузлами в мережі

Кінцевий вузол –відповідає за збір даних із середовища та передачу їх іншим вузлам у мережі.

1.3 Типові архітектури і топології БСМ

Стандартизація сенсорних мереж має важливе значення для забезпечення інтероперабельності, сумісності та надійності сенсорних пристроїв і мереж. Кілька міжнародних організацій: ISO (Міжнародна організація зі стандартизації), IEC (Міжнародна електротехнічна комісія), IEEE (Інститут інженерів з електротехніки та електроніки), беруть активну участь у стандартизації сенсорних мереж [4].

Один із напрямів стандартизації був ініційований Дослідницькою групою з сенсорних мереж (SGSN) Міжнародного союзу електрозв'язку (ITU). SGSN визначила базову архітектуру сенсорної мережі , яка включає наступні компоненти:

- Сенсорні вузли.
- Поглинаючі вузли: Це базові станції, які збирають дані з сенсорних вузлів і передають їх у внутрішні системи.

- Мережевий рівень: Цей рівень включає протоколи маршрутизації, механізми безпеки та функції управління, які забезпечують ефективну та надійну передачу даних з датчиків.
- Прикладний рівень: Цей рівень включає в себе програмне забезпечення, яке обробляє та аналізує дані датчиків для різних застосувань, таких як моніторинг навколишнього середовища, охорона здоров'я, промислова автоматизація і так далі.
- Внутрішні системи: Це сервери і бази даних, які зберігають, обробляють і аналізують дані датчиків, отримані з вузлів поглинання. Базову архітектуру сенсорної мережі та її основні інтерфейси, що показано на рисунку 1.5.

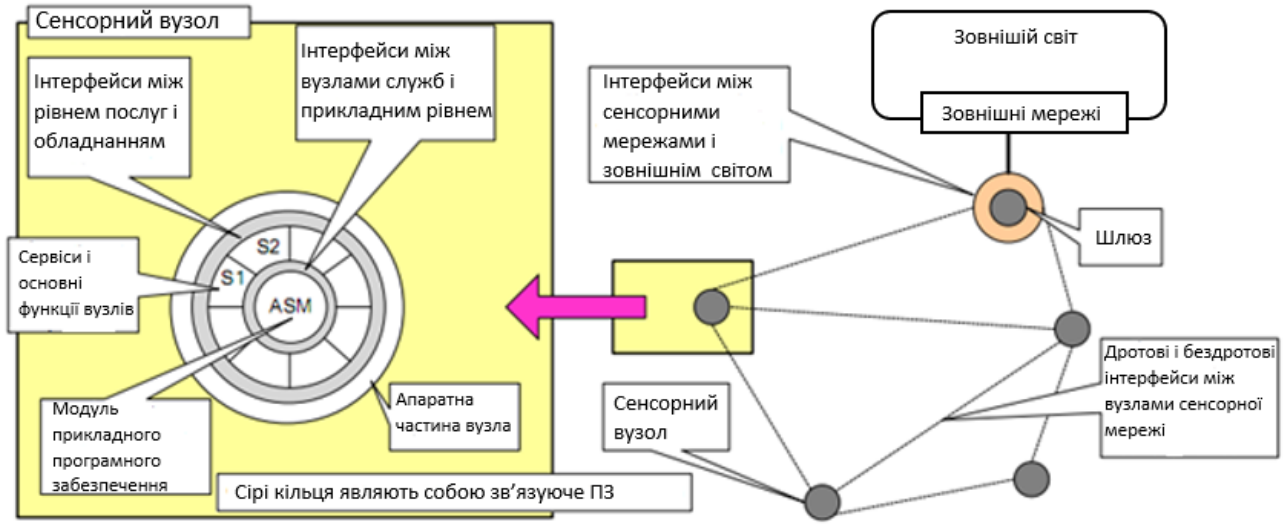

Рис. 1.5. Основні елементи сенсорної мережі

Проактивний і реактивний - це два підходи до проектування і управління БСМ, засновані на тому, як вони реагують на події і зміни в навколишньому середовищі [5].

- При проактивному підході мережа призначена для безперервного моніторингу та збору даних з датчиків, навіть якщо в навколишньому середовищі не відбувається ніяких подій або змін. Цей підхід підходить для застосувань, де дані є критично важливими і необхідний своєчасний аналіз. Проактивні мережі можуть виявляти події заздалегідь і вживати відповідних заходів, таких як оповіщення, налаштування параметрів датчиків або зміна топології мережі.

- При реактивному підході мережа розроблена таким чином, щоб реагувати тільки на події або зміни в навколишньому середовищі. Цей підхід підходить для застосувань, де дані не є критично важливими, і немає необхідності в постійному моніторингу датчиків. Реактивні мережі БСМ економлять енергію, занурюючи датчики в сплячий режим, коли немає активності, і пробуджуючи їх, коли відбувається якась подія. Тоді мережа реагує на подію, збираючи і передаючи відповідні дані. Як проактивний, так і реактивний підходи мають свої переваги і недоліки, і вибір підходу залежить від конкретних вимог застосування. Проактивні мережі забезпечують безперервний моніторинг і аналіз в режимі реального часу, але вони споживають більше енергії і вимагають більше ресурсів. Реактивні БСМ економлять енергію і ресурси, але можуть не забезпечувати своєчасний аналіз або виявлення подій.

Однорангова (P2P) та ієрархічна - це дві архітектури організації та управління БСМ, що базуються на структурі зв'язку та управління [6].

- В архітектурі P2P всі вузли мережі мають однаковий статус, і кожен вузол може безпосередньо спілкуватися з будь-яким іншим вузлом мережі. P2P БСМ підходять для додатків, де вузли розподілені випадковим чином, і немає центрального управління або координації. Кожен вузол в мережі може виступати в ролі приймача або джерела, а дані можуть передаватися декількома шляхами до вузла-джерела. P2P-мережі більш стійкі до збоїв і можуть адаптуватися до змін у топології мережі.

- В ієрархічній архітектурі вузли в мережі організовані в різні рівні або яруси на основі їх функцій і обов'язків. Кожен рівень відіграє певну роль в мережі, і вузли кожного рівня взаємодіють тільки з вузлами сусідніх рівнів. Ієрархічні мережі БСМ підходять для застосувань, де є потреба в централізованому контролі і координації, наприклад, в промислової автоматизації або в додатках для інтелектуальних електромереж. Вузли вищого рівня виступають в ролі поглиначів і відповідають за збір і обробку даних з вузлів нижчого рівня. P2P-мережі є більш гнучкими і стійкими, але вони можуть вимагати більше ресурсів і ними складніше керувати. Ієрархічні мережі БСМ простіші в управлінні і забезпечують

централізований контроль, але вони можуть бути менш стійкими і менш пристосованими до змін у топології мережі. Однорангову та ієрархічну мережу показано на рисунку 1.6.

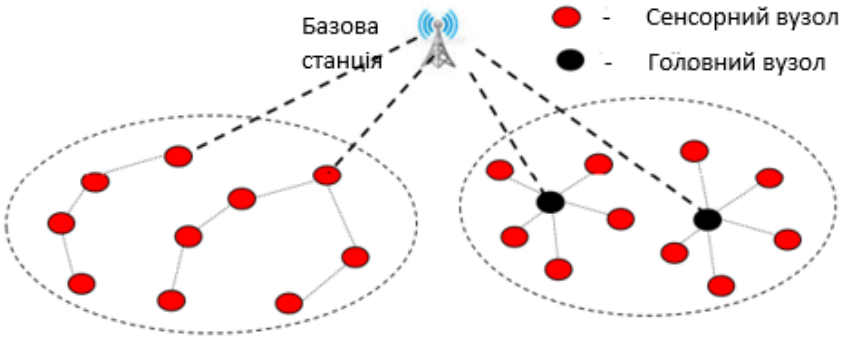

Рис.1.6. Однорангова та ієрархічна мережа

Випадкове і детерміноване розміщення - це два підходи до розгортання сенсорних вузлів БСМ, засновані на тому, як сенсорні вузли розподілені в мережі.

- Випадкове розміщення: При випадковому розміщенні сенсорні вузли розподіляються в мережі випадковим чином без будь-якого заздалегідь визначеного розташування або структури. Цей підхід підходить для застосувань, де область моніторингу велика і сенсорні вузли можуть бути легко розподілені в навколишньому середовищі, наприклад, для моніторингу навколишнього середовища або в сільському господарстві. Перевага випадкового розміщення полягає в тому, що його просто і легко розгортати, і воно забезпечує рівномірне покриття території. Однак, випадкове розміщення може призвести до нерівномірної щільності вузлів і покриття, а деякі області можуть бути недостатньо або надмірно охоплені вибіркою.
- Детерміноване розміщення: При детермінованому підході вузли датчиків розміщуються в заздалегідь визначених місцях або структурах на основі певного критерію, такого як покриття, зв'язок або енергоефективність. Цей підхід підходить для застосувань, де область моніторингу невелика або існують специфічні вимоги до топології мережі, наприклад, в промислової автоматизації або в додатках для розумного будинку. Перевага детермінованого розміщення полягає в тому, що воно забезпечує структуровану і оптимізовану топологію

мережі, яка може максимізувати покриття, зв'язок і енергоефективність. Однак детерміноване розміщення може вимагати більше ресурсів і планування, а також не може бути адаптоване до змін у навколишньому середовищі. Випадкове розміщення забезпечує простоту і рівномірне покриття, в той час як детерміноване розміщення забезпечує структуру і оптимізацію. Вибір підходу до розміщення також впливає на дизайн і продуктивність мережі, наприклад, на протокол маршрутизації, споживання енергії та агрегацію даних [7].

Стаціонарні та мобільні - це два типи сенсорних вузлів, які використовуються в БСМ на основі їх мобільності та розташування [8].

- Стаціонарні сенсорні вузли: У стаціонарній БСМ сенсорні вузли закріплені в певному місці і не рухаються. Це підхід для застосувань, де область, що підлягає моніторингу, є статичною, наприклад, моніторинг стану конструкцій або моніторинг навколишнього середовища. Стаціонарні сенсорні вузли прості і легко розгортаються, і вони забезпечують стабільний і безперервний моніторинг навколишнього середовища. Однак стаціонарні сенсорні вузли можуть бути не в змозі зафіксувати динамічні зміни або події в навколишньому середовищі, і їм можуть знадобитися додаткові вузли для покриття більшої площі.
- Мобільні сенсорні вузли: У мобільних БСМ сенсорні вузли оснащені можливостями мобільності, такими як мобільні приводи або безпілотні літальні апарати (БПЛА), для переміщення по території, що підлягає моніторингу. Цей підхід підходить для застосувань, коли територія, що підлягає моніторингу, є динамічною або важкодоступною, наприклад, при проведенні пошуково-рятувальних операцій або військового спостереження. Однак мобільні сенсорні вузли потребують додаткових ресурсів і енергії для переміщення, а також можуть бути складнішими в управлінні та контролі.

Стаціонарні сенсорні вузли забезпечують стабільний і безперервний моніторинг, в той час як мобільні сенсорні вузли забезпечують більш повне покриття і гнучкість. Вибір типу сенсорного вузла також впливає на дизайн і продуктивність мережі, такі як протокол зв'язку, споживання енергії та збір даних.

Двовимірні (2D) і тривимірні (3D) БСМ відносяться до фізичного розташування і топології сенсорних вузлів в мережі [9].

- Двовимірні БСМ: У двовимірній БСМ сенсорні вузли розміщуються у двовимірній площині, наприклад, на поверхні землі або на плоскій поверхні. Цей підхід підходить для застосувань, де область моніторингу є плоскою поверхнею, наприклад, в екологічному моніторингу, моніторингу дорожнього руху або точному сільському господарстві. 2D WSN відносно прості і легкі в розгортанні, і вони забезпечують хороше покриття території. Однак 2D-мережі можуть бути непридатними для застосування там, де навколишнє середовище має перепади висот або топографію.
- Тривимірні БСМ: У 3D БСМ сенсорні вузли розгортаються в тривимірному просторі, наприклад, в будівлі, під землею або в повітрі. Цей підхід підходить для застосувань, де область моніторингу має складну структуру або перепади висот, наприклад, для моніторингу стану конструкцій, підземного видобутку корисних копалин або повітряного спостереження. 3D-мережі можуть забезпечити більш повне покриття території і фіксувати динамічні зміни в навколишньому середовищі. Однак розгортання 3D-мереж може вимагати більше ресурсів і планування, а також вони можуть бути складнішими в управлінні і контролі.

2D БСМ прості і підходять для плоских поверхонь, в той час як 3D БСМ складніші, але підходять для складних структур або різних висот. Вибір топології мережі також впливає на дизайн і продуктивність мережі, такі як протокол маршрутизації, енергоспоживання і агрегація даних.

Гомогенні та гетерогенні - це два типи БСМ, засновані на схожості або відмінності сенсорних вузлів у мережі [10].

- Однорідні БСМ: В однорідній БСМ всі сенсорні вузли мають однакові апаратні та програмні можливості і виконують однакові завдання. Цей підхід підходить для застосувань, де завдання зондування є простими і однорідними, наприклад, вимірювання температури або вологості. Однорідні БСМ відносно легко розгортати і керувати ними, і вони забезпечують єдине уявлення про

навколишнє середовище. Однак однорідні мережі можуть не підходити для застосувань, де завдання зондування різноманітні або вимагають різних рівнів обчислювальної потужності або енергоспоживання.

- Гетерогенні БСМ: У гетерогенних БСМ сенсорні вузли мають різні апаратні та програмні можливості і виконують різні завдання. Цей підхід підходить для застосувань, де завдання зондування є складними або різноманітними, наприклад, в мультимедійному зондуванні, відстеженні об'єктів або моніторингу навколишнього середовища. Гетерогенні БСМ можуть забезпечити більш комплексні і точні можливості зондування і можуть вирішувати складні завдання, які вимагають різних рівнів обчислювальної потужності або енергоспоживання. Однак гетерогенними БСМ складніше керувати і вони вимагають більше ресурсів для розгортання. Гомогенні БСМ прості і підходять для однорідних завдань зондування, в той час як гетерогенні БСМ більш складні, але забезпечують більш комплексні і точні можливості зондування. Вибір типу мережі також впливає на дизайн і продуктивність мережі, такі як обробка і агрегація даних, споживання енергії і протокол зв'язку.

