ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Алгоритми виявлення атак і забезпечення безпеки в бездротових сенсорних мережах»

на здобуття освітнього ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

(код, найменування спеціальності)

освітньо-професійної програми Телекомунікаційні системи та мережі

(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Сергій ГОЛОВАШ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Сергій ГОЛОВАШ
Ім'я, ПРІЗВИЩЕ

Керівник: Катерина ДОМРАВЧЕВА
Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут телекомунікацій

Кафедра Телекомунікаційних систем та мереж

Ступінь вищої освіти магістр

Спеціальність 172 Телекомунікації та радіотехніка

Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ

Завідувач кафедрою ТСМ

_____ Віктор ЗАЇКА

«____» _____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Головаш Сергій Олександрович

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Алгоритми виявлення атак і забезпечення безпеки в бездротових сенсорних мережах.
Керівник кваліфікаційної роботи Катерина ДОМРАЧЕВА, к.т.н., доцент

(Ім'я, ПРІЗВИЩЕ)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи: «___» _____2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Методи аналізу ефективності алгоритмів виявлення атак та механізмів безпеки у WSN.
2. Класифікація сучасних кібератак та існуючих систем виявлення вторгнень.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Актуальність роботи та мета дослідження.
2. Аналітичний огляд теоретичних основ функціонування бездротових сенсорних мереж, існуючих загроз безпеки, класифікації атак та методів їх виявлення..
3. Практичне дослідження алгоритмів виявлення атак та механізмів безпеки.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	30.09.25	Виконано
2	Ознайомлення з предметом дослідження	16.10.25	Виконано
3	Детальний рогляд та організація текстової частини роботи	26.10.25	Виконано
4	Написання текстової частини роботи та експериментальне дослідження можливостей технології	26.11.25	Виконано
5	Висновки, вступ, реферат	30.11.25	Виконано
6	Розробка презентації	10.12.25	Виконано

Здобувач вищої освіти _____ Сергій ГОЛОВАШ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Катерина ДОМРАЧЕВА
(підпис) *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: __ стор., __ рис., __ табл., __ дж..

Мета роботи - дослідити та розробити ефективні алгоритми виявлення атак і механізми забезпечення безпеки в бездротових сенсорних мережах, а також оцінити їхню ефективність і стійкість до сучасних кіберзагроз.

Об’єктом дослідження є бездротові сенсорні мережі.

Предметом дослідження є алгоритми виявлення атак та особливості забезпечення безпеки в бездротових сенсорних мережах, а також оцінка їхньої ефективності та якості.

Короткий зміст роботи:

У першому розділі проведено ознайомлення з теоретичними основами функціонування бездротових сенсорних мереж, їхніми архітектурами, характеристиками та обмеженнями, а також детально розглянуто основні загрози безпеки та класифікацію атак.

У другому розділі детально проаналізовано та класифіковано існуючі алгоритми виявлення атак у бездротових сенсорних мережах, включаючи системи виявлення вторгнень, методи виявлення аномалій, сигнатурні та гібридні підходи.

У третьому розділі проведено обґрунтування, розробку та експериментальну оцінку запропонованих удосконалених алгоритмів виявлення атак і механізмів забезпечення безпеки в БСМ, включаючи моделювання, аналіз отриманих результатів та розробку механізмів протидії атакам і відновлення.

КЛЮЧОВІ СЛОВА: БЕЗПРОВІДНІ СЕНСОРНІ МЕРЕЖІ, WSN, КІБЕРБЕЗПЕКА, АТАКИ, ВИЯВЛЕННЯ ВТОРГНЕНЬ, АЛГОРИТМИ, ЕФЕКТИВНІСТЬ, КРИПТОГРАФІЯ, ЗАХИСТ.

ABSTRACT

Text part of the master`s qualification work: __ pages, __ pictures, __ table, __ sources.

The objective of the work is to study and develop effective attack detection algorithms and security mechanisms in wireless sensor networks, as well as to evaluate their efficiency and resilience against modern cyber threats.

The object of the research is wireless sensor networks.

The subject of the research is attack detection algorithms and the specific features of ensuring security in wireless sensor networks, as well as the evaluation of their effectiveness and quality.

Brief Summary of the Work.

The first chapter provides an overview of the theoretical foundations of wireless sensor network operation, their architectures, characteristics, and limitations. It also thoroughly examines major security threats and the classification of attacks.

The second chapter presents a detailed analysis and classification of existing attack detection algorithms in wireless sensor networks, including intrusion detection systems, anomaly detection methods, signature-based, and hybrid approaches.

The third chapter includes the justification, development, and experimental evaluation of the proposed improved attack detection algorithms and security mechanisms in WSNs, including modeling, analysis of the obtained results, and the development of attack countermeasures and recovery mechanisms.

KEYWORDS: WIRELESS SENSOR NETWORKS, WSN, CYBERSECURITY, ATTACKS, INTRUSION DETECTION, ALGORITHMS, EFFICIENCY, CRYPTOGRAPHY, PROTECTION.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Головаш С. О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Телекомунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Алгоритми виявлення атак і забезпечення безпеки в бездротових сенсорних мережах»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Головаш Сергій Олександрович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану магістерську роботу здобувача Головаша Сергія Олександровича на оцінку «добре» та присвоїти йому кваліфікацію «магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Катерина ДОМРАЧЕВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Головаш С.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 2025 року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістр

здобувача вищої освіти Головаш Сергій Олександрович
(прізвище, ім'я, по батькові)
на тему «Алгоритми виявлення атак і забезпечення безпеки в бездротових сенсорних мережах»

Актуальність.
У наш час бездротові сенсорні мережі активно впроваджуються в різноманітні критично важливі сфери, зокрема в промислову автоматизацію, екологічний моніторинг, медицину, інфраструктуру "розумних" міст та військову галузь. Проте через свою децентралізовану структуру, обмежені технічні ресурси та особливості бездротової передачі даних, ці мережі залишаються вразливими до численних кіберзагроз. З огляду на зростання кількості та складності таких загроз, виникає нагальна потреба у створенні ефективних алгоритмів виявлення атак, які можуть гарантувати безпеку, зокрема конфіденційність, цілісність і доступність як даних, так і самої мережевої інфраструктури. Відсутність надійних засобів захисту може призвести до серйозних економічних втрат, збоїв у критичних процесах або навіть до загроз для безпеки.

Позитивні сторони.
1. Зміст магістерської роботи відповідає завданню. Її автор, показав високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.
2. Текст викладений лаконічно, ясно, послідовно. Графічний матеріал оформлений якісно. Широко використовується сучасна науково-технічна література, включаючи англомовні видання.

Недоліки.
1. У роботі практично розглянуто переважно один тип атаки та один алгоритм детекції, без порівняння з альтернативними підходами.
2. Дослідження виконано на основі програмної симуляції без випробування на реальному апаратному стенді бездротової сенсорної мережі.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "_добре_", а здобувач Головаш Сергій Олександрович заслуговує присвоєння кваліфікації: магістр з телекомунікацій та радіотехніки.*

Рецензент _____ _____
науковий ступінь, вчене звання (підпис) *(Ім'я ПРІЗВИЩЕ)*

ЗМІСТ

ВСТУП..... 10

1 ОСНОВИ ФУНКЦІОНУВАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ ТА ЇХНІ ЗАГРОЗИ..... 12

1.1 Загальні відомості про безпровідні сенсорні мережі..... 12

1.2 Архітектура та основні компоненти. 12

1.2.1 Сенсорні вузли. 14

1.2.2 Проміжні вузли. 15

1.2.3 Центри керування. 16

1.3 Концепція безпеки. 17

1.3.1 Модель загроз та вразливостей. 18

1.3.2 Типові вразливості..... 19

1.4 Класифікація та механізми атак. 20

1.5 Пасивні та активні атаки. 21

1.6 Існуючі криптографічні механізми захисту. 22

1.6.1 Симетричні алгоритми шифрування. 23

1.6.1 Асиметричні алгоритми шифрування..... 24

1.6 Захищені протоколи маршрутизації. 25

Висновки до першого розділу 27

2 МЕТОДИ ТА АЛГОРИТМИ ВИЯВЛЕННЯ АТАК У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ 28

2.1 Підходи до виявлення вторгнень у бездротових сенсорних мережах..... 28

2.1.1 Сигнатурний підхід..... 29

2.1.2 Аномалійний підхід..... 31

2.1.3 Гібридні системи виявлення атак. 32

2.2 Методи оцінки поведінки вузлів..... 33

2.2.1 Моніторинг мережевого трафіку. 34

2.2.2 Аналіз енергоспоживання. 35

2.2.3 Виявлення підозрілої маршрутизаційної активності. 37
2.3 Класифікаційні та машинні алгоритми виявлення атак 38
2.3.1 Метод опорних векторів. 39
2.3.2 Дерева рішень і випадкові ліси. 40
2.3.3 Нейронні мережі та глибинне навчання 41
2.3.4 Байєсівські методи класифікації. 43
2.4 Методи виявлення специфічних атак..... 44
2.4.1 Виявлення атак типу “blackhole”, “sinkhole”, “wormhole”..... 45
2.4.2 Виявлення атак на рівні MAC. 46
2.4.3 Виявлення атак відмови в обслуговуванні (DoS, DDoS)..... 48
2.5 Моделі розподіленого виявлення загроз. 49
2.5.1 Локальні механізми детекції..... 50
2.5.2 Кооперативні та колективні схеми. 52
2.5.3 Узгодження рішень у сенсорних мережах. 53
Висновки до другого розділу..... 55
3 МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АЛГОРИТМУ ВИЯВЛЕННЯ АТАК..... 56
3.1 Вибір атаки для детекції. 56
3.2 Середовище для симуляції сценарію атаки на БСМ. 56
3.3 Опис моделі алгоритму для виявлення загрози. 58
3.4 Оцінка обчислювальної складності та ресурсних витрат. 60
3.5 Методика проведення експерименту. 61
3.6 Аналіз результатів експерименту. 67
3.7 Оцінка ефективності алгоритму та висновки експерименту. 73
3.8 Практичні рекомендації щодо сценаріїв інтеграції алгоритму в БСМ. 75
ВИСНОВКИ 78
ПЕРЕЛІК ПОСИЛАНЬ..... 80
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 83

ВСТУП

Сучасну інфраструктуру вже важко уявити без бездротових сенсорних мереж. Їхній вплив – глобальний. Від промислової автоматизації та агросектору до військових комплексів і медицини – усюди ці технології докорінно змінили підходи до моніторингу. Здатність розподілених вузлів збирати дані в реальному часі не просто підвищує ефективність процесів, а й надає системам небачену раніше автономність.