1.4 Класифікація та аналіз алгоритмів маршрутизації БСМ

Вибір алгоритму маршрутизації для БСМ залежить від різних факторів, таких як розмір мережі, топологія та вимоги додатків. Основні фактори, які можуть вплинути на вибір алгоритму маршрутизації:

- Розмір мережі: Розмір БСМ може суттєво впливати на вибір алгоритму маршрутизації. Наприклад, проактивні алгоритми маршрутизації, такі як DSDV і OLSR, можуть підходити для невеликих мереж БСМ, в той час як реактивні алгоритми маршрутизації, такі як AODV і DSR, можуть бути більш підходящими для великих мереж БСМ.
- Топологія мережі: Топологія БСМ також відіграє важливу роль у виборі алгоритму маршрутизації. Наприклад, ієрархічні алгоритми маршрутизації, такі як LEACH, ідеально підходять для кластерних топологій, в той час як

географічні алгоритми маршрутизації, такі як Greedy Perimeter Stateless Routing (GPSR), підходять для мереж з відомим розташуванням вузлів.

- Тип трафіку: Тип трафіку в БСМ також може впливати на вибір алгоритму маршрутизації. Наприклад, трафік реального часу, такий як аудіо та відео, може вимагати алгоритму маршрутизації з низькою затримкою, в той час як трафік не реального часу, наприклад, збір даних, може вимагати алгоритму з високою пропускною здатністю.
- Споживання енергії: Енергоспоживання БСМ є вирішальним фактором, який слід враховувати при виборі алгоритму маршрутизації. Енергоефективні алгоритми маршрутизації, такі як Low Energy Adaptive Clustering Hierarchy (LEACH) і Power-Efficient Gathering in Sensor Information Systems (PEGASIS), можуть продовжити термін служби БСМ.
- Безпека: Вимоги безпеки БСМ також можуть впливати на вибір алгоритму маршрутизації. Алгоритми безпечної маршрутизації, такі як безпечна ієрархічна агрегація в мережі (SHIA) і безпечна географічна маршрутизація (SGR), можуть захистити БСМ від різних загроз безпеки, таких як компрометація вузлів і підробка даних.

У моделі прямого зв'язку для БСМ кожен сенсор може безпосередньо зв'язуватися з будь-яким іншим сенсором в мережі. Ця модель передбачає, що всі датчики мають однаковий діапазон зв'язку і можуть спілкуватися один з одним без будь-яких проміжних вузлів, використовуючи зв'язок з одним переходом.

Модель прямого зв'язку [11] проста і ефективна для невеликих БСМ, де всі датчики знаходяться в зоні досяжності один одного. Однак, для великих мереж прямий зв'язок може бути неможливим через обмежений радіус дії сенсорів та енергетичні обмеження мережі. У таких випадках потрібні алгоритми багатохопової маршрутизації (проактивні та реактивні) для пересилання даних до місця призначення через проміжні вузли. Алгоритми маршрутизації, що використовуються, як правило, є проактивними, оскільки маршрути попередньо обчислюються, і вузлам не потрібно відкривати новий маршрут для кожної передачі даних. Прикладами проактивних алгоритмів маршрутизації є протокол

векторної маршрутизації з визначенням відстані (DVRP), протокол маршрутизації з оптимізацією стану каналу (OLSR) і протокол векторної маршрутизації з визначенням відстані до пункту призначення (DSDV). На рисунку 1.7 зображено принцип прямого зв'язку.

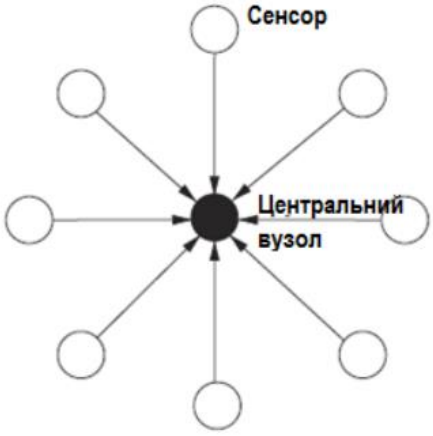

Рис.1.7. Модель прямого зв’язку

Тим не менше, більшість БСМ складаються з великої кількості сенсорних вузлів, які покривають масштабну територію, що потребує використання непрямого зв'язку [11], що показано на рисунку 1.8.

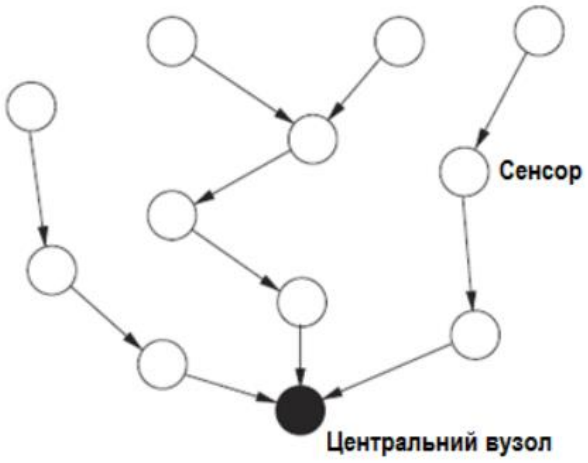

Рис.1.8. Модель непрямого зв’язку

У моделі непрямого зв'язку для БСМ датчики не можуть напряму зв'язуватися з усіма іншими датчиками в мережі. Замість цього вони повинні використовувати проміжні вузли для пересилання своїх даних до місця призначення.

У моделі непрямого зв'язку датчики покладаються на алгоритми багатохопової маршрутизації для пересилання своїх даних через проміжні вузли, щоб досягти місця призначення. Проміжні вузли діють як реле, пересилаючи дані на інші вузли, поки вони не досягнуть місця призначення. Вибір проміжних вузлів визначається алгоритмом маршрутизації, який обирає найбільш підходящий шлях на основі таких факторів, як споживання енергії, якість зв'язку та відстань.

Модель непрямого зв'язку має кілька переваг над моделлю прямого зв'язку. Наприклад, вона дозволяє розгортати більш масштабні БСМ, оскільки датчики можуть зв'язуватися з більшою кількістю вузлів через проміжні вузли. Крім того, вона забезпечує відмовостійкість, оскільки дані можуть бути перенаправлені через альтернативні шляхи, якщо вузол виходить з ладу. Однак модель непрямої комунікації також має деякі недоліки. Наприклад, вона збільшує затримку зв'язку та споживання енергії через необхідність пересилання даних через проміжні вузли. Крім того, проміжні вузли можуть бути перевантажені, що призводить до втрати пакетів і зниження продуктивності мережі.

Існує кілька алгоритмів маршрутизації, розроблених для непрямої моделі зв'язку, в тому числі Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) і Destination-Sequenced Distance Vector (DSDV). Ці алгоритми використовують різні методи, такі як переповнення, виявлення маршруту і обслуговування маршруту, щоб забезпечити ефективну передачу даних через мережу.

1.5 Гетерогенна модель для БСМ

Показники якості ГБСМ - це параметри, що використовуються для оцінки та вимірювання продуктивності БСМ, які складаються з різних типів сенсорних вузлів з різними сенсорними, обчислювальними та комунікаційними можливостями. Особливості показників якості гетерогенних БСМ:

- Якість даних: Точність і надійність даних, зібраних з гетерогенних сенсорних вузлів, може бути показником якості. На якість даних можуть впливати

такі фактори, як калібрування датчиків, методи об'єднання даних і алгоритми обробки, що використовуються для агрегування та аналізу даних.

- Енергоефективність: Енергоспоживання гетерогенних сенсорних вузлів може бути показником якості. У ГБСМ вузли з різними можливостями можуть мати різні профілі енергоспоживання, і оптимізація використання енергії може допомогти збільшити термін служби мережі.
- Зв'язність: Здатність гетерогенних сенсорних вузлів зв'язуватися один з одним і з базовою станцією може бути показником якості. На зв'язок можуть впливати такі фактори, як протоколи зв'язку, що використовуються, топологія мережі та рівень перешкод.
- Затримка: Час затримки між збором і доставкою даних може бути показником якості. У ГБСМ різні типи сенсорних вузлів можуть мати різні можливості обробки, і зменшення затримки мережі може допомогти поліпшити продуктивність системи в реальному часі.
- Масштабованість: Здатність мережі обслуговувати зростаючу кількість різнорідних сенсорних вузлів може бути показником якості. Такі фактори, як архітектура мережі, протоколи маршрутизації та комунікаційні технології, що використовуються, можуть впливати на масштабованість мережі.
- Безпека: Здатність мережі захищати дані, що передаються гетерогенними сенсорними вузлами, може бути показником якості. У ГБСМ різні типи сенсорних вузлів можуть передавати різні типи даних, деякі з яких можуть бути більш чутливими або критичними, ніж інші.

Загалом, показники якості ГБСМ повинні бути розроблені таким чином, щоб враховувати унікальні характеристики різних типів сенсорних вузлів і конкретні вимоги застосування. Вимірюючи та оптимізуючи ці показники якості, можна покращити продуктивність та надійність гетерогенних БСМ.

У сценарії розгортання однорідних датчиків легше представити ефективні рішення, оскільки датчики мають схожі характеристики (наприклад, потужність, дальність зв'язку тощо). З іншого боку, алгоритми розгортання, запропоновані для однорідних датчиків, можуть бути неефективними для різнорідних датчиків через

їх різні характеристики. У Гетерогенній безпроводовій сенсорній мережі (ГБСМ) одним з фундаментальних дослідницьких питань є те, як розгортати і організовувати гетерогенні сенсорні вузли при заданих обмеженнях, таких як енергія, зв'язність і дальність передачі [12].

Існує три основних типи гетерогенності ресурсів у сенсорних вузлах:

- Обчислювальна неоднорідність означає, що гетерогенний вузол має більш потужний мікропроцесор і більше пам'яті, ніж звичайний вузол. Завдяки потужним обчислювальним ресурсам гетерогенні вузли можуть забезпечувати складну обробку даних і довготривале зберігання.
- Неоднорідність каналів зв'язку Гетерогенність зв'язку означає, що гетерогенний вузол має більш широкосмуговий і далекобійний мережевий трансивер, ніж звичайний вузол. Гетерогенність лінії зв'язку може забезпечити більш надійну передачу даних.
- Енергетична неоднорідність означає, що гетерогенний вузол живиться від мережі або його батарея є змінною. Серед типів ресурсної неоднорідності найважливішою є енергетична неоднорідність, оскільки як обчислювальна неоднорідність, так і неоднорідність каналів зв'язку будуть споживати більше енергетичних ресурсів.

Розміщення декількох гетерогенних вузлів у сенсорній мережі може принести наступні переваги:

- Зменшення затримки транспортування даних: Обчислювальна неоднорідність може зменшити затримку обробки в безпосередніх вузлах, а неоднорідність каналів зв'язку може зменшити час очікування в черзі на передачу. Менша кількість переходів між вузлами-датчиками і вузлом-приймачем також означає меншу затримку пересилання.
- Продовження терміну служби мережі: Середнє споживання енергії для пересилання пакета від звичайних вузлів до вузла-джерела в гетерогенних сенсорних мережах буде набагато меншим, ніж в однорідних сенсорних мережах.
- Підвищення надійності передачі даних: Добре відомо, що з'єднання сенсорних мереж мають низьку надійність. І кожен стрибок значно знижує

наскрізну швидкість доставки. З гетерогенними вузлами буде менше переходів між звичайними сенсорними вузлами та приймачем. Таким чином, гетерогенна сенсорна мережа може отримати набагато вищу наскрізну швидкість доставки, ніж однорідна сенсорна мережа.

На рисунку 1.9 показана гетерогенна модель для безпроводової сенсорної мережі.

Рис 1.9. Гетерогенна модель БСМ

Кластерне об'єднання безпроводових датчиків також можна застосовувати в ГБСМ для агрегування даних з різних типів сенсорних вузлів. У ГБСМ різні типи сенсорних вузлів можуть мати різні сенсорні, обчислювальні та комунікаційні можливості, що може ускладнити агрегування та обробку даних.

Для подолання цих викликів кластерне безпроводове об'єднання сенсорів може бути спроектоване так, щоб враховувати неоднорідність сенсорних вузлів. Наприклад, різні сенсорні вузли в кластері можуть мати різні способи зондування, і дані з цих вузлів можуть потребувати попередньої обробки та об'єднання за

допомогою спеціалізованих алгоритмів, які можуть обробляти різні типи даних. Крім того, використання гетерогенних технологій зв'язку, таких як Wi-Fi, Bluetooth і ZigBee, може вимагати застосування різних протоколів маршрутизації та агрегації даних для різних типів сенсорних вузлів.

Однією з головних переваг використання кластерного об'єднання безпроводових датчиків в ГБСМ є те, що воно може допомогти оптимізувати використання мережевих ресурсів і зменшити споживання енергії. Агрегуючи дані на рівні кластера, мережа може зменшити обсяг даних, що передаються через мережу, що дозволяє заощадити енергію і збільшити термін служби мережі. Крім того, обробляючи дані локально в межах кожного кластера, мережа може зменшити затримку і підвищити продуктивність системи в реальному часі.

Приклад кластерної безпроводової сенсорної мережі показано на рисунку 1.10.

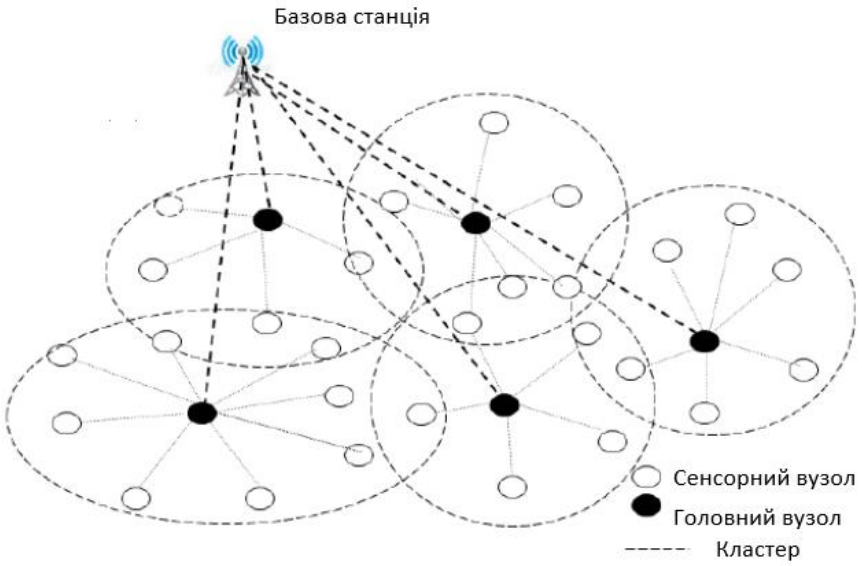

Рис.1.10. Кластерна БСМ

Протоколи маршрутизації на основі кластеризації у БСМ зазвичай складаються з двох фаз: фази кластеризації та фази маршрутизації.

Фаза кластеризації: На етапі кластеризації сенсорні вузли об'єднуються в кластери на основі певних критеріїв, таких як їх близькість до голови кластера, рівень енергії або залишковий час автономної роботи. На цьому етапі кожен

сенсорний вузол визначає свою приналежність до кластера і визначає голову кластера, до якої він буде надсилати свої дані. Голова кластера відповідає за збір даних з вузлів-учасників і пересилання їх на вузол-поглинач або інший визначений вузол у мережі.

Етап маршрутизації: На етапі маршрутизації дані передаються від голів кластера до вузла-джерела або іншого визначеного вузла в мережі. Дані можуть передаватися з використанням однохопового або багатохпового протоколу маршрутизації. При однохоповій маршрутизації дані передаються безпосередньо від голови кластера до вузла-приймача. При багатохоповій маршрутизації дані передаються через проміжні вузли, які допомагають розширити покриття мережі і підвищити надійність зв'язку.

Об'єднуючи сенсорні вузли в кластери, алгоритми кластеризації можуть зменшити мережевий трафік, підвищити ефективність мережі та продовжити термін служби мережі за рахунок зменшення споживання енергії [13].

Висновки до першого розділу

Проведено аналіз поняття сенсорної мережі та розкрито питання актуальності і важливості сенсорних мереж в різних галузях людської діяльності.

Проаналізовано найбільш важливі характеристики та структури безпроводових сенсорних мереж. Визначено, що саморегулюючий характер, особливі умови з енергетичної ефективності, стійкість до відмов та велике значення числа вузлів вимагають розробки специфічних алгоритмів маршрутизації для безпроводових сенсорних мереж.

Досліджено різні алгоритми маршрутизації для безпроводових сенсорних мереж, проведено їх аналіз та класифікацію.

Описано модель гетерогенної безпроводової сенсорної мережі. Проаналізовано метод кластеризаціїї, визначено його переваги та недоліки.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БОРОТЬБИ З ВРАЗЛИВІСТЮ БСМ

2.1 Проблеми безпеки БСМ

При передачі інформації в мережі дуже важливо забезпечити її безпеку. Це завдання вважається найскладнішим у БСМ, оскільки важко стежити за всіма сенсорними вузлами. Але мережа має бути захищена, щоб запобігти вторгненню зловмисника у систему передачі. Існує безліч обмежень, пов'язаних із сенсорним вузлом, особливо його розмір та вартість, які мають бути мінімальними. Ці обмеження призводять до дуже малого розміру пам'яті, обмеженого джерела енергії та дальності передачі. Це, зрештою, може призвести до відсутності шифрування, дешифрування та аутентифікації, які можуть бути реалізовані на сенсорний вузл.

Сенсорна мережа повинна відповідати вимогам для забезпечення безпечного зв'язку [14]. Загальні вимоги безпеки БСМ – це доступність, конфіденційність, цілісність та аутентифікація. Деякі інші вимоги відомі як вторинні вимоги, включають локалізацію джерела, самоорганізацію та свіжість даних. Ці вимоги забезпечують захист від атак на інформацію, що передається по сенсорній мережі.

Конфіденційність даних - це найважливіше питання мережевої безпеки. У сенсорній мережі потоки даних йдуть від безлічі проміжних вузлів, і вклика можливість витоку даних. Для забезпечення конфіденційності використовуються зашифровані дані, так що тільки одержувач може розшифрувати їх. Також для передачі конфіденційних даних дуже важливо мати захищений канал.Незважаючи на те, що конфіденційність захищає інформацію від атакуючого, це не означає, що інформація захищена. Зловмисники мають можливість модифікувати отриману інформацію та надіслати оброблені дані в приймач.

Доступність даних означає, що служби повинні бути доступні постійно, навіть у разі деяких атак, таких як відмова в обслуговуванні.

Зловмисник може змінювати не лише окремі пакети даних, а й весь поток даних, додаючи додаткові пакети. Тому обов'язок приймача у тому, щоб впевнитись у легітимності джерела. При побудові сенсорних мереж процес аутентифікації має важливе значення для багатьох додатків. У разі двостороннього зв'язку аутентифікацію даних забезпечує симетричний механізм шифрування. Код аутентифікації повідомлення обчислюється шляхом спільного використання секретного ключа між відправником та одержувачем.

Для передачі даних деякі програми використовують інформацію про місцезнаходження вузла приймача. Дуже важливо забезпечити безпеку інформації про місцезнаходження. Незахищені дані можуть контролюватись шкідливим вузлом шляхом надсилання помилкових сигналів.

У БСМ немає фіксованої інфраструктури, отже, кожен вузол незалежний, має властивості адаптації до різних ситуацій і зберігає самоорганізацію і властивості до самовідновлення . Це великий виклик для безпеки у БСМ.

Свіжість даних означає, що кожне повідомлення, що передається каналом, має бути новим та свіжим, і що старі повідомлення не можуть бути відтворені жодним вузлом. Це можна вирішити, додавши певний лічильник часу для перевірки свіжості даних.

Широкомовна природа каналу передачі даних робить беззпроводові мережі дуже сприйнятливими до різних типів атак. Зловмисники можуть атакувати радіопередачу; додавати свої власні біти даних у канал, відтворювати старі пакети та виробляти будь-які інші типи атак. Зловмисники можуть розгорнути деякі шкідливі вузли в мережі з аналогічними можливостями, як і у звичайного вузла або можуть перезаписати пам'ять звичайного розгорнутого вузла, захопивши його [14].

2.2 Моделі атак на БСМ та способи їх протидії

Характер атак досить складний, тому їх важко класифікувати. Тим не менш, виділяється дві великі категорії атак: пасивні та активні атаки.

У той час як пасивні атаки стосуються конфіденційності (прослуховування, збір і викрадення інформації шляхом перехоплення передачі даних або моніторингу пакетів, якими обмінюються в БСМ), активні атаки виконують такі дії, як введення помилкових даних у БСМ, видавання себе за іншу особу, зміна ресурсів і потоків даних, створення дірок у протоколах м безпеки, руйнуючи вузли датчиків, погіршуючи продуктивність, порушуючи функціональність і перевантажуючи мережу.

Детальне вивчення цих атак приводить до висновку, що вони в основному спричиняють два ефекти. Перший ефект - збільшення мережевого трафіку за рахунок введення в мережу нових пакетів. Другий – це протилежний ефект, зменшення мережевого трафіку через видалення або втрату мережевих пакетів. Ці два ефекти можуть діяти разом, збільшуючи мережевий трафік певного пакету та зменшуючи інші. Більш детальне вивчення атак показує, що не всі атаки можна змоделювати за допомогою цих ефектів, тому потрібна додаткова спеціальна модель.

Підсумовуючи, атаки на БСМ можна класифікувати за чотирма категоріями залежно від їхнього впливу на мережу:

- Атаки, які вводять пакети в мережу. Перший тип атак заснований на введенні фальшивих пакетів у мережу з метою змусити вихідні вузли їх обробляти, збільшуючи трафік у мережі та, таким чином, перевантажуючи її або навіть порушуючи дані мережі. До цього типу входять такі атаки:

Атака опитування: ця атака використовує двостороннє рукостискання RTS/CTS яке використовують багато протоколів керування доступом до медіа (MAC) для пом’якшення проблеми прихованого вузла. Зловмисник неодноразово надсилає повідомлення RTS, щоб отримати відповіді CTS від цільового сусіднього вузла.

Атака витрати енергії : через труднощі із заміною батарей сенсорних вузлів та їхні енергетичні обмеження зловмисники можуть використовувати скомпрометовані вузли для введення сфабрикованих звітів у мережу або створення великої кількості трафіку в мережі. Ці фальшиві повідомлення спричиняють

помилкові тривоги, які витрачають зусилля на реагування та споживають кінцеву кількість енергії в мережі, що живиться від акумулятора. Мета цієї атаки — знищити сенсорні вузли в мережі, знизити продуктивність мережі та, зрештою, розділити мережеву сітку, таким чином захопивши контроль над частиною сенсорної мережі, вставивши новий вузол приймача.

Атака Hello Flood : зловмисник зазвичай намагається викачати енергію з вузла або вичерпати його ресурси. Зловмисник із великою потужністю передачі може транслювати пакети «HELLO» (використовуються в багатьох протоколах для виявлення вузлів), щоб переконати кожен вузол у мережі, що зловмисник знаходиться в радіусі зв'язку з одним стрибком зв'язку, що змушує велику кількість вузлів витрачати енергію на надсилання пакетів. до цього уявного сусіда і, таким чином, у забуття.

Атака з неправильним спрямуванням : зловмисник направляє пакет від дочірніх вузлів до інших віддалених вузлів, але не обов'язково до законного батьківського. Основна мета зловмисника полягає в тому, щоб неправильно спрямувати вхідні повідомлення, щоб збільшити затримку, яка перешкоджає досягненню кількох пакетів базової станції.

Flooding атака : зловмисник може неодноразово робити нові запити на з'єднання, доки не буде вичерпано ресурси, необхідні для кожного з'єднання, або досягнуто максимального ліміту. Це створює серйозні обмеження ресурсів для законних вузлів [15].

- Атаки, які вносять шум в мережу. Наслідки атак, розміщених у цій групі, полягають у зниженні трафіку в мережі. Ці атаки зосереджені на запровадженні шуму в мережі (або інших методах) з метою збільшення ймовірності втрати пакетів. Основним наслідком цих атак є збільшення рівня втрати пакетів, що може порушити належне функціонування мережі. Атаки в цій категорії:

Атака з перешкодами: це працює шляхом відмови в обслуговуванні авторизованих користувачів, оскільки легітимний трафік перешкоджає величезній кількості нелегітимного трафіку. Він порушує роботу мережі, транслюючи сигнали високої енергії. Існує багато стратегій глушіння.

Атака зіткнення: під час атаки зіткнення вузол зловмисника не дотримується протоколу керування доступом до середовища та створює зіткнення з передачами сусіднього вузла, надсилаючи короткий пакет із шумом. Пакети зіштовхуються, коли два вузли намагаються передавати на одній частоті одночасно, створюючи пошкодження пакетів. Ця атака може спричинити багато збоїв у роботі мережі.

Атака з вичерпанням ресурсу: робота цієї атаки полягає в повторюваних зіткненнях і багаторазових повторних передачах, доки вузол не загине. Шкідливий вузол постійно запитує або передає через канал.

Атака чорна діра: атака чорна діра в основному полягає у зміні маршрутизації мережі з метою залучення всіх пакетів до атакуваного вузла призначення та тихого їх відхилення або скидання.

Атаки на відмову в обслуговуванні (DoS) : під час атаки DoS на основі шляху (PDoS) зловмисник переміщує вузли датчиків на велику відстань, заповнюючи наскрізний шлях зв’язку з кількома стрибками або реплікованими пакетами, або фальшивими пакетами. . Це може завдати серйозної шкоди системам з обмеженими ресурсами.

Атака самонаведення: під час атаки самонаведення зловмисник переглядає мережевий трафік, щоб визначити географічне розташування критичних вузлів, таких як головки кластерів або сусіди базової станції. Потім зловмисник може фізично вимкнути ці вузли. Це призводить до іншого типу атаки чорної діри.

Атака вибіркового пересилання: мережі з кількома стрибками припускають, що вузли-учасники сумлінно пересилають і отримують повідомлення. Однак зловмисний вузол може відмовитися пересилати певні повідомлення та просто скинути їх, гарантуючи, що вони більше не поширюватимуться. Процедура запуску вибіркових атак вперед дуже схожа на чорну діру. По-перше, зловмисний вузол повинен переконати мережу, що він є найближчим вузлом до базової станції, залучаючи мережевий трафік для маршрутизації даних через нього. Потім вибір пакетів скидається [15].

- Атаки, які вносять шум і пакети в мережу. Третя група складається з атак, які викликають різні ефекти в мережі шляхом змішування ефектів попередніх.

Ці атаки призводять до того, що мережа втрачає деякі пакети, але водночас вони вводять нові пакети в мережу. Таким чином, ці атаки змінюють типи пакетів, що передаються, зменшуючи кількість одних типів пакетів, але збільшуючи інші, з подальшим впливом на БСМ.

Підроблена атака: підроблена атака — це ситуація, в якій зловмисник успішно маскується під інший вузол, фальсифікуючи дані та отримуючи таким чином нелегітимну перевагу. Ця атака полягає в націлюванні на інформацію про маршрутизацію під час її обміну: створення циклів маршрутизації, залучення або відштовхування мережевого трафіку від вибраних вузлів, розширення та скорочення вихідних маршрутів, створення фальшивих повідомлень про помилки, розділення мережі тощо.

Атака Sybil: ця атака полягає в модифікації мережевої маршрутизації для залучення трафіку вузлів зловмисників з метою ізоляції цих вузлів. Коли ці вузли більше не можуть спілкуватися, зловмисник надсилає підроблений трафік, замінюючи вузли.

Атака реплікації вузла: це атака, під час якої зловмисник намагається підключити кілька вузлів з однаковими ідентифікаторами в різних місцях існуючої мережі. Хоча атаки Sybil і атаки Node Replication можуть здаватися схожими, ці атаки істотно відрізняються. У атаках Sybil один вузол існує з кількома ідентифікаторами, тоді як в атаках реплікації вузлів присутні кілька вузлів з однаковими ідентифікаторами. Таким чином, під час атаки Sybil зловмисник може досягти успіху, монтуючи лише один вузол, тоді як атака реплікації вузла вимагає монтування більшої кількості вузлів у всій мережі. Таким чином, зі збільшенням кількості мережевих вузлів шанс виявити цю атаку також зростає.

Зациклення в мережевій атаці: ця атака полягає в модифікації мережевої маршрутизації шляхом впливу на передачу даних вузла. «Підроблений» вузол інформує інший вузол, що він є останнім вузлом у ланцюжку або що він є найближчим вузлом до кінця ланцюжка вузлів. Цей «фальшивий» вузол знову надсилає пакет у мережу, замикаючи пакет у нескінченний цикл [15].

- Атаки, які змінюють мікропрограму вузла. Деякі атаки безпосередньо не впливають на мережевий трафік, але вони можуть вплинути на програмне забезпечення або апаратне забезпечення вузла. Ці атаки зазвичай вимагають прямого доступу до апаратного вузла (тамперні атаки).