Проте є і зворотний бік. Відкритість каналів зв'язку та фізична доступність датчиків роблять їх вразливою мішенню. Ситуацію критично ускладнюють апаратні обмеження: сенсори зазвичай мають мінімальний обсяг пам’яті, слабкі обчислювальні потужності та жорстку залежність від заряду батареї. Це створює ідеальний ґрунт для кібератак. Загрози варіюються від порушення конфіденційності та цілісності даних до повного блокування мережі через DoS-атаки. З огляду на те, як швидко еволюціонують методи злому, пошук захисних механізмів стає першочерговим завданням. Алгоритми виявлення атак мають бути не лише надійними, а й ресурсоефективними, щоб не перевантажувати слабкі вузли мережі.

Ця робота присвячена глибокому аналізу та порівняльній характеристиці сучасних алгоритмів виявлення вторгнень. Основна мета дослідження – не лише оцінити існуючі методи, а й сформувати теоретичні й практичні рекомендації щодо їх інтеграції в архітектуру бездротових сенсорних мереж для забезпечення стабільного рівня безпеки.

Методи дослідження БСМ:

- Аналіз наукової літератури з теми дослідження.
- Системний підхід.
- Експериментальне дослідження.
- Оцінка ефективності та якості.

Наукова новизна та практична значущість

Робота має наукову новизну, вона полягає у проведенні всебічного та систематичного порівняльного аналізу передових алгоритмів виявлення атак, адаптованих для умов бездротових сенсорних мереж з обмеженими ресурсами.
Практична значущість роботи полягає у її прямому застосуванні для підвищення рівня безпеки бездротових сенсорних мереж, що використовуються в критично важливих сферах.

Структура роботи

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та демонстраційних матеріалів.

1 ОСНОВИ ФУНКЦІОНУВАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ ТА ЇХНІ ЗАГРОЗИ

1.1 Загальні відомості про безпровідні сенсорні мережі.

Під бездротовими сенсорними мережами (БСМ) розуміють систему автономних пристроїв, які просторово розсереджені на досліджуваній території. Основою такої архітектури є кооперативна робота вузлів: оснащені датчиками, вони спільно моніторять фізичні чи екологічні параметри середовища. Усі зібрані відомості згодом акумулюються та передаються до центрального вузла обробки.

Спектр застосування цих технологій надзвичайно широкий. Вузли здатні фіксувати температуру, вологість, атмосферний тиск, акустичні шуми, рівень забруднення повітря або навіть детестувати рух. Це дає змогу не лише контролювати ситуацію в режимі реального часу, а й формувати ґрунтовну статистичну базу, необхідну для глибокого аналізу та прийняття виважених рішень.

1.2 Архітектура та основні компоненти.

Функціонування БСМ базується на чіткому алгоритмі передачі інформації за вектором «від периферії до центру». Процес ініціюється на рівні сенсорного вузла, проте його роль не обмежується пасивною фіксацією параметрів. Критично важливою є стадія первинної обробки. Оскільки передача даних вимагає значних енерговитрат, вузол часто виконує попередню агрегацію, стиснення або фільтрацію сигналу ще до моменту відправки. Далі вступає в дію механізм транзиту: дані рідко передаються напряму на великі відстані. Зазвичай пакет проходить крізь ланцюжок проміжних вузлів, використовуючи так звану мультихопову маршрутизацію, доки не досягне центру збору інформації.

Роль центру керування у цій архітектурі є визначальною. На відміну від звичайних сенсорів, цей елемент зазвичай має значно вищі обчислювальні

потужності та стабільне джерело живлення. Саме тут відбувається так званий data fusion (злиття даних): потік розрізнених сигналів аналізується, перевіряється на наявність аномалій та перетворюється на структуровану інформацію. Окрім аналітики, центр також відповідає за адміністративні функції – управління топологією мережі, синхронізацію часу та перерозподіл навантаження між вузлами.

У підсумку, центр керування виступає інтелектуальним шлюзом. Він абстрагує складну технічну "кухню" мережі від кінцевого споживача. Користувач взаємодіє не з окремими датчиками, а з уже готовими аналітичними висновками, поданими через зручний інтерфейс. Така ієрархія дозволяє забезпечити ефективний моніторинг, де людина приймає стратегічні рішення на основі даних, підготовлених автоматизованою системою.. Схематичне представлення БСМ зображено на рисунку 1.1.

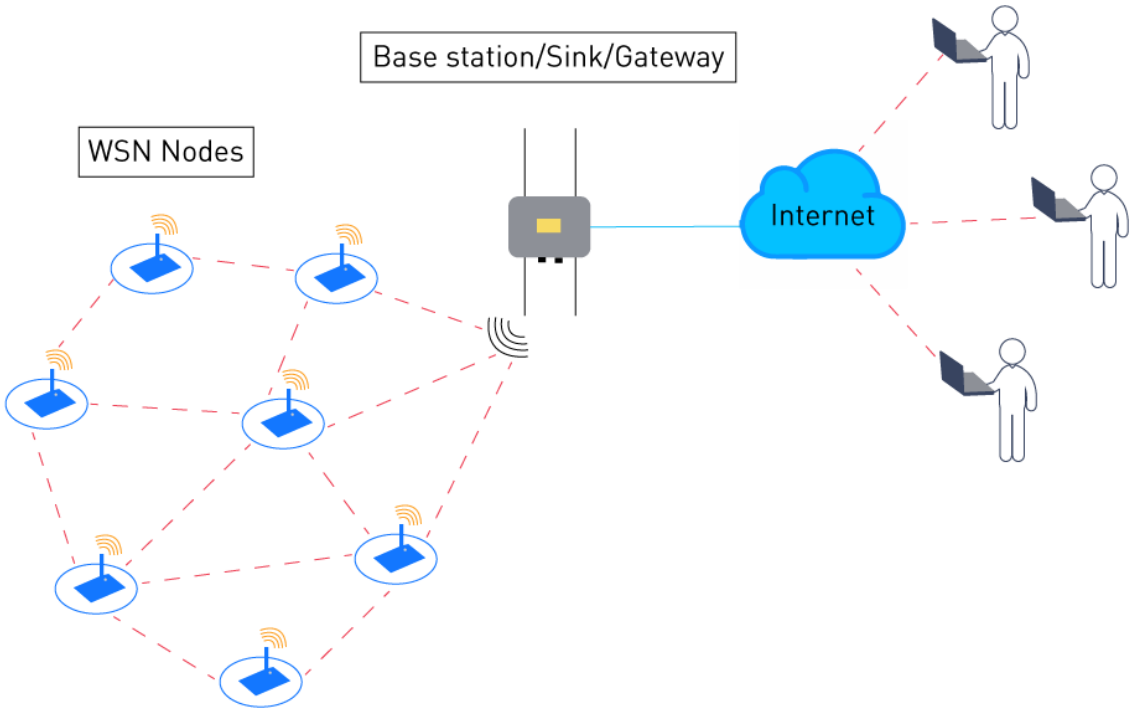


Рис. 1.1 Типова схема безпровідної сенсорної мережі

1.2.1 Сенсорні вузли.

Зазвичай БСМ складається з великої кількості, часто сотень, сенсорних вузлів, які обмінюються даними між собою за допомогою радіозв'язку. Кожен вузол обладнаний різними датчиками, процесорними модулями, прийомопередавачами та елементами живлення. Після розгортання вузли самостійно формують необхідну мережеву інфраструктуру, після чого розпочинають збір потрібних даних. Окрім цього, сенсорні вузли можуть реагувати на запити, що надходять із базової станції, виконуючи певні команди або передаючи параметри моніторингу. Режим роботи вузлів може бути постійним або активуватись лише під час виявлення певної події.

Основною складовою безпровідної сенсорної мережі є сенсорний вузол, нод, який по суті є мініатюрним комп'ютером з обмеженими ресурсами. Кожен такий вузол типово складається з декількох частин: мікроконтролера, який виконує роль процесорного блоку, радіопередавача з антеною для безпровідної комунікації, електронної схеми для комунікації з датчиками, так званий сенсорний блок, що включає сенсори та аналогово-цифрові перетворювачі, а також джерела енергії, зазвичай батареї. Приклад структурної схеми сенсорного вузла зображений на рисунку 1.2.