Атака на програму: ця атака змінює мікропрограму/програмне забезпечення, яке зберігається у вузлі. Зазвичай для цього потрібен доступ до процедури оновлення програмного забезпечення на місці (процедура програмування по повітрю) або фізичний доступ до апаратного забезпечення вузла.

Перевантажена атака: зловмисник може спробувати перевантажити сенсорні вузли стимулами датчиків, які можуть створити великі обсяги трафіку до базової станції. Серед інших проблем це спричиняє збільшення енергоспоживання в атакуваних вузлах і створення ненадійної інформації датчиків.

Захист проти DoS атак. Атаки відмови в обслуговуванні (DoS) в сенсорних мережах вимагають ефективних заходів, щоб уникнути їх або перешкодити їх поширенню по всій мережі. Наприклад, коли виявляється або підозрюється атака перешкод, сенсорна мережа може спробувати ізолювати порушену область, направивши трафік навколо відключених частин мережі. На канальному рівні атаки зіткнень і вичерпання ресурсів можуть бути адресовані шляхом використання кодів корекції помилок (які додають витрати на обробку і комунікації) і схем, які обмежують розмір, що дозволяють пристрою ігнорувати запити, які можуть привести до передчасного енергетичного виснаження. Спуфінг і перетворення може бути адресовано на мережевому рівні за допомогою коду аутентифікації повідомлень або MAC, яка може бути розглянута як криптографічно безпечна контрольна сума повідомлення. Ці контрольні суми дозволяють одержувачу перевірити, чи імітувалося або змінювалося повідомлення. Атака на відмову в обслуговуванні на основі шляху - це атака, в якій атакуючий нищить вузли в віддаленій сенсорній мережі, лавинно розсилаючи мультитранзитну ділянку наскрізного каналу зв'язку з відтвореними пакетами, або з пакетами, введеними в довільному порядку. Кожен вузол в мережі використовує ланцюжок хешування, щоб перевірити отриманий пакет, тобто вузол систематично циркулює через

ланцюжок, щоб визначити, чи пакет з довіреного джерела. Якщо пакет не може бути перевірений, він відкидається.

Захист проти атак маршрутизації. Більшості атак «із зовні» мережі можна запобігти, використовуючи шифрування на канальному рівні і аутентифікацію з використанням глобального загального ключа. Оскільки противнику перешкоджають приєднатися до мережі, такі атаки як вибіркова передача неможливі. Однак коли мережі піддаються нападу «зсередини», використовуючи компрометуючий вузол, цей підхід неефективний, і необхідні більш складні рішення. Атаці Сібіл можна запобігти шляхом перевірки ідентичності сенсорних вузлів. Наприклад, кожен сенсорний вузол може спільно використовувати унікальний симетричний ключ з довіреною базовою станцією, яка може бути використана для перевірки ідентифікаційних даних один одного. Базова станція може також обмежити число сусідів, яких дозволено мати вузлу, тобто навіть коли вузол скомпрометований, він може зв'язатися тільки з перевіреними сусідами. Проти атаки Воронка важко захиститися в протоколах, де маршрути встановлені на основі інформації, яку важко перевірити, наприклад надійність або енергетичні показники. Маршрути, засновані на мінімальній кількості хопів легше перевірити, але кількість хопів може бути спотворено через кротовину. Категорія протоколів, стійких до цих атак називається географічна маршрутизація. Мережі, використовуючи засновані на місцезнаходженні методи маршрутизації, встановлюють топологію на основі локалізованих взаємодій та інформації без ініціювання з базової станції. Так як трафік спрямований до фізичного розташування базової станції, важко перенаправити його в інше місце, щоб створити воронку. В атаці стрімкого натиску мета вузла полягає в тому, щоб використовувати процес відкриття маршруту в протоколах маршрутизації на вимогу, щоб привернути до себе якомога більше маршрутів. Однак, щоб запобігти таким атаки, може використовуватися комбінація декількох заходів захисту. Наприклад, деякі зловмисники можуть передати запити маршруту за рамки нормального діапазону радіопередач (наприклад, використовуючи високу потужність передачі) тим самим пригнічуючи наступні повідомлення запиту.

Підхід виявлення безпечного сусіда може використовуватися, щоб дозволити для відправника і для одержувача запити на перевірку маршруту, підтвердження, що інша сторона на нормальному діапазоні передачі. Наприклад, протокол взаємної аутентифікації з трьома циклами з жорстким часом затримки може бути розгорнутий. У першому циклі вузол передає пакет сусіднього клопотання (або через широкомовну передачу або через одноадресну передачу до певного вузла). У другому циклі вузол, який отримує пакет клопотання, відповідає сусіднім повідомленням, а в третьому циклі, ініціатор цієї комунікації квитирування відправляє сусіднє повідомлення перевірки, яке включає трансляцію аутентифікації, мітки часу і посилання від джерела до місця призначення [15].

2.3 Протоколи безпеки для БСМ

Проект Протоколи захисту для сенсорних мереж (SPINS) робить два основних вклади в захист від атак: Протокол шифрування безпеки мережі (SNEP) і Протокол синхронізованої, ефективної, з можливістю передавання потоків, стійкою до втрати аутентифікації (μTESLA). Основна мета протоколу SNEP полягає в тому, щоб забезпечити конфіденційність, двопартійну аутентифікацію даних і їх актуальність, в той час як μTESLA забезпечує аутентифікацію для широкомовної передачі даних [16]. Кожен вузол, як передбачається, спільно використовує закритий ключ з базовою станцією. SNEP бере до розгляду обмеження ресурсу типових сенсорних вузлів, покладаючись на прості алгоритми для шифрування, аутентифікації і генерації випадкових чисел. Ключові властивості SNEP - її симетрична безпека, відтворення захисту і низькі накладні витрати зв'язку. Симетрична безпека стосується того факту, що одне й те саме повідомлення кожного разу шифрується по-іншому. Щоб досягти двопартійної аутентифікації і цілісності, SNEP використовує MAC, де більше MAC більш складне для противника, щоб вгадати відповідний код для повідомлення. З іншого боку великі коди означають великі розміри пакетів. Два суміжних вузла A і B спільно використовують головний секретний ключ, який використовується, щоб вилучити

чотири незалежних ключа, використовуючи псевдовипадкову функцію. Двоє з цих ключів використовуються для шифрування повідомлень в кожному напрямку, і два ключа використовуються в якості кодів цілісності повідомлення, знову один для кожного напряму

SNEP забезпечує аутентифікацію даних (використовуючи MAC), захист відтворення (використовуючи значення лічильника MAC), актуальність (значення лічильника здійснюють упорядкування повідомлень), семантичну безпеку (тому що, лічильник зашифрований кожним повідомленням, і кожне повідомлення буде зашифровано кожен раз по-різному) і низькі накладні витрати зв'язку (передбачає, що стан лічильника збережено в кожній кінцевій точці і не відправлено в повідомленні). Актуальність даних в рамках SNEP вважається слабкою тільки через те, що SNEP здійснює порядок передачі в вузол B, але не дає ніякої гарантії вузлу A, що повідомлення було створено вузлом B, у відповідь на подію в вузлі A. Щоб досягти актуальності, випадок (тобто, випадкове число таке довге, що вичерпний пошук всіх можливих випадків неможливий) може бути включений в протокол. Вузол в довільному порядку генерує випадок NA і відправляє його разом з повідомленням запиту до вузла B. Потім вузол B повертає випадок з відповідним повідомленням у аутентифікованому протоколі.Якщо MAC перевіряє правильно, вузол A знає, що вузол B генерував свою відповідь після запиту A.

Протокол μTESLA фокусується на потребі в аутентифікованій широкомовній передачі в безпроводових сенсорних мережах [16]. Він покладається на симетричні механізми, забезпечені SNEP, для аутентифікації першого пакету в широкомовному повідомленні. Це розширення TESLA, не було розроблено для використання в середовищах з обмеженими обчислювальними ресурсами. TESLA використовує цифрові підписи, щоб аутентифікувати початковий пакет і має витрати 24 байта за пакет, які можуть бути значними для сенсорних мереж, де повідомлення зазвичай дуже маленькі. Аутентифікована широкомовна передача вимагає асиметричного механізму (інакше, будь-який компрометуючий одержувач зможе підробити повідомлення від відправника), але асиметричні криптографічні механізми часто мають високі вимогаи до ресурсів. Замість цього μTESLA емулює

асиметрію за допомогою затримання розкриття симетричних ключів. μTESLA передбачає, що базова станція і сенсорні вузли вільно синхронізовані за часом і кожен вузол знає верхню межу максимальної помилки синхронізації. Коли базова станція відправляє повідомлення, вона аутентифікує його, обчислюючи MAC на пакеті з ключем, який є закритим в цій точці. Коли вузол отримує пакет, і ключ невідомий, вузол знає, що ключ MAC відомий тільки базової станції. Вузол зберігає пакет до базової станції, під час ключового розкриття, широкомовно передає ключ перевірки всім одержувачам. Тепер вузол може використовувати ключ, щоб аутентифікувати збережений пакет.

Структура TinySec - легкий і універсальний пакет захисту на канальному рівні, які розробники можуть легко інтегрувати в додатках сенсорної мережі. Він підтримує два різних параметра безпеки: аутентифіковане шифрування (TinySec-AE), де корисне навантаження даних зашифроване і MAC використовується, щоб аутентифікувати пакет, і тільки аутентифікація (TinySec- Auth), де весь пакет аутентифікується з MAC (але корисне навантаження залишається незашифрованим) [17]. TinySec покладається на ланцюжок цифрових блоків і спеціально відформатований 8-байтовий вектор ініціалізації для шифрування. Для аутентифікації TinySec покладається на ефективну і швидку конструкцію ланцюжка цифрових блоків (CBC MAC) для обчислень і перевірки MAC. Перевага CBC MAC полягає в тому, що, він покладається на цифровий блок, він мінімізує число криптографічних примітивів, які повинні бути реалізовані, що вигідно для сенсорних вузлів з обмеженими ємностями зберігання. Довжина MAC тільки 4 байта, тобто противник може неодноразово робити спроби сліпих підробок, які привели б до успіху найбільше після 232 спроби. Хоча це число здається маленьким, потрібно відзначити, що противник має оцінити достовірність коду, відправивши його авторизованому одержувачу. Що в подальшому означає, що до 232 повідомлень повинні бути передані, що забезпечує достатній рівень безпеки для сенсорних мереж.

Локалізоване шифрування і протокол аутентифікації (LEAP) - протокол управління ключами для сенсорних мереж, розроблених, щоб підтримувати

мережеву обробку [18]. Ключова мотивація цього протоколу - спостереження за тим, щоб різні типи повідомлень (наприклад, контрольні пакети в порівнянні з пакетами даних) в сенсорної мережі мали різні вимоги до захисту. Єдиний механізм маніпулювання не може підходити для зустрічі цих різних вимог, наприклад, в той час як аутентифікація може бути необхідна для всіх типів пакетів, конфіденційність, може бути необхідна тільки для певних типів повідомлень (наприклад, агрегованих сенсорних даних).

LEAP забезпечує чотири механізми маніпулювання: окремі ключі, ключі групи, кластерні ключі, і попарно спільно використовувані ключі. В індивідуальному ключовому механізмі у кожного вузла є свій власний унікальний ключ спільно використовуваний з базовою станцією. Цей ключ використовується для конфіденційного зв'язку або для обчислень кодів аутентифікації повідомлень, якщо вузол хоче, щоб базова станція перевірила свої дані. Груповий ключ - використовується глобально і спільно.

Він використовується базовою станцією для передачі зашифрованих повідомлень до всієї сенсорної мережі. Кластерний ключ – ним користуються одночасно з сенсорним вузлом і його сусіди, і він використовується для забезпечення локальних широкомовних повідомлень (наприклад, повідомлення про маршрут). Попарно - спільно використовуваний ключ - ключ, яким користуються сенсорний вузол і одим з його безпосередніх сусідів. LEAP використовує ці ключі для безпечних комунікацій серед пар вузлів, наприклад, дозволяючи вузлу надійно розподілити кластерний ключ своїм сусідам або надійно передати свої сенсорні дані до вузла агрегації. LEAP також забезпечує метод для локальної широкомовної аутентифікації.

Кожен вузол генерує однобічний ланцюжок для ключів певної довжини і передає перший ключ в ланцюжок кожному сусідові, зашифрований попарно спільно використовуваних ключем. Кожен раз, коли вузол відправляє повідомлення, він бере наступний ключ з ланцюжка (кожен ключ називають ключем AUTH), і приєднує його до повідомлення. Ці ключі розкриті в зворотному

порядку їх генерації, і одержувач може перевірити повідомлення на основі першого отриманого ключа або недавно відкритого ключа AUTH.

Стандарт IEEE 802.15.4 і специфікація ZigBee - популярний вибір протоколу для БСМ. Даний стандарт широко використовується при побудові БСМ і працює на фізичному та канальному рівнях моделі OSI [19]. Стандарт IEEE 802.15.4 забезпечує чотири основні моделі безпеки: управління доступом, цілісність повідомлення, конфіденційність повідомлення і захист відтворення. Безпека в IEEE 802.15.4 оброблена рівнем MAC, і додаток може вибрати певні вимоги до захисту, встановивши належні параметри в радіо-стеку (за замовчуванням, безпека не включена).

Стандарт розрізняє вісім наборів безпеки, що наведено в таблиці 2.1, кожен з різними рівнями захисту для переданих даних. Перший набір не пропонує захист, другий набір пропонує тільки шифрування (AES - CTR), супроводжуваний групою наборів тільки з аутентифікацією (AES - CBC - MAC), і групою наборів і з аутентифікацією і з шифруванням (AES - CCM). Набори, які пропонують аутентифікацію, відрізняються за розмірами MAC, які варіюються від 32 до 128 бітів.

Таблиця 2.1

Набори безпеки, які підтримуються в IEEE 802.15.4

Назва	**Опис**
AES-CTR	Encryption only, CTR mode
AES-CBC-MAC-128	128-bit MAC
AES-CBC-MAC-64	64-bit MAC
AES-CBC-MAC-32	32-bit MAC
AES-CCM-128	Encryption and 128-bit MAC
AES-CCM-64	Encryption and 64-bit MAC
AES-CCM-32	Encryption and 32-bit MAC

Всі набори безпеки використовують цифровий блок Вдосконаленого стандарту шифрування (AES), який також відомий як Rijndael. Національний

інститут стандартів і технологій визначає п'ять режимів роботи, включаючи лічильник (CTR) і режим ланцюжка цифрових блоків (CBC). Коли необхідна аутентифікація, може використовуватися один з трьох AES - CBC - MAC варіантів, які обчислюють код цілісності повідомлення, використовуючи цифровий блок в режимі CBC. Три набору AES - CCM комбінують шифрування і аутентифікацію за допомогою режиму Лічильника і режиму CBC (CCM закоротка для Лічильника CBC - MAC).

На додаток до засобів захисту IEEE 802.15.4 специфікація ZigBee також представляє поняття центру довіри, відповідальність зазвичай прийнята на координатора ZigBee. Центр довіри відповідальний за аутентифікацію пристроїв, що бажають приєднатися до мережі (адміністратор довіри), підтримку і розподіл ключів (адміністратор мережі) і включення наскрізної безпеки між пристроями (менеджер конфігурації).

ZigBee також диференціюється між житловим і комерційним режимом. У житловому режимі центр довіри дозволяє вузлам приєднуватися до мережі, але не встановлює ключі з мережевими пристроями. У комерційному режимі він генерує і підтримує ключі, і свіжість лічильників з кожним пристроєм в мережі. Недолік комерційного режиму - вартість пам'яті, яка росте з розміром мережі.

Специфікація ZigBee використовує режим CCM* для своїх служб безпеки, яка також є комбінацією режимів CTR і CBC - MAC. У порівнянні з режимом CCM, CCM * пропонує можливості тільки для шифрування і тільки для цілісності. Подібно специфікаціям в стандарті IEEE 802.15.4, у ZigBee є кілька рівнів безпеки, включаючи нульова безпеку, тільки шифрування, тільки аутентифікація, і обидва і шифрування і аутентифікація. Рівні, які забезпечують аутентифікацію, використовують MAC, який може змінюватися від 4 до 16 байтів.

Висновки до другого розділу

Досліджено проблеми безпеки БСМ. Розглянуто типи атак на БСМ та методи протидіїї цим атакам. Що стосується протоколів безпеки для БСМ, то для

забезпечення конфіденційності, цілісності та доступності даних вибір і реалізація протоколів безпеки може змінюватися в залежності від конкретних вимог і обмежень розгортання БСМ.

Зазначено, що жоден окремий контрзахід не може забезпечити абсолютну безпеку. Для захисту мереж БСМ від різних атак і забезпечення їх загальної безпеки зазвичай необхідна комбінація декількох заходів безпеки і протоколів. Крім того, регулярний аудит безпеки, оновлення та виправлення є важливими для усунення нововиявлених вразливостей та підтримання безпечного середовища БСМ.

3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО СТВОРЕННЯ ЗАХИЩЕННИХ БСМ

3.1 Характеристика інструментів симуляції БСМ

Вузли в безпроводових сенсорних мережах зазвичай мають високі енергетичні обмеження, і часто очікується, що вони працюватимуть протягом тривалого часу з обмеженими запасами енергії. З цієї причини рання оцінка продуктивності є важливим кроком у будь-якій методології проектування вбудованої системи. Спочатку, швидкі та точні симуляції можуть надати інформацію розробникам БСМ, що дозволяє модифікувати алгоритми програмного забезпечення або мережеву архітектуру з метою оптимізації дизайну для найкращого використання обмежених ресурсів [20].

Багато мережевих факторів у БСМ ще не завершені і не встановлені. Створення випробувального стенду БСМ коштує дорого. Проводити реальні випробування на симуляціних платформах також дорого і проблематично. Крім того, проведення реального тесту є досить важким. Таким чином, симуляція БСМ є важливим фактором для покращення БСМ. Протоколи та плани можуть бути оцінені у значному масштабі. Симулятори глобальних мереж дозволяють клієнтам відключати унікальні елементи, налаштовуючи конфігуровані параметри. Таким чином, моделювання має важливе значення для ознайомлення з БСМ , являючись технікою для перевірки нових пакетів та протоколів в межах області. Це спонукає до постійного вдосконалення симуляторів. Незважаючи на це, отримання точних визначень за допомогою симуляції - це дійсно важливе завданням. Існує кілька ключових точок зору на симулятори БСМ: правильність моделювання і відповідність обраного інструменту для виконання версії. Правильна версія, що залежить від презумпції, є обов'язковою для отримання достовірних результатів.

Є три типи симуляції для БСМ:

1. Симуляція методом Монте-Карло

2. Імітаційна симуляція на основі трасування

3. Дискретно-подієва симуляція .

Зазвичай у БСМ використовується симуляція на основі трасування та дискретних подій.

Симуляція дискретних подій застосовується у БСМ, оскільки може легко моделювати багато завдань, що виконуються на різних сенсорних вузлах. Дискретно-подієва симуляція містить ряд елементів [20]. Ця симуляція може містити список очікуваних подій, які можуть бути змодельовані за допомогою розкладів. Глобальні елементи, які відображають стан системи, можуть посилатися на час моделювання, що дозволяє розраховувати цей час заздалегідь. Ця симуляція містить графіки входу, графіки виходу, розклади запуску та стан виконання розкладів. Крім того, ця симуляція дає динамічне управління ремінісценціями, яке може включати нові матеріали і додавати вінтажні елементи до моделі. Точки зупинки надаються в дискретно-подієвому моделюванні, і, крім того є можливість поглянути на впорядкований код, не перериваючи при цьому активність програм.

Симуляція, керована трасуванням надає численні послуги. Цей тип симуляції зазвичай застосовується в реальному гаджеті. Результати симуляції мають додаткову достовірність, що також дає додаткове навантаження; ці факти дозволяють глибоко вивчати імітаційну модель. Для максимального компонента, вхідні значення в цій симуляції залишаються незмінними . Ця симуляція також має кілька недоліків. Наприклад, статистика аномальних елементів створює багатогранну природу симуляції [20].

Іструменти для симуляції БСМ. Для підтримки дослідників у виборі правильної симуляційної системи для створення нових алгоритмів, протоколів і стратегій в безпроводових сенсорних мережах, пропонується детальне роз'яснення різних цілей та конкретних причин призначення інструменту моделювання.

Приклади інструментів симуляції для БСМ:

- Network Simulator 2 (NS-2) вважається інструментом для моделювання дискретних подій і добре зарекомендував себе в дослідженнях динамічних мереж зв'язку. NS-2 повністю базується на об'єктно-орієнтованому програмуванні, тому він також відомий як об'єктно-орієнтований симулятор дискретних подій. Він

складається з двох мов: C++ та об'єктно-орієнтованої мови інструментальних команд (OTcl). C++ в основному використовується для реалізації різних протоколів і розширення бібліотек моделювання, в той час як скрипти OTcl виконують завдання конфігурації симулятора, налаштування топології мережі, створення мережевих сценаріїв і відображення результатів моделювання. C++ та OTcl пов'язані між собою за допомогою TclCL. Він може працювати на різних операційних системах, таких як Linux, FreeBSD, MAC OS X, Solaris і навіть Windows за допомогою стороннього програмного забезпечення Cygwin. Що стосується БСМ , NS-2 забезпечує підтримку різних протоколів, таких як 802.11, 802.16, 802.15.4, IR-UWB тощо. Але NS-2 стикається з серйозними недоліками з точки зору симуляції БСМ, в ньому не існує моделі зондування. Параметри, які використовуються під час моделювання вузлів у БСМ, такі як енергетична модель, формати пакетів та MAC протоколи, повністю відрізняються від тих, які використовуються в реальному сценарії сенсорної мережі. Іншим недоліком результатів моделювання NS-2 є те, що йому також не вистачає підтримки додатків, яка необхідна через взаємодію сенсорної мережі між рівнем додатків та рівнем протоколів. NS-2 підтримує подвійний вихід, який може бути як текстовим, так і графічним. Для графічного моделювання NS-2 має вбудований інструмент NAM (Network Animator), який показує рух пакетів у вузлах, положення вузлів і сценарій моделювання в реальному часі, а також містить XGraphs, який показує графічний аналіз результатів, отриманих в кінці моделювання [21].

- NS3 також є симулятором мережі дискретних подій. Метою його розробки було поглиблення досліджень в галузі комунікаційних мереж. NS-3 є симулятором з відкритим вихідним кодом. NS-3 не розглядається як розширення симулятора NS-2, NS-3 - це новий симулятор, який не підтримує жодного API, що належить до NS-2.Оскільки програми, написані в NS-2, кодуються на OTcl і результати можуть бути візуалізовані за допомогою NAM і XGraph, але чистий C++ код в NS-2 неможливий. Натомість у NS-3 всі програми написані чистою мовою C++ з додатковими прив'язками до python. У NS-3 немає графічного інструменту, але графічні результати можна інтерпретувати за допомогою програмного

забезпечення з відкритим вихідним кодом NetAnim. Для проводової топології NS-3 надає модель пристрою простої мережі Ethernet, яка використовує CSMA/CD як схему протоколу з експоненціально зростаючим відступом для боротьби за спільне середовище передачі. Що стосується БСМ, різні модулі, такі як 802.15.4, 6LoWPAN і RPL, вже інтегровані в NS-3 [22].

- NS4 (Network Simulator-4) — це мережевий симулятор, керований P4. NS4 призначений для зменшення важкої роботи, яка є результатом надлишку кодів у NS-3 [22]. Конфігурація NS4 складається з площини керування та площини даних. Площина керування складається з реального світу, керуючої програми, яка є графічним інтерфейсом користувача для клієнта. Ця програма контролера пропонує доповнення до дисплея оператора. NS4 дозволяє організовувати відтворення для конвенцій Bluetooth, 802.11a, CSMA, LTE. Вхідна програма передається в диспетчер каналів, декапсулятор і інкапсулятор пакетів. Контролер каналу розширює межі таблиці моделювання пристроїв P4. Пізніше він змінює інформаційні програми на двійковий файл P4, що робить програму P4. NS4 незмінно ідеально підходить для NS-3. Він заповнює загальний набір інструментів, який забезпечує організоване відтворення. Це забезпечує кращу універсальність.

- OMNet++ - ще один потужний об'єктно-орієнтований симулятор дискретно-подієвих мереж для БСМ . Він розглядається як розширювана, модульна та компонентна бібліотека імітаційного моделювання на мові C++ для побудови симуляцій. По суті, OMNeT++ не є симулятором, але надає фреймворки та інструменти для написання сценаріїв моделювання. Вона сумісна з різними операційними системами, такими як Windows, Linux та MAC OS X. Графічний інтерфейс TKenv було перероблено для одновіконного режиму, щоб покращити користувацький досвід та використання симулятора. Основна роль TKenv полягає в тому, щоб показати анімацію мережевої моделі, рух вузлів, відображення результатів, візуалізацію змін тощо. OMNeT++ можна безкоштовно завантажити для навчальних та дослідницьких цілей. Компанія також має ліцензійну версію під назвою «OMNEST», ліцензія доступна через Simulcraft Inc. Базові елементи, з яких складається OMNeT++, називаються модулями. Модулі бувають трьох типів: (A):

Простий модуль: Написаний на C++; (B): Складений модуль: Модуль, який пов'язує інші модулі за допомогою з'єднань; (C): мережевий модуль: Складений модуль верхнього рівня називається мережевим модулем. До складу OMNeT++ входить середовище IDE на основі Eclipse, яке дозволяє програмувати на C++ та налагоджувати модулі, а також графічно та текстово редагувати NED файли. NED (Network Description) дозволяє користувачеві оголошувати прості модулі, з'єднувати та збирати їх у складні модулі [23].

- J-Sim — це Симулятор J-Sim (JavaSim) вважається симулятором загального призначення і базується на компонентній архітектурі програмного забезпечення, автономній компонентній архітектурі (ACA). J-Sim розроблений на мові Java і тісно пов'язаний з ACA, що робить J-Sim нейтральним до платформи, розширюваним і багаторазово використовуваним середовищем. J-Sim має інтерфейс сценаріїв, який забезпечує виконання різних скриптових мов, таких як Perl, TCL або Python.J-Sim має значну перевагу над симулятором NS-2, оскільки на відміну від NS-2, класи/методи/поля в Java не потрібно явно експортувати, щоб отримати доступ до них в середовищі TCL; навпаки, всі загальнодоступні класи/методи/поля в Java можуть бути доступні в TCL-середовищі [24].

J-Sim надає фреймворк для моделювання БСМ, який побудований на основі ACA, INET та стеку безпроводових протоколів і складається з вузлів цілі, датчика та поглинача, каналів датчиків та каналів безпроводового зв'язку, фізичних носіїв, таких як сейсмічні канали, моделі мобільності та енергетичні моделі.

Розглядаючи моделювання БСМ , J-Sim використовує для реалізації три протоколи БСМ: Локалізація, Географічна маршрутизація та Спрямована дифузія . Порівняно з NS-2, симулятор J-Sim має ряд переваг з точки зору часу виконання, розподілу пам'яті та масштабованості. Крім того, він надає хорошу платформу для проведення великомасштабних симуляцій БСМ з більш ніж 1000 вузлів, що є дещо неможливим в NS-2. J-Sim надає фреймворк для декількох класів для моделювання сенсорної мережі з точки зору покриття, індексації часу та управління живленням.

- Tossim — це емулятор, спеціально призначений для БСМ, що працює на TinyOS, яка є ОС з відкритим вихідним кодом. TOSSIM — це емулятор мережі

з дискретними подіями на бітовому рівні, який працює на Python, мові програмування з аномальним станом, що підкреслює узгодженість коду, і C++. Окремі особи можуть запустити TOSSIM в операційних системах Linux. TOSSIM додатково надає відкриті джерела та онлайн-архіви [25].

- EmStar — це емулятор, керований таблицею, що працює безперервно, спеціально розроблений на C для БСМ. Окремі особи можуть запускати цей емулятор у робочій системі Linux. Ці резервні копії емулятора для створення програми БСМ на кращих апаратних датчиках. Крім бібліотек, інструментів і служб, є розширення мікроядра Linux інтегровано в емулятор EmStar [26].
- Avrora — це симулятор, спеціально призначений для побудування БСМ на Java. Як і ATEMU, Avrora також може симулювати сенсорні вузли мікроконтролера MICA2 на базі AVR. Цей симулятор виробляється Університетом Каліфорнія, Los Angeles Compilers Group. Аврора пропонує інтенсивний вид інструментів, які можуть бути застосовані при моделюванні БСМ [27].
- Програмне забезпечення для симуляції індустріальної спільноти QualNet-(Quality Networking) від Scalable Technologies в основному є похідним об’єктом від GloMoSim Simulator. QualNet забезпечує «віртуальну» версію системи високої надійності , яка складається з комутаторів, маршрутизаторів, точок доступу, радіоприймачів, антен, ПК і кількох різних апаратних засобів. Різні протоколи для розширення можливостей пакетів у мережевому сценарії. Мережевий симулятор QualNet 7 і EXata підтримується на певних платформах, таких як Windows 7/8/8.1, Centos 5.9, RHEL 6/7 і Ubuntu 12.04, починаючи з версій, і їх було припинено в жовтні 2013 року. У таблиці 3.3 висвітлюються загальні порівняння продуктивності на основі параметрів різноманітних інструментів симуляції.