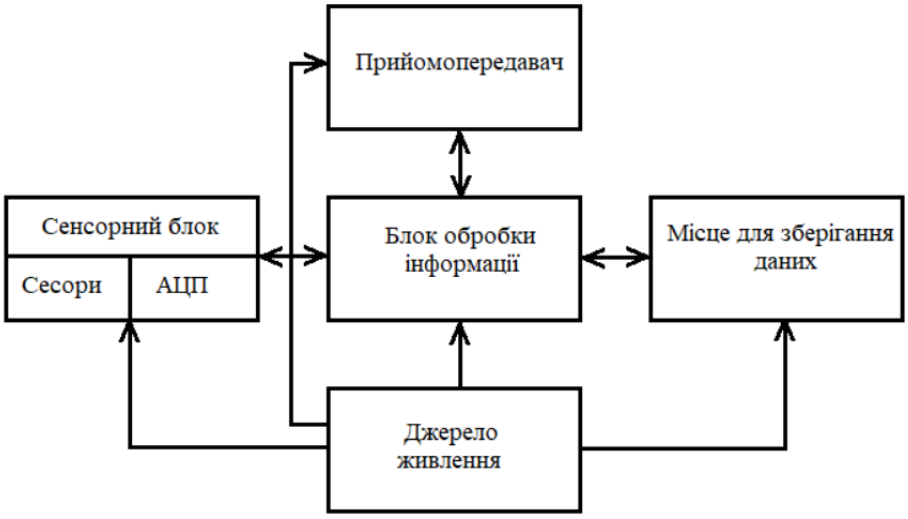


Рис. 1.2 Блок-схема нода (сенсорного вузла)

Набір сенсорних чутливих пристроїв, як правило, містить дві складові: самі сенсори та аналого-цифровий перетворювач (АЦП). Фундаментальний принцип дії такий: сенсорні елементи фіксують потрібні характеристики та трансформують їх у форму аналогового імпульсу. АЦП, зі свого боку, здійснює перетворення цього аналогового імпульсу на цифровий формат і далі надсилає його модулю опрацювання даних. Цей модуль опрацьовує отриманий аналоговий сигнал, встановлюючи чи виявляючи зміну статусу контрольованого об'єкта або фіксуючи певну подію, здійснюючи це через зіставлення здобутого значення з попередньо заданим пороговим значенням. Услід за цим, імпульс направляється до приймально-передавального апарату. Він функціонує як засіб для налагодження комунікації між окремими компонентами сенсорної мережі. Для забезпечення енергопостачання усіх перелічених модулів залучається відповідне джерело енергії.

1.2.2 Проміжні вузли.

У типовій БСМ не всі сенсорні вузли можуть напряму передати дані до базової станції через обмежений радіус зв’язку або енергетичні ресурси. Тому в деяких конфігураціях має місють місце проміжні вузли, які ще іноді називають транзитними. Такий сетап схематично зображено на рисунку 1.3.

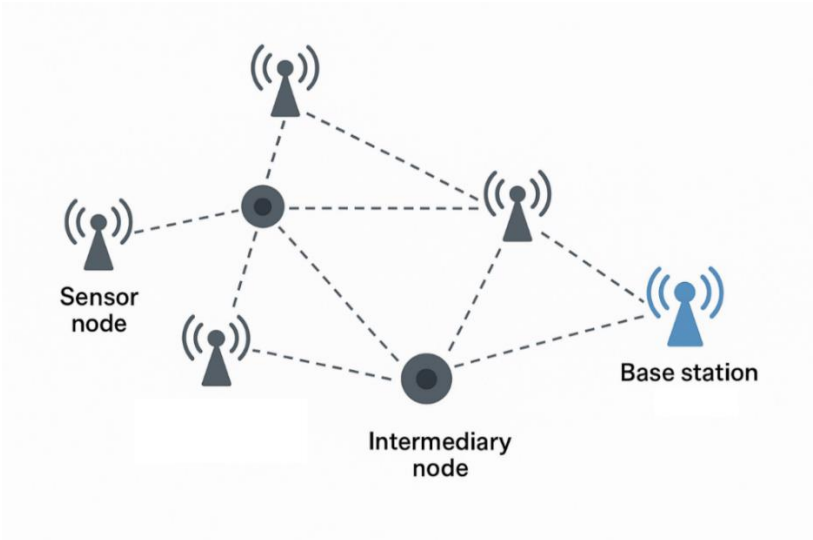


Рис. 1.3 Приклад конфігурації БСМ з проміжними вузлами

Проміжні вузли можуть реалізовуватись у вигляді маршрутизаторів або шлюзів. Їх основне завдання полягає у зборі даних від сенсорних вузлів та подальшій передачі цих даних до базової станції. Між ними може створюватись багатохопова (multi-hop) структура, де дані передаються через кілька вузлів і саме ці проміжні вузли ретранслюють пакети далі мережею. Крім того, такі вузли відповідають за налаштування основних параметрів мережі, підключення нових вузлів і можуть здійснювати моніторинг загального стану мережі. Зазвичай транзитний вузол містить модуль із прийомопередавачем для отримання інформації від сенсорів і пристрій для комунікації з базовою станцією.

За своєю структурою проміжний вузол дуже схожий на звичайний сенсорний вузол, оскільки він також є невеликим обчислювальним пристроєм, що забезпечує безпровідну комунікацію. Відрізняється лише номіналами, потужністю та фізичним розміром окремих елементів електронної плати, оскільки, знову ж, функціональне призначення транзитного вузла не у зборі даних із сенсорів, а у ретрансляції, маршрутизації та, за потреби, агрегації інформації, що надходить від інших вузлів мережі.

1.2.3 Центри керування.

Центром керування в контексті БСМ прийнято вважати базову станцію - елемент безпровідної сенсорної мережі, який приймає дані від усіх сенсорних і транзитних вузлів та передає їх у зовнішній світ – сервер, хмарну платформу чи локальну систему моніторингу. Саме через неї відбувається взаємодія з користувачами або вищими рівнями системи.

Роль центру керування полягає в зборі даних, передачі даних у зовнішню мережу, управлінні локальною мережею, централізованій обробці інформації, її фільтрацію, структуризацію чи аналітику.

Залежно від протоколу, обраного спеціалістами на етапі проектування БСМ, будова базових станцій може різнитись, але загальна структура така:

- потужний обчислювальний модуль;

- радіомодуль підвищеної потужності;
- мережеві модулі (Ethernet, Wi-Fi, GSM-GPRS модем);
- пам’ять;
- джерело живлення.

Тобто для керування БСМ достатньо пристрою функціонально подібного до сучасного невиликого персонального комп’ютера, за винятком того, що його призначення не у відмальовуванні комп'ютерної графіки, а в «перегонці», зборі та обробці великих масивів даних. Навідміну від сенсорних вузлів базові станції розміщуються у місцях де люди мають легший доступ для їх обслуговування, наприклад у складських приміщеннях, теплицях, підстанціях, на дахах будівель, в спеціальних захищених шафах на стовпах.

1.3 Концепція безпеки.

Головним завданням інформаційної безпеки в БСМ є гарантування конфіденційності, цілісності, доступності, автентичності та актуальності даних, з якими працює система.

Під конфіденційністю слід розуміти захист інформації від потрапляння до зловмисників, тобто дані БСМ мають бути недоступними для неавторизованих осіб. Цілісність означає запобігання зміні або фальсифікації повідомлень сторонніми. Автентифікація забезпечує, що обмін даними в мережі відбувається виключно між справжніми, зареєстрованими вузлами. Доступність означає можливість своєчасного, коректного та повного отримання інформації користувачами, які є частиною системи і мають відповідні права. Актуальність же передбачає, що на приймальному боці надходитимуть лише свіжі та оновлені дані, а отже зловмисник не зможе підмінити їх застарілою інформацією. Це особливо важливо в сенсорних мережах зі спільними ключами, адже при недостатньому контролі актуальності зловмисник може отримати старий ключ і використати його, щоб видавати себе за легітимний вузол.

1.3.1 Модель загроз та вразливостей.

Безпровідні сенсорні мережі мають принципово інший профіль ризиків порівняно з традиційними мережами через свою розподілену архітектуру, ресурсно обмежені вузли та відкритий безпровідний канал зв’язку. Модель загроз охоплює класифікацію порушників, їх можливості, векторів атак, а також типові вразливості системи. Приблизну модель загроз можна розкласти наступним чином:

Об’єкти захисту:

- сенсорні вузли;
- комунікаційні канали;
- центр керування;
- дані датчиків;
- конфігурації та ключі доступу.

Зловмисник:

- може бути внутрішнім, зовнішнім, пасивним, активним:
- має можливість фізичного доступу.

Типові атаки:

- атаки на мережевий трафік;
- атаки на маршрутизацію;
- атаки на дані;
- атаки з доступом до фізичного обладнання;

Потенційні наслідки:

- втрата даних;
- фальшиві вимірювання;
- порушення маршрутизації;
- відмова працездатності системи.

1.3.2 Типові вразливості.

Існує вразливість бездротових сенсорних мереж – це наслідок фундаментального конфлікту між відкритістю середовища передачі та жорсткими апаратними обмеженнями самих пристроїв. Найкращим рішенням для розгляду типових вразливостей буде їх поділ згідно з рівнями моделі OSI.

Доцільно почати з фізичного рівня. Тут головною проблемою є доступність. Сенсори часто розміщують у необладнаних локаціях без нагляду, а їхні корпуси рідко мають захист від злому. На практиці це означає, що зловмисник може отримати фізичний доступ до плати, підключитися до інтерфейсів налагодження та зчитати вміст пам'яті. Захиститися від цього складно: слабкі процесори просто не "тягнуть" складні криптографічні алгоритми. Радіоефір теж не додає надійності. Канал за своєю природою є відкритим, що робить перехоплення трафіку або глушіння сигналу тривіальною задачею.

На мережевому рівні ситуація ускладнюється специфікою маршрутизації. Стандартні протоколи БСМ оптимізовані під енергоефективність, а не під безпеку, і зазвичай працюють на довірі до сусідніх вузлів. Цим активно користуються нападники. Вони можуть реалізувати атаку "black hole" (вибіркове або повне відкидання пакетів) або "sinkhole", змушуючи сусідні вузли пересилати трафік через скомпрометований пристрій. Ще витонченішою є атака "wormhole": створення прихованого тунелю між двома точками мережі для викривлення маршрутів.

Проблеми транспортного рівня часто б’ють по найслабшому місцю сенсорів – енергоспоживанню. Зловмисник може ініціювати шквал запитів на з'єднання (flooding), змушуючи вузли витрачати дорогоцінний заряд батареї на обробку та ретрансляцію сміттєвого трафіку. При цьому класичні рішення на кшталт TLS/SSL тут непридатні через свою "важкість", тому дані часто передаються без надійного шифрування.

На рівні застосунків виникає питання довіри до інформації. Якщо система не перевіряє джерело походження даних, можлива ін'єкція хибних вимірювань, що

призведе до прийняття невірних рішень центром керування. Додатковим вектором атаки стають механізми оновлення прошивки "на льоту", тобто без фізичного підключення до пристрою, які, за відсутності належної автентифікації, дозволяють зловмисникам повністю перехопити контроль над вузлами.

1.4 Класифікація та механізми атак.

БСМ належать до категорії децентралізованих розподілених систем, що функціонують у відкритому радіоефірі та часто розгортаються у неконтрольованих або частково контрольованих середовищах. Така специфіка визначає підвищену вразливість цих мереж до широкого спектра кібератак, спрямованих на порушення конфіденційності, цілісності, доступності та автентичності інформаційних потоків.

На фізичному рівні поширеними є атаки глушіння, що полягають у навмисному створенні завад у радіоканалі з метою блокування обміну даними між вузлами. Сюди також належать атаки фізичної компрометації, коли зловмисник отримує доступ до апаратної частини вузла для вилучення криптографічних ключів або зміни прошивки.

На мережевому рівні зосереджено найбільшу кількість атак, оскільки маршрутизація є критичним компонентом функціонування БСМ. До таких атак належать selective forwarding, sinkhole, sybil, hello flood, wormhole та підміна або маніпуляція маршрутних оголошень. Їхньою спільною метою є перехоплення, спотворення або блокування транзитного трафіку, а також порушення коректності побудови маршрутів.

На транспортному рівні загрозою є атаки типу, спрямовані на створення надмірної кількості запитів, а також атаки desynchronization, коли зловмисник надсилає фальшиві підтвердження або службові повідомлення, спричиняючи порушення синхронізації сеансів між вузлами.

На прикладному рівні виникають атаки, що стосуються змісту переданих даних або логіки їх обробки. Це можуть бути replay-атаки, інжекція фальшивих даних сенсорних вимірювань, а також атаки на механізми оновлення прошивки, що

дозволяють зловмиснику встановити шкідливе програмне забезпечення на компрометовані вузли.

Механізми реалізації кібератак залежать від обраного рівня впливу та наявних можливостей атакувальника. На фізичному рівні атаки реалізуються шляхом генерування високопотужних радіосигналів або отримання доступу до апаратної конфігурації вузла. На канальному рівні зловмисник підбирає моменти передачі кадрів, створюючи колізії або ініціюючи повторні спроби надсилання. Для атак мережевого рівня характерне використання фальшивих маршрутних повідомлень, модифікація метрик або створення «тунелів» між різними частинами мережі. На транспортному рівні здійснюється підміна службових повідомлень або штучне збільшення кількості запитів. На прикладному рівні переважно реалізуються атаки, пов’язані з підробкою даних або впливом на механізми оновлення програмного забезпечення.

1.5 Пасивні та активні атаки.

Усі кібератаки традиційно поділяють на пасивні та активні, що дозволяє чітко визначити їхній вплив на інформаційні потоки та функціонування мережі. Такий поділ ґрунтується на характері взаємодії зловмисника з мережею: пасивні атаки не змінюють передавані дані, тоді як активні передбачають пряме втручання у процеси обміну інформацією, маршрутизації або роботи вузлів.

Пасивні атаки спрямовані на перехоплення, спостереження або аналіз інформації, яка передається в мережі, без будь-якої зміни її вмісту або структури. Зловмисник у цьому випадку не втручається у процес комунікації, що робить такі атаки складними для виявлення. Їхня головна мета – здобуття конфіденційної інформації, відомостей про топологію мережі, закономірності руху трафіку або ключової інформації.

Активні атаки пов’язані з активним втручанням у роботу БСМ, що проявляється через модифікацію передаваних даних, порушення процедури маршрутизації, створення перешкод у радіоканалі, блокування ресурсів або

імітацію роботи легітимних вузлів. Такі атаки можуть мати як локальний, так і системний характер, порушуючи цілісність, доступність та автентичність інформації.

Порівняння типових ознак пасивних та активних атак наведено в таблиці 1.1.

Таблиця 1.1

Порівняльна характеристика пасивних та активних атак

Ознака	**Пасивні атаки**	**Активні атаки**
Втручання в передачу даних	Відсутнє	Присутнє
Можливість виявлення	Дуже низька	Порівняно висока
Основна мета	Отримання інформації	Порушення роботи мережі
Рівень загрози	Інформаційний	Деструктивний
Приклади	Eavesdropping, Traffic Analysis	Jamming, Sinkhole, Data injection

1.6 Існуючі криптографічні механізми захисту.

Криптографічний захист у безпровідних сенсорних мережах спрямований на забезпечення конфіденційності, цілісності, автентичності та доступності інформації, що передається між сенсорними вузлами. В таких мережах застосовують спеціально адаптовані або полегшені варіанти класичних криптографічних алгоритмів.

Одним із базових напрямів є застосування симетричних криптографічних алгоритмів, які завдяки своїй продуктивності та низьким витратам ресурсів залишаються найбільш поширеними в сенсорних мережах. Сучасні дослідження зосереджуються на адаптації легковагових блокових шифрів та потокових алгоритмів, що дозволяють забезпечити конфіденційність переданих даних без значного впливу на тривалість роботи вузла. Водночас актуальною залишається

проблема безпечного та масштабованого розподілу ключів, адже саме цей аспект визначає стійкість мережі до компрометації окремих сенсорів.

Паралельно з удосконаленням симетричних механізмів активно досліджуються можливості використання асиметричної криптографії з урахуванням модернізації апаратного забезпечення вузлів. Попри значні обчислювальні витрати, сучасні оптимізовані схеми на основі еліптичних кривих демонструють потенціал для застосування в БСМ, зокрема у процесах автентифікації, обміну ключами та формування довірчих відносин між вузлами. Такі рішення дозволяють підвищити рівень захищеності мережі, але потребують ретельного врахування енергоспоживання та часу виконання.

Окремий напрям розвитку стосується побудови комплексних криптографічних протоколів, що інтегрують механізми шифрування, автентифікації та цілісності в єдину систему захисту. Сучасні підходи все частіше орієнтуються на адаптивність і можливість враховувати контекстні параметри, такі як стан батареї, щільність мережі або поточний рівень загроз. Завдяки цьому формується більш гнучка модель безпеки, здатна реагувати на зміну умов експлуатації та загрозового середовища.

1.6.1 Симетричні алгоритми шифрування.

Симетричні алгоритми вважаються найбільш придатними для БСМ завдяки низькій обчислювальній складності та мінімальним енергетичним затратам. Вони базуються на принципі використання одного спільного секретного ключа для обох процесів - шифрування та розшифрування, що різко зменшує обчислювальні витрати порівняно з асиметричними методами.

Принцип роботи симетричної криптографії полягає у перетворенні відкритого тексту в зашифрований за допомогою одного й того самого ключа. Сама структура алгоритмів може будуватися на блокових або потокових шифрах: блокові алгоритми обробляють дані фіксованими блоками, тоді як потокові формують ключовий потік, який поєднується з даними на рівні окремих бітів або

байтів.

Прикладами реалізації симетричних алгоритмів є легковагові блокові шифри, зокрема SPECK, SIMON, PRESENT, TEA та їх модифікації. Вони розроблені спеціально як енергоефективні рішення, що потребують мінімального числа логічних операцій та мають компактну апаратну реалізацію. Такі алгоритми демонструють високу продуктивність на мікроконтролерах із мінімальною кількістю пам’яті та обмеженою тактовою частотою. Потокові шифри, такі як Grain або Trivium, також активно застосовуються, оскільки забезпечують швидку генерацію ключового потоку при малих апаратних витратах.

1.6.1 Асиметричні алгоритми шифрування.

Асиметрична криптографія базується на використанні двох ключів – відкритого та закритого, де відкритий ключ може бути поширений у мережі без ризику, тоді як закритий ключ зберігається лише на одному вузлі. Принципова особливість цього підходу полягає в тому, що дані, зашифровані відкритим ключем, можуть бути розшифровані лише відповідним приватним ключем, що забезпечує сильний рівень захисту без необхідності обміну секретами між усіма учасниками мережі.

Принцип роботи асиметричних алгоритмів пов’язаний із використанням складних математичних задач, таких як факторизація великих чисел або обчислення дискретного логарифма. Саме ці задачі формують основу сучасних криптографічних протоколів RSA, Diffie–Hellman або схем на еліптичних кривих. Однак у контексті сенсорних мереж найбільшого поширення набули алгоритми, що ґрунтуються на еліптичних кривих (ECC), оскільки вони забезпечують порівнянний рівень криптографічної стійкості при значно менших ключах та менших обчислювальних витратах, ніж класичні RSA або DH. Наприклад, ключ ECC розміром 160-256 біт забезпечує рівень захисту, еквівалентний RSA-ключу розміром понад 1024-2048 біт, при цьому потребуючи набагато менше пам’яті та енергії для виконання операцій.

У сенсорних мережах асиметрична криптографія використовується передусім у процедурах безпечної ініціалізації, аутентифікації вузлів та встановлення сесійних секретів, після чого основне навантаження переходить на симетричні алгоритми. Такий підхід дозволяє уникнути постійного виконання дорогих обчислень та зберегти енергетичний ресурс. Асиметричні схеми можуть застосовуватися для перевірки цілісності та немодифікованості даних, а також для підпису повідомлень, особливо у вузлах вищого рівня, таких як базові станції або шлюзи, що мають більші обчислювальні ресурси.

1.6 Захищені протоколи маршрутизації.

Захищені маршрутизувальні протоколи передбачають використання методів автентифікації маршрутних повідомлень, що унеможливлює їх модифікацію або ін’єкцію зловмисником. В основі таких рішень часто застосовуються симетричні або асиметричні криптографічні схеми, за допомогою яких підтверджується справжність джерела кожного управляючого пакета. У деяких протоколах цей підхід поєднується з перевіркою цілісності даних, що дозволяє запобігати атакам типу spoofing, alteration або replay. Такі механізми особливо корисні при побудові деревоподібних або кластерних структур маршрутизації, оскільки вони зменшують ризик компрометації критичних вузлів, таких як кластер-хеди або маршрутизатори проміжного рівня.

Одним із найбільш цитованих протоколів є INSENS - Intrusion-Tolerant Routing in Wireless Sensor Networks. Він ґрунтується на централізованому підході, де базова станція генерує захищені маршрути та поширює їх серед вузлів, використовуючи автентифікаційні механізми для перевірки службових повідомлень. INSENS мінімізує ризик впливу компрометованих вузлів, оскільки сенсори не беруть участі у прийнятті критичних маршрутних рішень.