Оцінка розглядає стандартні симулятори: NS-2 і NS-3, NS-4, TOSSIM, EmStar, OMNeT++, JSim і Avrora, SENS, QualNet, а також аналізує їхні переваги та обмеження. Продуктивність утиліти залежить від багатьох інших факторів, окрім її реалізації та використання обладнання. Дослідження повинно бути в рамках

моделювання точних ситуацій реального світу для того щоб змоделювати респектабельний проект БСМ.

3.2 Моделі довіри та репутації

Традиційні засоби захисту мережі включають криптографічні методи та методології. Складні обчислення в криптографічних стратегіях стають їх основними недоліками і роблять ці політики непридатними для розгортання в БСМ, які мають серйозні обмеження по потужності. Деякі легкі криптографічні механізми доступні в літературі, але вони не відповідають поставленій меті в повній мірі. Тому залишається нагальна потреба дослідити аспект надійності бездротової сенсорної мережі та знайти деякі додаткові засоби, щоб додати більше довіри до загального сценарію. Моделі довіри та репутації є рішенням даної проблеми для дотримання надійності в бездротових сенсорних мережах [28]. Саме тому дослідження моделей довіри і репутації набрали значних обертів за останні кілька років. У минулому було запропоновано багато моделей довіри та репутації. Деякі з них були зосереджені на безпечній маршрутизації, агрегації даних, виборі голови кластера і синхронізованому управлінні довірою, але все ще існує потреба у вирішенні різних питань, таких як змова, масштабованість, мобільність і обчислюваність в БСМ . В даний час більшість систем оцінки довіри належать до алгоритмічної методології, від якої залежить вся поведінка вузлів - точність, зручність використання ресурсів і споживання енергії. Тому необхідно зосередитися на цих питаннях паралельно з їхньою продуктивністю і деякими аспектами реального часу, такими як змова і шахрайське середовище. Змовою можна назвати певний рівень ймовірності, з яким кожен зловмисний сервер присвоює максимальний рейтинг іншим зловмисним серверам і мінімальний рейтинг доброзичливому серверу. В результаті, найбільш слухняний вузол буде не в змозі надавати свої послуги системі більшу частину часу, що в подальшому серйозно вплине на загальну продуктивність системи. Присутність зловмисних серверів у БСМ є основною і реальною першопричиною параметру змови. Тому

така специфічна проблема, як змова, повинна бути вирішена, щоб розширити можливості всієї структури БСМ. Тому обрано п'ять популярних моделей довіри та репутації для їх порівняння та оцінки з точки зору точності, довжини шляху, задоволеності та енергоспоживання. Це дослідження фокусується на проблемі змови і представляє аналіз в екстремальному шахрайському середовищі.

Eigen Trust Model (Модель власної довіри) - це модель довіри на основі репутації, яка використовується в однорангових мережах. Її запропонували Сепандар Д. Камвар, Маріо Т. Шлоссер та Ектор Гарсія-Моліна у 2003 році [28].

Модель власної довіри використовується для виявлення та запобігання зловмисній поведінці в БСМ, де вузли часто розподілені у віддаленому та ворожому середовищі, що робить їх вразливими до різних типів атак. Присвоюється значення довіри кожному вузлу мережі на основі зворотного зв'язку від інших вузлів. Значення довіри представляє ступінь довіри, яку інші вузли мають до конкретного вузла. Значення довіри оновлюється ітеративно на основі принципу потоків репутації, що означає, що на значення довіри вузла впливають значення довіри інших вузлів, які його оцінили.

У БСМ модель власної довіри може бути використана для виявлення різних типів атак, включаючи атаки на маршрутизацію, атаки на компрометацію вузлів і атаки на відмову в обслуговуванні. Наприклад, якщо вузол отримує інформацію про те, що інший вузол надсилає шкідливі дані або скидає пакети, його значення довіри до цього вузла зменшиться, і це зменшить ймовірність пересилання пакетів через цей вузол. Модель власної довіри показала свою ефективність у запобіганні зловмисній поведінці в мережах БСМ . Вона була використана в декількох додатках, включаючи моніторинг навколишнього середовища, виявлення вторгнень і військове спостереження.

Peer Trust Model (Модель однорангової довіри) - це механізм безпеки на основі довіри, який використовується для виявлення та запобігання зловмисній поведінці в БСМ. Вона була запропонована Юн Чжоу та Сяопін Вангом у 2007 році. У цій моделі поєднано багато аспектів, пов'язаних з управлінням довірою та репутацією, таких як зворотній зв'язок, який пейджер отримує від інших пейджерів,

загальна кількість транзакцій пейджера, довіра до рекомендацій, наданих пейджером, фактор контексту транзакції та фактор контексту спільноти [28].

Bioinspired Trust and Reputation Model (BTRM-WSN) - це механізм безпеки, заснований на довірі, який натхненний біологічними системами. Він був запропонований Мохамадом Бадра і Назаром Закі в 2013 році [28].

BTRM базується на концепції імунної системи живих організмів, де імунна система захищає організм від чужорідних об'єктів, таких як бактерії та віруси. BTRM використовує подібний підхід для виявлення і запобігання зловмисній поведінці в БСМ. У BTRM кожен вузол мережі має імунну систему, яка захищає його від атак. Імунна система відповідає за виявлення атак і реагування на них, а також за оновлення репутації вузла і значень довіри. Імунна система використовує набір антитіл, специфічних для різних типів атак. Коли вузол виявляє атаку, він виробляє антитіло, специфічне для цієї атаки, і ділиться ним з іншими вузлами в мережі. BTRM також використовує підхід, заснований на репутації, для оцінки надійності вузлів.

Загалом, BTRM забезпечує біологічно натхненний і ефективний підхід до захисту глобальних мереж, і він має потенціал для використання і в інших розподілених системах.

The Local Feedback-based Trust Model (LFTM) Ця лінгвістична нечітка модель довіри використовує концепцію нечітких міркувань. З одного боку, вона використовує силу представлення лінгвістично позначених нечітких множин для задоволення клієнта або доброчесності сервера. З іншого боку, на нього впливає сила виведення нечіткої логіки, як, наприклад, неточна залежність між початково запитаною послугою і фактично отриманою, або покарання, яке слід застосувати у випадку шахрайства. Очікуваним результатом буде легко інтерпретована система з адекватною продуктивністю. У цій моделі набір лінгвістичних міток, що описують кілька рівнів змінної або поняття, може бути пов'язаний з нечіткою множиною. Отримана множина складається з таких лінгвістичних міток, як «дуже низький», «низький», «середній», «високий» і «дуже високий». Ці визначені нечіткі множини, пов'язані з такими мітками, визначають рівень задоволеності клієнта [28].

Trust and Reputation Infrastructure Based Proposal (TRIP) Models - ця модель ґрунтується на специфічних особливостях середовища, таких як інфраструктура, площа, щільність і т.д., в межах заданих умов. Кожного разу, коли вузол отримує сигнал від іншого вузла, він оцінює репутацію цього вузла, щоб відхилити або скинути повідомлення, виходячи з його надійності. Кожне повідомлення відображає його фактичний рівень важливості або ризику. Навіть шкідливе повідомлення не вплине на систему через те, що кожне повідомлення має свій рівень довіри. Чим вищий рівень довіри, тим більша ймовірність його відбору. Крім того, розрахунок оцінки репутації для кожного повідомлення базується на трьох різних аспектах, а саме: інформація безпосередньо від цілей, інформація від сусідніх вузлів і інформація від центрального вузла. Інформаційна база даних з усіх трьох джерел може зберігатися в центральному блоці. Беручи до уваги всю інформацію, можна легко прийняти найкраще і найдоцільніше рішення [28].

3.3 Симулятор моделей довіри та репутації для БСМ

Існує велика кількість мережевих симуляторів, які дозволяють тестувати низькорівневі протоколи зв'язку. Тим не менш, бракує симуляторів, спрямованих на перевірку коректності та точності моделей довіри та репутації для розподілених систем і, зокрема, для БСМ. Актуальність і корисність розподілених мереж зростає з кожним днем завдяки численним застосуванням і дослідницьким зусиллям, які зосереджені на них. Зокрема, БСМ широко розповсюджені і використовуються у багатьох сценаріях, таких як виявлення пожеж, вимірювання погоди і навіть управління трафіком у мережах типу V2V. Проте, цей тип мереж має свої недоліки: безпроводовий спосіб зв'язку, обмеженість батареї і пропускної здатності або розташування у відкритому середовищі, наприклад, призводять до певних загроз для безпеки. Останнім часом управління довірою та репутацією стало новим способом вирішення деяких з цих важливих питань.

Для тестування нових протоколів зв'язку та перевірки їх коректності, стійкості та точності було розроблено багато мережевих симуляторів. Автори

PGNet, наприклад, представляють огляд симуляторів P2P-мереж, описуючи їх основні можливості та обмеження. Однак, незважаючи на значну кількість таких симуляторів, існує брак моделей довіри та репутації для симуляторів розподілених мереж. Одним з небагатьох розроблених і опублікованих є TOSim. Він був створений як високомодульний і конфігурований, без надмірного перевантаження як з точки зору пам'яті, так і часу. Для того, щоб імітувати поведінку, пов'язану з довірою, автори розглядають чотири моделі загроз з боку зловмисних однорангових користувачів, які можуть спричинити завантаження небезпечного контенту в систему. Іншою важливою платформою для імітації моделей репутації є ART, який в останні роки став еталонним середовищем в області моделей репутації для мультиагентних систем. Цей тестовий стенд слугує набором інструментів зі змінними параметрами, що дозволяє дослідникам проводити кастомізовані та легко повторювані експерименти. Проте не знайдено жодного симулятора середовища, орієнтованого на системи довіри та репутації для БСМ. Тому, TRMSim-WSN є першим інструментом для моделювання довіри та репутації, що охоплює цю мету [29].

Симулятор TRMSim-WSN на основі подій Java версії 0.5 для безпроводової сенсорної мережі, що дозволяє дослідникам моделювати і представляти випадкові розподіли в мережі, а також надає статистику різних політик розповсюдження даних, в тому числі для тестування різних стратегій моделей довіри і репутації. Багато рішень, таких як статичні, динамічні або осцилюючі мережі, комбінація динамічних і осцилюючих мереж, відсоток шахрайських вузлів, відсоток вузлів, що діють як клієнти або сервери, і так далі, можуть бути реалізовані і протестовані на ній. На рисунку 3.1 показано меню програми TRMSim-WSN.

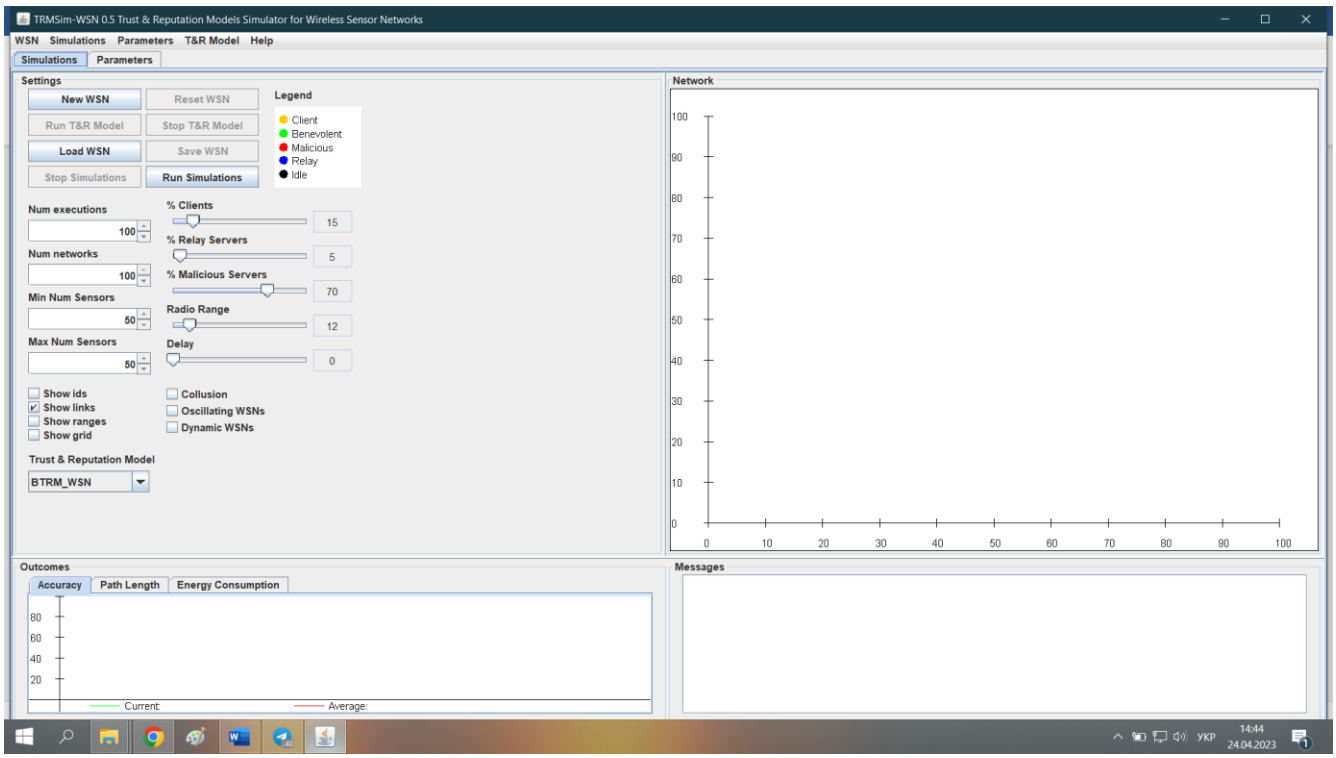

Рис.3.1.Меню TRMSim-WSN

Перший крок, який потрібно зробити при використанні TRMSim-WSN - це створити нову БСМ. Для цього є два поля, де можна вказати максимальну та мінімальну кількість датчиків, які ми хочемо мати в мережі, а також повзунок для встановлення радіусу дії безпроводового зв'язку для кожного датчика. Ці три параметри визначатимуть щільність зв'язків у мережі (тобто сусідство кожного вузла). Крім того, можна вибрати, який відсоток вузлів потрібно зробити клієнтами, що вимагають обслуговування за замовчуванням. Решта з них будуть діяти, таким чином, як сервери. Також можна вказати, який відсоток цих серверів не буде надавати необхідний сервіс і буде діяти лише як ретрансляційні вузли. Щодо серверів, які насправді надають потрібний сервіс, можна визначити відсоток тих, які будуть зловмисниками, тобто надаватимуть не той сервіс, який вони насправді пропонують, а гірший або взагалі ніякого сервісу. Після того, як встановлено всі ці параметри відповідно до потреб, можна створити нову випадкову БСМ, просто натиснувши кнопку «New WSN» внизу. Також можна завантажити БСМ з XML-файлу, натиснувши кнопку «Load WSN», і зберегти поточну БСМ у XML-файл, натиснувши кнопку «SaveWSN». Якщо є потреба оцінити готову БСМ, але з іншою

щільністю зв'язку, можна змінити параметр діапазону безпроводовго зв'язку і натиснути кнопку «Reset WSN».