Захищеним варіантом реактивної маршрутизації є SRP (Secure Routing Protocol), створений як доповнення до ад-хок протоколів типу AODV. SRP використовує двосторонню автентифікацію між джерелом і ціллю, що дозволяє

запобігати атакам типу route spoofing та route fabrication. Подібним за функціональністю є SEAD (Secure Efficient Ad hoc Distance Vector) – протокол, який використовує хеш-ланцюжки для підтвердження достовірності маршрутних метрик, тим самим запобігаючи маніпуляціям з відстанями або показниками якості маршруту.

Серед протоколів, орієнтованих на попередження атак типу wormhole та blackhole, значного поширення набув ARAN (Authenticated Routing for Ad hoc Networks). Він використовує цифрові сертифікати та перевірку автентичності всіх маршрутних повідомлень, що унеможливлює підміну маршрутів зловмисником. У контексті сенсорних мереж ARAN зазвичай застосовується у змішаних або ієрархічних архітектурах, де частина вузлів має підвищені ресурси для виконання асиметричних операцій.

Варто зазначити RRS (Robust Routing Scheme) та TRANS (Trust-based Routing for Sensor Networks), у яких поєднуються криптографічні механізми та моделі довіри. Такі протоколи аналізують поведінку сусідніх вузлів та формують маршрути з урахуванням того, наскільки надійним є кожен потенційний ретранслятор. Подібні схеми демонструють високу стійкість до атак типу selective forwarding та grayhole.

Загалом ці протоколи демонструють різні концепції захисту - від централізованого контролю та криптографії до розподілених моделей довіри та поведінкового аналізу. Їх використання дозволяє формувати стійкі маршрути навіть у складних умовах, де значний ризик фізичної компрометації вузлів або активної діяльності зловмисника.

Висновки до першого розділу

У першому розділі було представлено узагальнену характеристику безпровідних сенсорних мереж як об’єкта подальшого дослідження в контексті кібербезпеки. Розкрито їхню структурну організацію, функціональні складові та принципи взаємодії між основними елементами, що забезпечує цілісне розуміння специфіки побудови та роботи таких систем. Окремо окреслено засади забезпечення безпеки, включно з поширеними загрозами, типовими вразливостями та умовами їх виникнення.

Також було узагальнено класифікацію атак на БСМ та розглянуто основні криптографічні механізми, що можуть застосовуватися для захисту інформації в умовах обмежених ресурсів. Висвітлено підходи до створення захищених протоколів маршрутизації, які відіграють важливу роль у забезпеченні стійкості мережі до впливу зловмисника.

Зміст першого розділу формує необхідне теоретичне підґрунтя для подальшого поглибленого вивчення аспектів кіберзахисту в безпровідних сенсорних мережах і визначає ключові напрями подальших досліджень у межах цієї роботи.

2 МЕТОДИ ТА АЛГОРИТМИ ВИЯВЛЕННЯ АТАК У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

2.1 Підходи до виявлення вторгнень у бездротових сенсорних мережах

Забезпечення інформаційної безпеки в БСМ вимагає побудови глибокоешелонованої оборони, оскільки покладатися лише на один бар'єр небезпечно. Традиційні засоби, такі як криптографія та автентифікація, формують «першу лінію» захисту, проте вони виявляються безсилими у випадках, коли атака походить від скомпрометованого вузла або внутрішнього порушника, що вже володіє ключами доступу. Саме цей фактор зумовлює необхідність впровадження систем виявлення вторгнень IDS (Intrusion Detection Systems), які діють як другий ешелон оборони. Їхнє ключове завдання – безперервний моніторинг мережевої активності та виявлення підозрілих патернів поведінки, що можуть свідчити про злом.

Реалізація таких систем у сенсорних мережах є нетривіальним інженерним викликом через жорсткі апаратні ліміти. На відміну від класичних дротових мереж, де аналіз трафіку покладається на потужні сервери, у БСМ алгоритми часто мусять працювати безпосередньо на сенсорах із мінімальним обсягом пам'яті та слабкими процесорами. Це створює критичну дилему: необхідно знайти баланс між точністю виявлення загроз та енергоефективністю, адже надмірно складні обчислення можуть виснажити батареї вузлів швидше, ніж сама атака.

Центральним елементом будь-якої IDS є аналітичний метод, від якого залежить здатність системи розпізнавати загрози та рівень хибних спрацювань. У сучасній науковій літературі виділяють три основні підходи до аналізу даних. Перший з них – метод виявлення зловживань, також відомий як сигнатурний аналіз. Він працює за принципом порівняння поточної активності із заздалегідь відомими шаблонами (сигнатурами) атак, що забезпечує високу точність при ідентифікації відомих загроз, але є неефективним проти нових типів втручань. Альтернативою виступає метод виявлення аномалій, який фокусується на

моделюванні «нормальної» поведінки мережі; будь-яке суттєве відхилення від базового профілю розцінюється як потенційна атака. Цей підхід дозволяє виявляти невідомі раніше загрози, хоча й часто страждає від підвищеного рівня хибних тривог. Третім напрямом є гібридні системи, які намагаються комбінувати обидві методології для нівелювання їхніх недоліків та підвищення загальної надійності детекції.

Варто також зазначити, що ефективність IDS залежить не лише від математичного апарату, а й від архітектури розміщення агентів моніторингу – централізованої, розподіленої чи ієрархічної. Утім, саме алгоритмічна здатність коректно відрізняти легітимний трафік від зловмисного залишається визначальним фактором для забезпечення стабільності та безпеки бездротових сенсорних мереж.Першою категорією є метод виявлення зловживань, більш відомий як сигнатурний підхід. Він ґрунтується на порівнянні поточної активності з попередньо визначеними шаблонами відомих атак. Друга категорія – це метод виявлення аномалій, який фокусується на створенні профілю нормальної поведінки мережі та фіксації будь-яких суттєвих відхилень від цієї норми. Третім напрямом є використання гібридних систем, які намагаються поєднати переваги обох вищезгаданих методів для підвищення загальної ефективності виявлення та нівелювання їхніх індивідуальних недоліків.

Окрім аналітичного методу, важливим аспектом класифікації підходів є архітектура розміщення агентів моніторингу. Залежно від топології мережі та доступних ресурсів, підходи до виявлення вторгнень можуть реалізовуватися централізовано, розподілено або ієрархічно. Проте саме алгоритмічна складова - те, як саме система відрізняє легітимний трафік від зловмисного залишається ключовим фактором, що визначає надійність системи безпеки.

2.1.1 Сигнатурний підхід

В основі методу виявлення зловживань, який частіше називають сигнатурним аналізом, лежить принцип пошуку за зразком. Система спирається на

базу апріорних знань – набір унікальних цифрових відбитків або правил, що описують уже відомі сценарії атак. Функціонування таких механізмів зводиться до безперервного зіставлення: поточний мережевий трафік або поведінкові патерни вузлів порівнюються із записами у цій бібліотеці загроз. Щойно алгоритм фіксує кореляцію між спостережуваною подією та збереженим шаблоном, система ідентифікує це як атаку конкретного типу і генерує сигнал тривоги.

Беззаперечною перевагою цього підходу є його надійність у роботі з відомими загрозами. Рівень помилок першого роду, ситуацій, коли легітимна дія помилково сприймається як ворожа, тут залишається вкрай низьким, оскільки реакція відбувається лише на чітко визначені умови. Крім того, сигнатурний метод не просто фіксує факт вторгнення, а дозволяє одразу класифікувати його, що значно полегшує адміністратору вибір стратегії захисту. З погляду ресурсів цей підхід також виграє: пряме порівняння з шаблонами вимагає значно менше обчислювальних потужностей, ніж складні статистичні обчислення чи нейромережі, що робить його привабливим для простих мікроконтролерів.

Проте в реаліях бездротових сенсорних мереж сигнатурний метод стикається із фундаментальним обмеженням. Він «сліпий» до всього нового. Будь-яка атака «нульового дня» або навіть незначна модифікація відомого шкідливого коду пройде крізь такий захист непоміченою, адже її сигнатура ще відсутня в базі. Ця інертність створює небезпечний часовий проміжок між появою загрози та оновленням правил детекції, залишаючи мережу вразливою.

Не менш серйозним викликом є апаратна реалізація. Пам'ять сенсорних вузлів ресурс дефіцитний, зберігати в ній розгалужену базу сигнатур, яка постійно розростається, часто просто фізично неможливо. Розробникам доводиться йти на компроміси: зберігати лише найкритичніші правила або використовувати компактні ймовірнісні структури даних, такі як фільтри Блума, що, в свою чергу, може знизити ефективність захисту. До того ж, сама процедура оновлення бази створює додаткове навантаження на канал зв'язку і пришвидшує розряд батарей, скорочуючи життєвий цикл мережі.

2.1.2 Аномалійний підхід.

В основі аномалійного підходу лежить фундаментальна гіпотеза про те, що поведінка порушника неминуче дисонує з діями легітимного користувача. Якщо сигнатурний метод шукає «відбитки» конкретних злочинів, то системи виявлення аномалій діють від супротивного: вони визначають, що є нормою. Життєвий цикл таких систем поділяється на дві фази. Спершу, під час навчання, формується еталонний профіль поведінки мережі або окремого вузла. Надалі, у фазі активного моніторингу, реальний трафік постійно співставляється з цим еталоном, і будь-яке суттєве відхилення, що перетинає визначений поріг, маркується як потенційна загроза.

Головним козирем цієї методології є її універсальність. Оскільки система не прив’язана до бази даних відомих експлойтів, вона здатна ідентифікувати абсолютно нові, раніше не бачені вектори атак, включно із загрозами «нульового дня». Для бездротових сенсорних мереж це особливо актуально. Специфіка роботи БСМ – регулярність передачі даних та циклічність завдань – дозволяє сформувати досить чіткий і стабільний профіль «нормальної» поведінки, на тлі якого аномалії стають контрастнішими.

Проте за високу чутливість доводиться платити. Надважливим недоліком аномалійного підходу є високий рівень хибних спрацювань, іншими словами помилок другого роду. Головна складність полягає в інтерпретації рідкісних, але легітимних подій. Уявімо ситуацію: сенсори раптово починають генерувати шквал даних. Для алгоритму це виглядає як DDoS-атака, але насправді це може бути реакція на реальну надзвичайну подію, наприклад, пожежу чи витік газу. Блокування такого трафіку системою безпеки може призвести до втрати критично важливої інформації саме тоді, коли вона найбільше потрібна.

Іншим бар'єром стає ресурсоємність. Математичний апарат, що стоїть за моделюванням норми, від статистичного аналізу до нейромереж та штучних імунних систем, часто виявляється занадто важким у обробці для слабких мікроконтролерів. Обчислення швидко виснажують заряд батарей. Ситуацію

ускладнює ще й динамічна природа радіосередовища: зміна топології мережі чи деградація «заліза» з часом призводять до того, що поняття норми зміщується. Це вимагає регулярного перенавчання системи, що створює додаткове, і часто критичне, навантаження на ресурси БСМ.

2.1.3 Гібридні системи виявлення атак.

Усвідомлення того, що жоден із монолітних методів не є панацеєю підштовхнуло розробників до створення гібридних архітектур. Ідея тут проста, але ефективна – об'єднати різнорідні модулі в єдиний механізм, щоб досягти синергії. Логіка такого синтезу полягає у взаємній компенсації слабких сторін. Якщо сигнатурний аналіз гарантує точність у розпізнаванні відомих загроз, а аномальний дозволяє бачити нові вектори атак, то їх поєднання дає змогу закрити критичні вразливості. Гібридна система фактично нівелює проблему атак нульового дня і водночас суттєво знижує рівень хибних тривог, що є головним недоліком чистих аномальних детекторів.

На практиці взаємодія цих компонентів у БСМ може бути організована по-різному. Найчастіше застосовують каскадну модель. Вона працює як дворівневий фільтр: наприклад, спершу легкий сигнатурний модуль відсіює весь відомий трафік, і лише те, що залишилося неідентифікованим, передається на глибокий аналіз аномалій. Можливий і зворотний порядок, де аномальний модуль діє як "грубий фільтр" для підозрілої активності. Альтернативою є паралельна архітектура, де обидва аналізатори працюють одночасно, а фінальний вердикт виносить спеціальний модуль прийняття рішень, спираючись на методи голосування або нечітку логіку.

Очевидно, за підвищену надійність доводиться платити ресурсами. Одночасна робота кількох алгоритмів створює значне навантаження на процесор і пам'ять, що для енергозалежних сенсорів може стати вироком. Тому інженери часто вдаються до хитрощів з архітектурою, використовуючи ієрархічний підхід. Ідея полягає в делегуванні: рядові сенсори виконують лише найпростіші функції

моніторингу, тоді як важка аналітика переноситься на потужні кластерні головні вузли або безпосередньо на базову станцію. Це дозволяє утримати баланс між високим рівнем безпеки та автономністю мережі.

Можна сміливо стверджувати, що саме гібридні системи наразі є найбільш зрілим рішенням для захисту сенсорних мереж. Вони пропонують комплексне покриття загроз, адаптуючись як до стандартних експлойтів, так і до нестандартної поведінки хакерів. Успіх їх впровадження залежить насамперед від того, наскільки вдало вдасться оптимізувати алгоритми взаємодії та розподілити обчислювальні завдання, мінімізуючи обчислювальні витрати складових мережі.

2.2 Методи оцінки поведінки вузлів.

Фундаментом ефективності будь-якої IDS чи системи управління довірою в БСМ є якість первинних даних. Оцінка поведінки вузла – це не статичний зріз, а динамічний процес безперервного вимірювання параметрів, що характеризують дотримання мережевого етикету. Тут криється ключова архітектурна відмінність від класичних систем: якщо у дротових мережах «всевидячим оком» виступають центральні шлюзи, то в розподілених сенсорних мережах тягар моніторингу лягає на плечі самих пристроїв. Вузли змушені виконувати роль наглядачів, взаємно відстежуючи дії сусідів у межах свого радіопокриття.

Кінцева мета цього нагляду – сформувати об'єктивний профіль надійності, чітко розмежувавши доброчесних учасників, несправні девайси та відвертих зловмисників. Це завдання ускладнюється стохастичною природою бездротового зв'язку. Втрата пакету чи затримка не завжди є ознакою атаки; це часто наслідок природної інтерференції, колізій або банального перевантаження каналу. Саме тому примітивні метрики тут не працюють. Адекватна оцінка вимагає глибокого аналізу часових рядів та врахування контексту роботи мережі, щоб мінімізувати ризик помилкового блокування легітимного вузла через тимчасові технічні збої.

Для побудови цілісної картини безпеки сучасні підходи пропонують аналізувати поведінку вузла у багатовимірному просторі, поєднуючи різні джерела

даних. Першою площиною аналізу є мережева активність, яка показує дисциплінованість вузла в прийомі та ретрансляції пакетів. Другим критичним маркером виступає енергетична поведінка: будь-які аномалії у споживанні ресурсу часто є індикатором атаки на виснаження (denial of sleep) або свідченням компрометації. Третій вектор – це моніторинг участі в маршрутизації, що дозволяє своєчасно виявити спроби маніпуляції топологією мережі чи викривлення маршрутів передачі даних.

2.2.1 Моніторинг мережевого трафіку.

Моніторинг мережевого трафіку виступає фундаментальним інструментом діагностики стану бездротової сенсорної мережі, забезпечуючи первинні дані для виявлення порушень цілісності та доступності інформаційного обміну. Цей метод полягає у систематичному спостереженні за потоками даних, що циркулюють між сенсорними вузлами, з метою виявлення відхилень у частоті, обсязі або напрямку передачі пакетів. У контексті БСМ такий аналіз дозволяє фіксувати ознаки як зовнішніх атак, спрямованих на перевантаження каналів зв’язку, так і внутрішніх загроз, пов’язаних із деструктивною поведінкою скомпрометованих маршрутизаторів.

Основним технічним прийомом реалізації моніторингу трафіку на рівні окремих вузлів є використання механізму прослуховування ефіру (promiscuous listening), часто реалізованого у вигляді архітектури «сторожового пса» (Watchdog). Суть методу полягає в тому, що вузол-відправник після передачі пакету сусідньому вузлу не переходить у сплячий режим, а продовжує прослуховувати радіоканал, щоб переконатися, що сусідній вузол здійснив подальшу ретрансляцію цього пакету. Якщо протягом визначеного інтервалу часу ретрансляція не фіксується або пакет передається у спотвореному вигляді, система інкрементує лічильник помилок для відповідного сусіда. Перевищення порогового значення таких помилок дає підстави класифікувати вузол як несправний або зловмисний, що

реалізує атаку типу «чорна діра» (blackhole) або вибіркову пересилальну атаку (selective forwarding).

Окрім контролю факту ретрансляції, важливим аспектом є статистичний аналіз інтенсивності трафіку. Раптове, лавиноподібне зростання кількості пакетів у мережі може свідчити про спробу атаки типу «флудинг» (flooding), метою якої є виснаження енергетичних ресурсів вузлів та блокування легітимного доступу до середовища передачі. Для виявлення таких аномалій застосовуються метрики середньої частоти надходження пакетів, коефіцієнта доставки (Packet Delivery Ratio - PDR) та часу затримки. Порівняння поточних значень цих параметрів із історичними даними або теоретично розрахованими нормами дозволяє виявляти джерела генерації паразитного трафіку та ізолювати їх від решти мережі.

Варто зазначити, що реалізація постійного моніторингу трафіку пов’язана з низкою технічних викликів, зумовлених специфікою бездротового середовища. Головною проблемою є енергоємність процесу прослуховування каналу, що вимагає утримання радіомодуля в активному стані довше, ніж це необхідно для звичайної передачі даних. Крім того, висока ймовірність колізій та інтерференції сигналу в бездротових мережах може призводити до ситуацій, коли чесний вузол не може передати пакет або факт його передачі не фіксується монітором через завади. Це створює ризик виникнення помилок першого роду, коли легітимні вузли помилково позначаються як зловмисні, тому алгоритми аналізу трафіку повинні включати механізми фільтрації випадкових збоїв та адаптації до поточного стану зашумленості ефіру.

2.2.2 Аналіз енергоспоживання.

Моніторинг мережевого трафіку слугує фундаментом діагностики в БСМ, надаючи первинні дані для контролю цілісності та доступності інформаційного обміну. Суть методу зводиться до систематичного відстеження потоків даних: система аналізує частоту, обсяги та вектори передачі пакетів. Такий підхід дозволяє виявляти широкий спектр загроз – від масованих зовнішніх атак, націлених на

перевантаження каналів, до прихованої деструктивної діяльності внутрішніх вузлів-зрадників.

На рівні окремих пристроїв ключовим інструментом моніторингу є техніка promiscuous listening (прослуховування ефіру), яка найчастіше реалізується в архітектурі Watchdog. Алгоритм діє наступним чином: вузол-відправник, передавши пакет сусідові, не переходить одразу в режим енергозбереження, а залишається активним, щоб перевірити, чи виконав сусід подальшу ретрансляцію. Якщо протягом визначеного тайм-ауту ефір мовчить або пакет передано зі спотвореннями, система фіксує порушення. Накопичення таких інцидентів понад встановлений поріг стає підставою для маркування вузла як несправного або зловмисного, що, ймовірно, реалізує атаку типу blackhole або вибіркову маршрутизацію (selective forwarding).

Окрім перевірки конкретних транзакцій, критично важливим є аналіз загальної статистики трафіку. Раптовий, лавиноподібний сплеск кількості пакетів зазвичай є індикатором атаки flooding, мета якої – паралізувати мережу та виснажити батареї пристроїв. Для діагностики таких аномалій використовують набір метрик: середню частоту надходження пакетів, час затримки та коефіцієнт успішної доставки PDR (Packet

Delivery Ratio). Порівнюючи поточні показники з історичним профілем або розрахунковою нормою, система здатна локалізувати джерело паразитного трафіку та ізолювати його.