Наступне, що потрібно налаштувати - це параметри симуляції. По-перше, можна визначити кількість виконань для симуляції, тобто кількість разів, коли кожен клієнт в мережі буде запитувати свою послугу за замовчуванням, використовуючи обрану модель довіри та репутації. Також можна встановити кількість різних випадкових БСМ, які потрібні, відповідно до налаштувань, описаних попередньо. Можна прийняти деякі рішення щодо візуального або графічного представлення мереж, які тестуються в симуляціях. Наприклад, вирішити, чи потрібно, щоб були показані безпроводові діапазони чи ні, а також датчики з'єднань або ідентифікатор кожного з них. Панель параметрів дозволяє встановити файл вхідних параметрів або вручну вказати значення кожного параметра, необхідного для поточної обраної моделі довіри та репутації. Оскільки однією з основних характеристик БСМ є обмеження щодо заряду батареї та споживання енергії, можна також змоделювати динамічну БСМ, в якій деякі датчики на деякий час переходять у стан очікування, якщо вони не отримують жодного запиту протягом певного періоду часу. Датчик у стані очікування не приймає і не передає жодних повідомлень або пакетів. Після певного часу очікування вони знову прокидаються. Після того, як встановлено всі попередні налаштування, можна розпочати симуляцію. Якщо потрібно запустити симуляцію тільки в поточній мережі, треба натиснути «Run WSN», кнопка «Stop WSN» дозволяє нам примусово завершити симуляцію. В іншому випадку, щоб запустити симуляцію для заданої кількості випадкових БСМ , потрібно натиснути кнопку з «Run Simulations». Можна зупинити симуляцію, натиснувши кнопку «Stop Simulations», і буде показано поточні результати. Також є можливість додати деяку затримку між кожною змодельованою мережею, якщо потрібно перевірити топологію кожної протестованої БСМ. Максимальне значення відповідає одній секунді.

Для того, щоб перевірити точність кожної імітованої моделі довіри та репутації, в симулятор включено дві загрози безпеці. Перша загроза пов'язана з

коливальною поведінкою серверів, що надають запитувані послуги. Таким чином, якщо обрано цю опцію, після кожних 20 виконань (тобто транзакцій або взаємодій), кожен зловмисний сервер стає доброзичливим. Потім той самий відсоток випадковим чином обирається, щоб стати зловмисними. За такої схеми зловмисний сервер може залишатися зловмисним і після 20 виконань. Друга загроза безпеці полягає у можливості змови зловмисних серверів між собою. Це означає, що кожен зловмисний сенсор буде давати максимальну оцінку кожному іншому зловмисному сенсору і мінімальну оцінку кожному доброзичливому. Хороша модель довіри і репутації повинна швидко реагувати на ці зміни поведінки і змови і переналаштовуватися, щоб запобігти вибору зловмисного вузла як найбільш надійного або авторитетного .

Дві панелі допомагають дізнатися, що відбулося або відбувається в симуляторі, і які результати останньої симуляції. На панелі повідомлень на рисунку 3.2, наприклад, показано кілька повідомлень, що містять корисну інформацію, наприклад, момент початку або завершення останньої симуляції, або те, яка саме мережа тестується в даний момент.

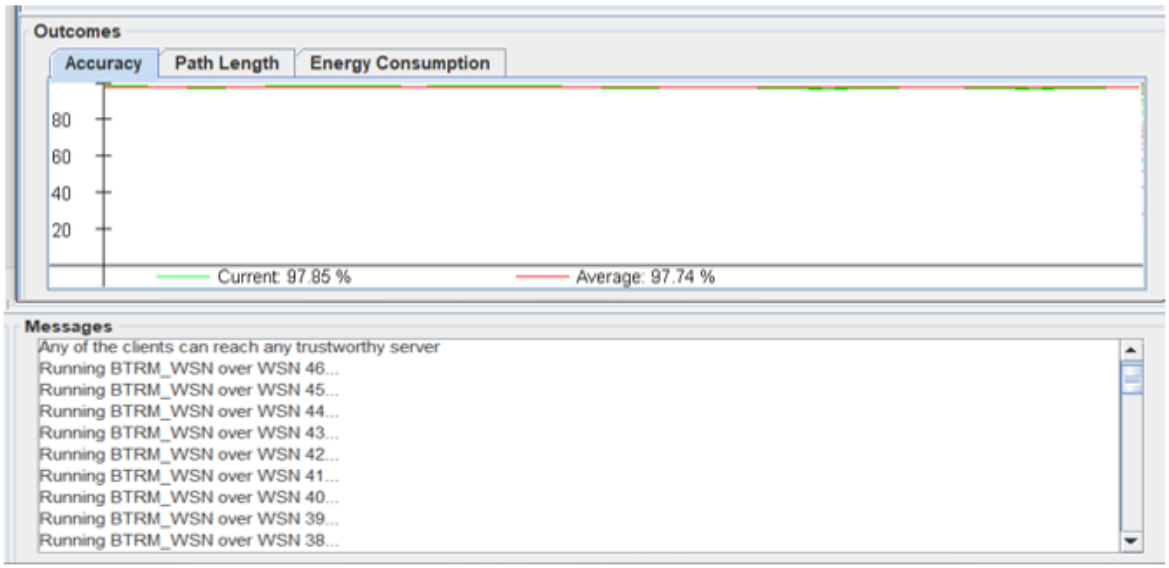

Рис.3.2. Панелі повідомлень

З іншого боку, панель результатів дозволяє дізнатися результати поточної змодельованої мережі або середні результати для всієї симуляції. Тут можна спостерігати три важливі величини: точність моделі, середню довжину всіх шляхів,

знайдених кожним клієнтом кожної змодельованої мережі, та енергію, спожиту моделлю. Додаткові панелі можна легко додати, якщо потрібно показати більше деталей про експерименти. Середня задоволеність обчислюється, збираючи задоволеність кожного клієнта, що належить до кожної з протестованих мереж БСМ. Однак клієнти, які не можуть зв'язатися з будь-яким доброзичливим сервером, не беруться до уваги при обчисленні цих результатів (оскільки будь-яка модель довіри та репутації є корисною в такій ситуації).

3.4 Реалізація моделей довіри та репутації на основі змови в екстремальному шахрайському середовищі через статичні та динамічні безпроводові сенсорні мережі

Дослідження зосереджено на трьох параметричних аспектах, а саме: точності, довжині шляху та споживанні енергії для поширення інформації в БСМ. Для цього розроблено сценарій без пом'якшення, який визначає дві основні цілі. По-перше, знаходженні значень трьох вищезгаданих параметрів для статичної БСМ з урахуванням та без урахування аспекту змови. Меншій довжині шляху роботи вузла завжди приділяється належна увага, оскільки вона споживає менше ресурсів і демонструє більшу ефективність. По-друге, оцінено вплив мобільності на продуктивність зв'язку в кореляції зі змовою для різних моделей довіри та репутації. Проведено комплексну оцінку споживання енергії статичними і динамічними БСМ в запропонованій структурі.

Розроблено шаблон БСМ, використовуючи наступні параметри: 20% всіх вузлів у випадково створеній БСМ виступали в якості клієнтів, а решта 80% вузлів виступали в якості серверів. Під клієнтськими вузлами мається на увазі відсоток вузлів, які хочуть мати або запитують послуги у БСМ. 5% вузлів працювали як ретрансляційні сервери, які не надають жодних послуг.Радіус дії радіозв'язку вузлів встановлений на рівні 10 хопів до своїх сусідів. Розглянуто сценарій, в якому відсоток шахрайських серверів залишився на рівні 70%, що визначає обов'язкову умову для оцінки фреймворку БСМ. Шахрайські сервери відображають відсоток

супротивників у БСМ. Встановлено мінімальну та максимальну кількість вузлів, які можуть створити БСМ, рівними 200. Сенсорні вузли, що належать до розроблених мереж, розкидані на площі 100 м×100 м. Всього було досліджено десять мереж, а остаточні результати відображають середнє значення всіх мереж. Процес пошуку надійного сервера проводився десять разів для кожної мережі. На рисунку 3.3 показано налаштування симуляції. У вікні симуляції жовті точки позначають клієнтські вузли, зелені точки - доброзичливі вузли, червоні точки - зловмисні вузли, сині точки - ретрансляційні вузли, а чорні точки - простоюючі вузли відповідно.

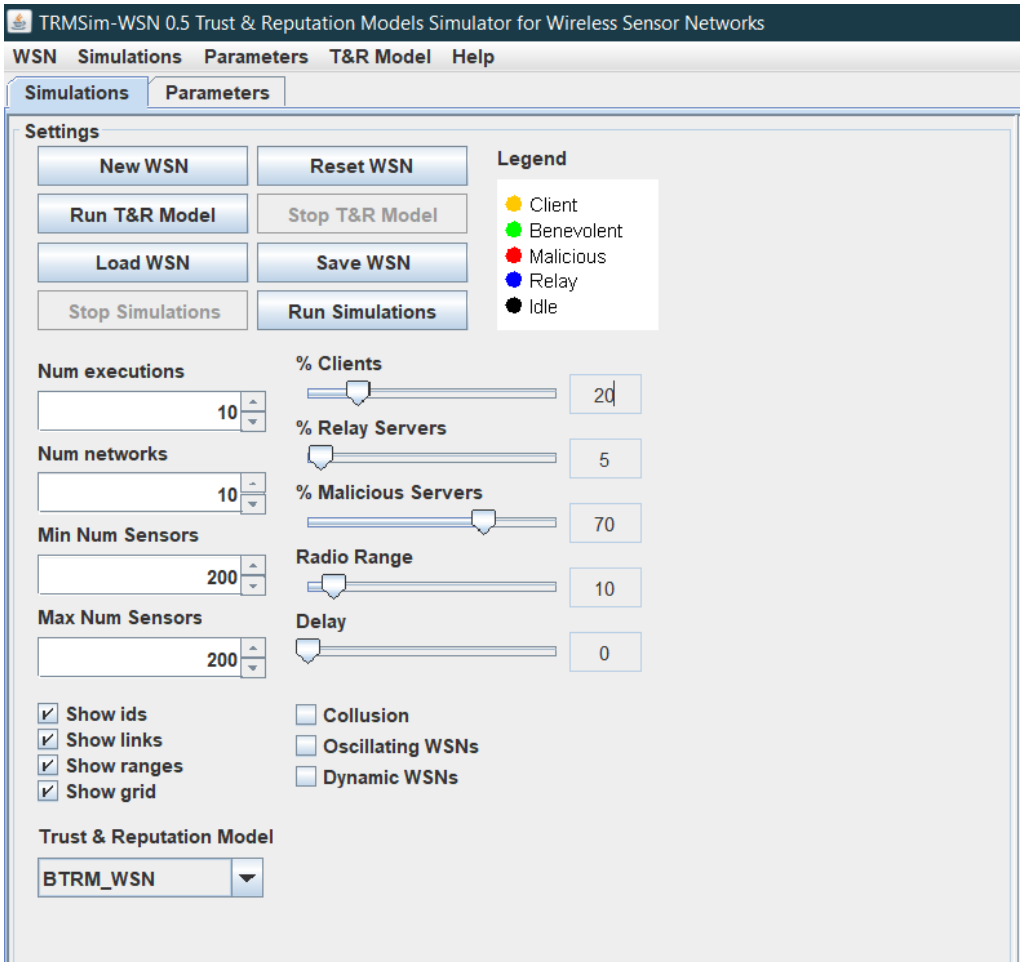

Рис.3.3. Налаштування симуляції

Проведено комплексний аналіз на основі змови зі статичними та динамічними БСМ. Зібрано дані для чотирьох метрик, а саме: точності, довжини шляху, задоволеності та енергоспоживання. Дослідженл порівняльний аналіз моделей довіри та репутації зі статичними БСМ та динамічними, з параметром

змови та без нього. Статичний вузол відноситься до типу вузлів, положення яких залишається фіксованим, тоді як динамічний вузол може бути мобільним у мережі. Розглянуто чотири режими БСМ , а саме: статична БСМ (SW), статична БСМ зі змовою (SWC), динамічна БСМ (DW) та динамічна БСМ зі змовою (DWC).

Точність. Поняття точності в системах довіри та репутації можна визначити як вибраний відсоток надійних вузлів. Параметр точності розраховано в термінах їх поточного та середнього значення. Поточна точність означає значення надійності, розраховане для останнього вузла, тоді як середня точність представляє значення всіх вузлів, доступних у згаданому фреймворку. Спочатку розраховано середню точність, яка відповідає різним моделям довіри та репутації, як показано на рисунку 3.4. Значення поточної точності залишається найвищим у випадку статичної БСМ порівняно з іншими режимами БСМ через те, що статичні вузли менш схильні до збоїв, ніж динамічні, а також через поєднання статичної та динамічної БСМ з аспектом змови.