Втім, впровадження безперервного моніторингу стикається з серйозними технічними бар'єрами. Головна проблема – енергоємність. Утримання радіомодуля в активному стані для прослуховування каналу призводить до швидкого розряду батарей, що скорочує життя мережі. Додатковим ускладненням є фізика бездротового зв'язку: колізії та інтерференція можуть перешкодити чесному вузлу передати пакет або ж завадити монітору зафіксувати факт успішної передачі. Це створює високий ризик помилок першого роду, коли легітимний вузол помилково визнається шкідливим. Тому алгоритми аналізу мають бути адаптивними, вміючи відрізняти зловмисні дії від випадкових збоїв у зашумленому ефірі.

2.2.3 Виявлення підозрілої маршрутизаційної активності.

Захист маршрутизації залишається чи не найскладнішим аспектом безпеки бездротових сенсорних мереж. Корінь проблеми криється у пріоритетах: популярні протоколи (RPL, AODV, LEACH) проектувалися передусім задля енергоефективності, часто залишаючи стійкість до зловмисних втручань на другому плані. У фокусі систем захисту тут опиняється службовий трафік, адже саме маніпулюючи повідомленнями про структуру мережі, зловмисники можуть перенаправляти потоки даних через підконтрольні їм вузли, замикати трафік у петлі або взагалі відрізати цілі сегменти мережі від шлюзу.

Головним маркером підозрілої активності зазвичай стає розбіжність між тим, що вузол обіцяє, і реальним станом речей. Яскравим прикладом є атака типу sinkhole, під час якої зловмисний вузол агресивно рекламує себе як власника найкращого маршруту до базової станції, декларуючи нереалістично високу якість каналу або мінімальну кількість хопів [1]. Завдання системи виявлення вторгнень – скептично оцінювати такі анонси, зіставляючи їх із даними сусідів або географічною логікою. Наприклад, якщо периферійний сенсор раптово заявляє про прямий зв'язок із центральним сервером, це майже гарантовано є аномалією.

Ще один поширений вектор загрози – це маніпуляції з ідентичністю, зокрема атака sybil. Її сутність полягає в тому, що один фізичний пристрій генерує повідомлення від імені безлічі віртуальних сутностей, намагаючись викривити результати голосування або захопити маршрути. Ефективним методом протидії тут є аналіз фізичних параметрів сигналу (RSSI – Received Signal Strength Indicator): якщо пакети від нібито «різних» користувачів надходять з однаковою потужністю та синхронізацією, це вірна ознака атаки. Також критично важливо контролювати послідовність номерів пакетів, щоб запобігти атакам повторного відтворення, які реанімують старі, вже неактуальні маршрути.

Найвищу ефективність у виявленні таких загроз демонструє крос-шаровий підхід, коли підозри на мережевому рівні перевіряються даними фізичного рівня. Проте головна інженерна складність полягає в тому, щоб відрізнити атаку від

норми. БСМ – це динамічна система. Вузли вимикаються через розряд батарей, йдуть у сплячий режим або переміщуються, що викликає цілком легітимну перебудову маршрутів. Алгоритми захисту мусять бути достатньо гнучкими, щоб не сприйняти процес самовідновлення мережі за вороже втручання.

2.3 Класифікаційні та машинні алгоритми виявлення атак

Ескалація кіберзагроз та лавиноподібне зростання обсягів даних у сучасних сенсорних мережах зробили очевидним той факт, що епоха простих евристичних методів добігає кінця. Класичні механізми захисту, які тримаються на статичних порогових значеннях чи прописаних вручну правилах, виявилися занадто інертними. Вони просто не встигають адаптуватися до динамічного середовища БСМ. Відповіддю на цей виклик стало впровадження технологій машинного навчання ML (Machine Learning). Їхня ключова перевага – здатність автоматизувати побудову моделей безпеки, виявляючи приховані кореляції у великих масивах даних. Це перетворює систему захисту зі статичного бар'єра на адаптивний інструмент.

З математичної точки зору, застосування ML у кібербезпеці зводиться до переформулювання проблеми виявлення вторгнень у задачу класифікації. Алгоритм працює з «цифровим зліпком» стану системи – вектором ознак. Цей вектор формується з параметрів трафіку, таких як тривалість сесії, кількість байтів, прапорці TCP, або фізичних показників вузла, таких як рівень сигналу чи залишок заряду батареї. Мета моделі – віднести кожну спостережувану подію до певного класу. У найпростішому випадку це бінарний вибір – норма або атака. Втім, складніші сценарії передбачають мультикласову класифікацію, що дозволяє не лише зафіксувати факт нападу, а й ідентифікувати його тип – будь то DoS-атака, сканування портів чи R2L-експлойт.

Життєвий цикл такої системи традиційно ділиться на два етапи: навчання та безпосередню експлуатацію. На першому етапі алгоритм тренується на історичних даних, калібруючи свої внутрішні параметри для мінімізації похибки. На другому

– модель застосовується до реального потоку даних для прийняття миттєвих рішень. Вибір конкретного алгоритму для БСМ перетворюється на нетривіальну інженерну задачу. Розробнику доводиться шукати хиткий баланс між точністю, здатністю моделі до узагальнення на нових даних та її «важкістю». Адже обчислювальна складність алгоритму має вписуватися в жорсткі рамки обмежених ресурсів сенсорних вузлів.

2.3.1 Метод опорних векторів.

Метод опорних векторів SVM (Support Vector Machine) заслужено утримує позиції одного з найпотужніших інструментів для задач бінарної класифікації в системах кіберзахисту. Його математична філософія базується на пошуку оптимальної розділової гіперплощини у багатовимірному просторі ознак. Головна мета – не просто провести межу між «нормальним» трафіком та атакою, а зробити це максимально ефективно. Ключовою відмінністю SVM від інших лінійних класифікаторів є принцип максимізації зазору – відстані між розділовою лінією та найближчими точками даних – опорними векторами. Саме наявність цієї буферної зони робить модель стійкою до перенавчання та гарантує високу точність при роботі з новими даними.

У контексті бездротових сенсорних мереж, де дані часто мають хаотичну структуру і не піддаються простому лінійному поділу, вирішальну роль відіграє kernel trick (ядровий трюк). Використовуючи спеціальні функції, наприклад радіальні базисні RBF (Radial basis function), алгоритм віртуально проектує вхідні вектори у простір вищої розмірності. Там, де у вихідному просторі класи були перемішані, у новому вимірі вони стають лінійно роздільними. Це дозволяє ефективно виявляти складні нелінійні патерни атак, не перевантажуючи процесор прямим перерахунком координат.

Додатковим вагомим аргументом на користь SVM є його ефективність в умовах дефіциту даних. Якщо глибокі нейронні мережі потребують колосальних навчальних вибірок для налаштування мільйонів ваг, то SVM здатен формувати

надійні границі рішень на основі значно меншої кількості прикладів. До того ж, процес навчання SVM зводиться до задачі опуклої квадратичної оптимізації, що математично гарантує знаходження глобального оптимуму. Це виключає ризик застрягання в локальних мінімумах, що є типовою проблемою для багатьох інших алгоритмів машинного навчання.

Втім, імплементація цього методу на слабких вузлах БСМ стикається з проблемою ресурсоємності: складність навчання зростає квадратично залежно від кількості зразків. Виходом із ситуації часто стає гібридна архітектура: важкий етап навчання переноситься на потужну базову станцію або у хмару, а сенсори отримують лише готові параметри гіперплощини для миттєвої класифікації в реальному часі. Також перспективним є використання полегшеної версії – однокласового SVM (One-Class SVM). Він фокусується виключно на описі «нормальної» поведінки, що дозволяє суттєво спростити модель та зменшити вимоги до пам'яті пристроїв.

2.3.2 Дерева рішень і випадкові ліси.

Серед методів машинного навчання, що застосовуються для класифікації мережевих атак, окрему нішу займають дерева рішень (Decision Trees). Їхня популярність зумовлена унікальним поєднанням простоти та інтерпретованості. На відміну від «чорних скриньок», якими часто є нейронні мережі, дерево рішень пропонує прозору логіку прийняття рішень. Структурно модель нагадує перевернуту ієрархію: процес починається з кореневого вузла і через серію розгалужень, що базуються на перевірці певних атрибутів трафіку, наприклад, «чи перевищує розмір пакету X байт?», спускається до «листків», які містять фінальний вердикт – клас атаки або нормальна поведінка. Така архітектура дозволяє автоматично генерувати чіткі правила типу «ЯКЩО-ТО» (IF-THEN), які легко аналізувати та інтегрувати в системи безпеки.

Однак, попри інтуїтивну зрозумілість, поодинокі дерева рішень мають суттєвий недолік – схильність до перенавчання (overfitting). Якщо не обмежувати

глибину дерева, алгоритм намагатиметься побудувати ідеально точні правила для навчальної вибірки, запам'ятовуючи навіть випадковий шум та аномалії, які не є загальними закономірностями. У результаті така модель показує блискучі результати на тренувальних даних, але безпорадна при зустрічі з реальним, раніше не баченим трафіком.

Логічним еволюційним кроком для вирішення цієї проблеми стала поява ансамблевих методів, найвідомішим з яких є алгоритм випадкового лісу (Random Forest). Ідея методу проста, але геніальна: замість того, щоб покладатися на одне «експертне» дерево, система будує цілий комітет із сотень незалежних дерев. Ключовим моментом тут є стохастичність, себто випадковість. Кожне дерево навчається на випадковій підмножині даних і, що важливо, при кожному розгалуженні розглядає лише випадковий набір ознак. Це змушує окремі моделі фокусуватися на різних аспектах даних, ролячи їх різноманітними.