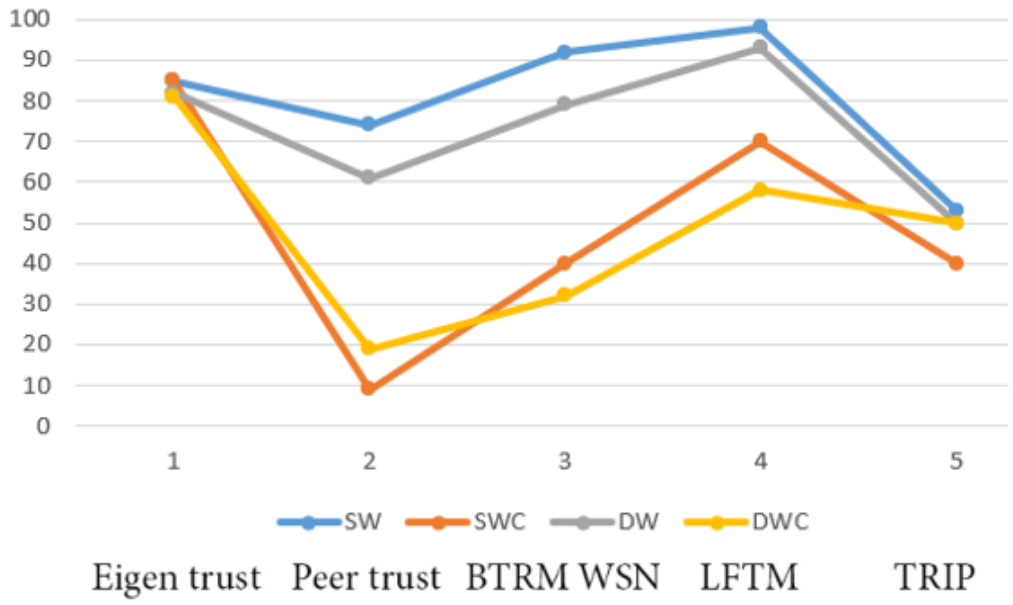

Рис.3.4. Поточна точність різних режимів БСМ з моделями довіри та репутації

Модель власної довіри відмічено значенням 1, модель рівноправної довіри - значенням 2, модель BTRM-WSN - значенням 3, модель LFTM - значенням 4, а модель TRIP - значенням 5.

Проведено другу оцінку середньої точності з тією ж структурою БСМ. Згідно з рисунком 3.5 , середня точність знову демонструє подібну поведінку до поточної точності на рисунку 3.4, оскільки значення середньої точності залишається найвищим у випадку статичної БСМ , ніж у решті режимів БСМ . Для режимів статичної БСМ (SW) та динамічної БСМ (DW) значення поточної та середньої точності залишається найвищим у моделі LFTM, ніж в інших моделях у більшості випадків шахрайства, тоді як модель TRIP демонструє мінімальне значення. У випадку статичного режиму БСМ зі змовою (SWC) та динамічного режиму БСМ зі змовою (DWC) модель власної довіри випереджає інші моделі за поточним та середнім значенням точності, тоді як модель пірінгової довіри демонструє мінімальне значення точності. Існує серйозний вплив змови і мобільності вузлів на точність системи БСМ, оскільки точність знижується до дещо складного рівня, коли вузол змінює свій стан зі статичного на динамічний.

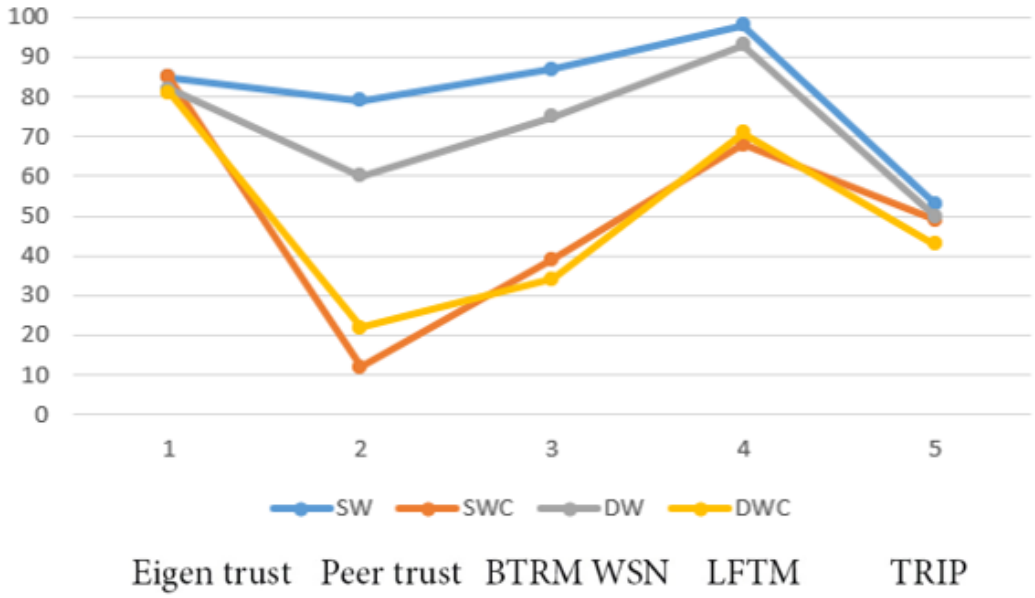

Рис.3.5. Середня точність різних режимів БСМ з моделями довіри та репутації

Довжина шляху. Наступним параметром є довжина шляху, яку можна визначити як кількість ресурсів, що використовує певна мережа з певною моделлю довіри та репутації. В рамках послідовної схеми оцінювання типів точності оцінено поточну та середню довжину шляху за аналогічною схемою точності для всіх

режимів роботи БСМ . Поточна довжина шляху відображає значення використання ресурсів, розраховане для останнього вузла, тоді як середня довжина шляху відображає значення для всіх вузлів, присутніх у сценарії. На рисунках 3.6 та 3.7 показано значення поточної та середньої довжини шляху, які у випадку моделі TRIP залишаються незмінними як для поточного, так і для середнього сценарію, порівняно з іншими моделями. Це пов'язано з тим, що модель TRIP має фіксовану інфраструктуру для своєї функціональності, що призводить до меншої довжини шляху порівняно з іншими моделями. Серед інших моделей модель LFTM споживає меншу довжину шляху, ніж інші моделі, у випадку режиму SW та режиму DW, тоді як режими SWC та DWC моделі BTRM використовують мінімальну довжину шляху.

Рис.3.6. Довжина шляху в різних режимах БСМ з моделями довіри та репутації

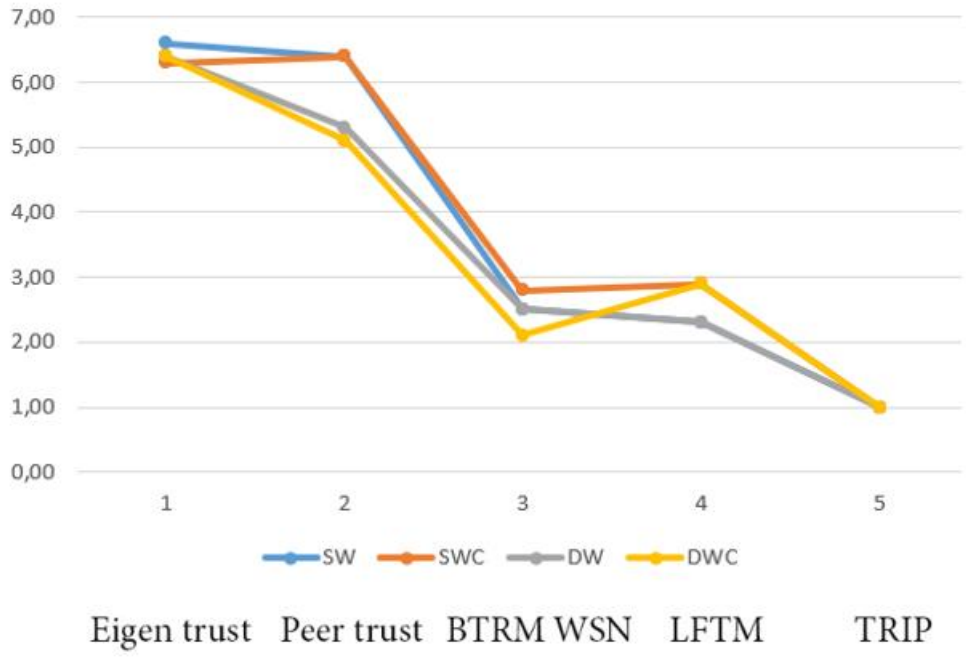

Рис.3.7. Середня довжина шляху в різних режимах БСМ з моделями довіри та репутації

BTRM використовує максимальну довжину шляху для всіх режимів SW, SWC, DW і DWC . Це показує відмінне узгодження з результатами, наведеними в роботі.

Задоволеність. Крім того, розраховано рівень задоволеності різними режимами БСМ для моделі LFTM, як показано на рисунку 3.8. В контексті моделей довіри і репутації, задоволеність можна визначити як певний рівень суб'єктивності до певної міри, в якій система може поводитися відповідно до бажаної мети із зазначеною ймовірністю. Спостереження показують, що в статичному режимі рівень задоволеності є дуже високим порівняно з іншими режимами БСМ, тоді як включення змови в режимах SW і DW зменшує його значення.

Рис.3.8. Аналіз задоволеності за допомогою моделі довіри та репутації LFTM

Однією з основних проблем при роботі з БСМ є енергоспоживання. Було проведено аналіз середнього енергоспоживання в режимах SW, SWC, DW та DWC п'яти моделей довіри та репутації в БСМ . Потреба в енергії сенсорного вузла може бути проаналізована як функція. Для більшості моделей споживання енергії E повідомленням на відстані d визначається за формулою

$$E(d)=d^{\alpha}+C, \qquad (3.1.)$$

де α - коефіцієнт затухання, а C - константа, яка використовується для радіосигналу і є безрозмірною.

У таблиці 3.1 порівнюються п'ять моделей довіри та репутації з точки зору енергоспоживання.

Таблиця 3.1

Споживання енергії для моделей довіри та репутації з режимами БСМ

Моделі довіри та репутації з режимами БСМ	Eigen trust(mj)	Peer trust(mj)	BTRM(mj)	LFTM(mj)	TRIP(mj)
SW	8.2×10^{24}	8.7×10^{16}	4×10^{17}	2.5×10^{17}	4×10^{9}
SWC	6.4×10^{24}	1×10^{17}	8×10^{17}	1.4×10^{18}	4×10^{9}
DW	5.1×10^{24}	3.2×10^{16}	1.1×10^{17}	1.2×10^{17}	4×10^{9}
DWC	8.6×10^{24}	2.2×10^{16}	6.8×10^{17}	7.6×10^{17}	4×10^{9}

Модель власної довіри споживає максимальну потужність у всіх режимах SW, SWC, DW і DWC, тоді як модель TRIP показала мінімальне споживання енергії. Більша складність моделі власної довіри є причиною максимального споживання енергії, а у випадку моделі TRIP споживання енергії є мінімальним через простіші обчислення, пов'язані з обчисленням значення довіри. Математичну залежність споживання енергії для моделей довіри та репутації в системі:

$$E_O = E_C + E_S + E_F + E_R + E_{Sim}, \quad (3.2.)$$

де E_O загальне споживання енергії, E_C позначає енергоспоживання клієнтських вузлів, E_S показує енергоспоживання серверних вузлів, E_F показує енергоспоживання шахрайського вузла, E_R енергоспоживання релейного вузла, а E_{Sim} позначає енергоспоживання симулятора.

Загалом, досліджено весь фреймворк двадцять разів для різних режимів БСМ і відповідних п'яти моделей довіри та репутації. Чим складніша модель довіри та репутації, тим більше вона використовує ресурсів та споживає більше енергії. Використано різноманітні стратегії оцінювання, засновані на точності, довжині шляху, задоволеності та енергоспоживанні для операцій сенсорних вузлів у запропоновану структуру, що робить сценарій надійним.

З прийняттям змови в режимах БСМ відбувається деградація продуктивності. У випадку статичних вузлів, змова менше впливає на БСМ, коли вона включена в динамічний режим. Крім того, операції вузлів залишаються більшими у випадку

змови, ніж без неї. З цього дослідження видно, що чим менше вузлів, що змовилися, тим більша ймовірність точності, краще використання ресурсів, адекватний рівень задоволеності і менше споживання енергії всією БСМ буде демонструвати система.

Висновки до третього розділу

Проаналізовано та порівняно засоби моделювання для БСМ. Проведена оцінка представляє, що таке БСМ, чому вони вимагають моделювання та які основні моменти слід розглядати одночасно з моделюванням БСМ.

Досліджено вплив змови на різні моделі довіри та репутації у БСМ. З моделювання видно, що існує сильний взаємозв'язок між змовою і режимами БСМ в оцінці моделі довіри і репутації.

Оцінено фреймворк БСМ на предмет змови за чотирма показниками продуктивності, а саме: точність, довжина шляху, задоволеність та енергоспоживання. Оцінено точність і довжину шляху у відсотках від загальної функціональності, тоді як споживання енергії - у міліджоулях, спеціально для операцій сенсорних вузлів. Продуктивність системи БСМ змінюється разом з різними режимами і змовами, присутніми в сценарії.

ВИСНОВКИ

В бакалаврській роботі отримано наступні теоретичні та наукові результати:

1) Проаналізовано основні поняття та принципи сенсорних мереж.

2) Визначено переваги БСМ такі як: економічність, гнучкість, мобільність, енергоефективність, моніторинг в реальному часі. Та визначено недоліки: обмежений радіус дії та пропускна здатність, проблеми безпеки.

3) Описано методи маршрутизації та модель створення гетерогенної безпроводової мережі, причини переваги гетерогенної мережі над гомогенною.

4) Виокремлені методи боротьби з вразливістю БСМ. Для усунення загроз безпеки можуть бути реалізовані різні заходи безпеки, такі як шифрування, автентифікація і безпечні протоколи зв'язку.

5) Охарактеризовано симуляційні програми для створення моделі БСМ. Визначено їх переваги та недоліки

6) Реалізовано моделі довіри та репутації на основі змови в екстремальному шахрайському середовищі через статичні та динамічні безпроводові сенсорні мережі. Ця робота дозволяє аналітично сформулювати стратегії розслідування за визначеними сценаріями і, отже, дає уявлення про те, як керувати визначеною моделлю для еволюції безпроводових сенсорних мереж. Дотримуючись цих рекомендацій, можна захистити безпроводову сенсорну мережу від загроз і забезпечити її надійність.

7) Зроблено висновок, що БСМ стають дедалі популярнішими завдяки можливості моніторингу та збору даних з віддалених або важкодоступних місць. Незважаючи на проблеми, БСМ мають багато потенційних застосувань, включаючи моніторинг навколишнього середовища, промислову автоматизацію, моніторинг здоров'я та розумні міста. Завдяки постійним дослідженням і розробкам, потенціал безпроводових сенсорних мереж для революційної зміни способу збору і аналізу даних в широкому спектрі галузей і застосувань є величезним.