Фінальне рішення у випадковому лісі приймається шляхом голосування більшістю: об'єкт відноситься до того класу, за який «проголосувала» найбільша кількість дерев. Такий підхід дозволяє кардинально знизити дисперсію помилки та нівелювати проблему перенавчання. У контексті бездротових сенсорних мереж Random Forest демонструє високу стійкість до шуму та здатність ефективно працювати з багатовимірними даними, де ознаки атак можуть бути неочевидними. Хоча цей метод є більш ресурсомістким, ніж прості дерева, його висока точність та низький рівень хибних спрацювань роблять його ідеальним кандидатом для розгортання на рівні базових станцій або потужних шлюзів, де він виступає надійним бар'єром проти складних кіберзагроз.

2.3.3 Нейронні мережі та глибинне навчання

Вершиною еволюції інтелектуальних систем захисту сьогодні безперечно є штучні нейронні мережі (ШНМ) та методи глибинного навчання (Deep Learning). Це не просто покращення попередніх методів, а зміна підходу: якщо класичне машинне навчання вимагає від інженера ручного, кропіткого конструювання ознак,

то глибокі мережі вчаться самі. Вони здатні автоматично виокремлювати приховані ієрархічні патерни безпосередньо з «сирого» потоку даних. Математичним фундаментом тут є здатність нейронів, організованих у шари, апроксимувати надскладні нелінійні функції. Це дозволяє моделювати «нормальний» профіль трафіку з хірургічною точністю, навіть коли мережа працює в умовах сильного зашумлення та динамічних змін топології.

У розрізі кібербезпеки особливу цінність демонструють архітектури, що володіють «пам'яттю» – рекурентні мережі RNN (Recurrent Neural Networks) та їх удосконалена варіація – мережі довгої короткострокової пам'яті LSTM (Long Short-term Memory). Логіка їх використання продиктована самою природою трафіку: це не набір розрізнених знімків, а часовий ряд, де кожна подія є наслідком попередньої. Завдяки здатності аналізувати контекст і часові кореляції, LSTM ефективно виявляють розтягнуті у часі, «повільні» атаки, які непомітні для звичайних детекторів. Свою нішу знайшли і згорткові мережі (CNN): спочатку створені для обробки зображень, вони чудово справляються з пошуком аномалій у просторових матрицях трафіку.

Проте інтеграція цієї потужності в обмежену екосистему БСМ наштовхується на жорсткий бар'єр – ресурсоємність. Навчання глибокої мережі, наприклад оновлення мільйонів ваг через зворотне поширення помилки, вимагає потужних GPU, яких у сенсорних мережах просто немає. Більше того, навіть етап використання готової моделі може стати непосильною ношею для скромного мікроконтролера, призводючи до критичних затримок передачі даних та миттєвого розряду батареї.

Вихід із цього глухого кута шукають у гібридних архітектурах та оптимізації. Стандартна практика сьогодні – це навчання важких моделей у хмарі з подальшою їх «дієтою»: використанням дистиляції знань або квантування (зниження розрядності чисел) для створення компактних версій, придатних для запуску на периферії. Але залишається ще одна фундаментальна проблема – ефект «чорної скриньки» (Black Box). Через складність внутрішніх зв’язків нейромережа часто не може «пояснити», чому вона вважає певний пакет атакою. Це ускладнює

верифікацію системи та розслідування інцидентів, стимулюючи інтерес до нового напрямку – пояснюваного штучного інтелекту XAI (Explainable Artificial Inteligance).

2.3.4 Байєсівські методи класифікації.

В основі байєсівських методів класифікації лежить імовірнісна філософія, що базується на класичній теоремі Байєса. Замість того, щоб намагатися провести жорстку демаркаційну лінію між класами, ці алгоритми оперують категорією шансу. У контексті кіберзахисту БСМ це означає перехід від детермінованого так/ні до оцінки апостеріорної ймовірності: наскільки цей конкретний набір ознак схожий на атаку? Система діє подібно до аналітика: вона акумулює статистичний досвід і, отримуючи новий пакет даних, висуває гіпотезу про його природу, зважуючи поточні спостереження проти накопиченої історії поведінки мережі.

В умовах жорсткої ресурсної дієти, характерної для сенсорних мереж, безумовним лідером став Наївний байєсівський класифікатор (Naive Bayes). Епітет «наївний» тут не випадковий: він вказує на фундаментальне спрощення – припущення про повну незалежність ознак. Алгоритм «вірить», що, наприклад, висока частота пакетів ніяк математично не пов'язана з їхнім розміром. Хоча в реальному житті цей зв'язок часто існує, така математична сліпота дає колосальний виграш. Складні матричні операції замінюються серією елементарних множень ймовірностей, перетворюючи цей метод на еталон енергоефективності, здатний працювати прямо на кристалі найпростішого мікроконтролера.

Сильною стороною цієї групи методів є їхня стійкість до неідеальних умов. Вони демонструють стабільні результати навіть на зашумлених або неповних даних, що для нестабільного радіоефіру є нормою. Ще один критичний плюс – здатність до інкрементного навчання. Модель можна оновлювати «на льоту» по мірі надходження нових даних, не зупиняючи систему для повного перенавчання з нуля. Це робить захист гнучким до зміни тактики хакерів. До того ж, на відміну від ненаситних до інформації нейромереж, байєсівські алгоритми здатні будувати

адекватні прогнози навіть на скромних навчальних вибірках, що спрощує старт системи.

Втім, за простоту доводиться платити. Ігнорування взаємозв'язків між ознаками стає недоліком наївного підходу при зустрічі зі складними, скоординованими атаками, де кореляція параметрів є головним індикатором загрози. Щоб нівелювати цей недолік, застосовують Байєсівські мережі довіри (Bayesian Belief Networks). Ці моделі структурують залежності у вигляді орієнтованого ациклічного графа, що дозволяє системі розуміти причинно-наслідкові ланцюжки подій. Хоча такий підхід забезпечує значно вищу точність, він вимагає несумірно більших обчислювальних потужностей, тому в архітектурі БСМ його застосування зазвичай обмежується рівнем базової станції або потужних шлюзів.

2.4 Методи виявлення специфічних атак.

Хоча загальні алгоритми машинного навчання створюють надійний фундамент для пошуку аномалій, побудова справді ефективного ешелону оборони в БСМ вимагає більш точкового підходу – впровадження спеціалізованих механізмів, адаптованих до конкретних векторів атак. Природа сенсорних мереж, з їхнім відкритим ефіром та кооперативною моделлю поведінки, створює унікальний ландшафт вразливостей по всьому стеку OSI: від грубого фізичного глушіння до витончених маніпуляцій маршрутизацією. Глибоке розуміння «анатомії» конкретних загроз дає розробникам значну перевагу. Воно дозволяє замінити громіздкі універсальні класифікатори на легкі, прицільні евристики, які спрацьовують швидше і точніше, що є критичним фактором в умовах жорсткого дефіциту обчислювальних ресурсів.

Стратегія виявлення специфічних вторгнень базується на ідентифікації унікальних поведінкових сигнатур – невід'ємних атрибутів тієї чи іншої атаки. Наприклад, втручання в систему маршрутизації неминуче проявляється через аномальні стрибки в топології мережі або спотворення метрик шляху, тоді як атаки

на рівні MAC десинхронізує механізми доступу до середовища та розклад передач. Для успішної протидії таким загрозам найефективнішим інструментом стає крос-шаровий підхід (cross-layer detection). Зіставляючи дані з різних рівнів мережевого стеку, система отримує здатність «бачити контекст», що дозволяє впевнено відрізняти технічні збої, спричинені поганим зв'язком, від цілеспрямованих зловмисних дій.

2.4.1 Виявлення атак типу “blackhole”, “sinkhole”, “wormhole”.

Атаки на систему маршрутизації справедливо вважаються слабким місцем бездротових сенсорних мереж. Експлуатуючи базову довірчу модель, необхідну для мультихопової передачі даних, вони здатні паралізувати роботу навіть захищених криптографією систем. У цій площині найбільш руйнівний потенціал мають три вектори: атаки типу «blackhole» (чорна діра), «sinkhole» (воронка) та «wormhole» (червоточина). Спільним знаменником для них є маніпуляція топологією мережі з метою перехоплення або блокування трафіку, проте механіки реалізації та методи протидії суттєво різняться.

Атака «blackhole» діє за принципом пастки. Зловмисний вузол агресивно рекламує себе як власника найкоротшого або найстабільнішого маршруту до базової станції. Щойно сусідні вузли, спокушені фальшивими метриками, перемикають свої потоки даних на нього, він просто відкидає пакети, не виконуючи ретрансляції. Для протидії цій загрозі класичним рішенням став механізм «сторожового пса» (Watchdog), детально описаний у фундаментальних роботах з безпеки сенсорних мереж [2]. Сутність методу полягає у взаємному нагляді: вузли, працюючи в режимі прослуховування ефіру (promiscuous mode), контролюють, чи переслав їхній сусід пакет далі по ланцюжку. Якщо відсоток втрат перевищує статистично допустимий поріг (з урахуванням природних колізій), активується система репутації, яка ізолює порушника.

Значно підступнішою є атака «sinkhole», яка часто виступає плацдармом для інших втручань. Тут мета хакера – не просто знищити дані, а «притягнути» до

підконтрольного вузла максимальну кількість мережевого трафіку. Це досягається шляхом фальсифікації метрик якості каналу (LQI) або штучного зменшення кількості хопів до шлюзу. Детекція таких «воронок» вимагає аналізу топологічної узгодженості. Система безпеки повинна порівнювати маршрутні анонси від різних джерел: ситуація, коли один вузол пропонує маршрут, який на порядок ефективніший за маршрути його фізичних сусідів, є чітким індикатором аномалії.

Унікальним інженерним викликом є атака «wormhole», оскільки для її реалізації зловмиснику навіть не потрібно знати криптографічні ключі мережі. Сценарій передбачає наявність двох зловмисників, з’єднаних прихованим швидкісним каналом (тунелем). Пакети, захоплені в одній точці мережі, миттєво передаються в іншу і відтворюються там, створюючи ілюзію прямого сусідства між віддаленими вузлами. Ефективно виявити таке викривлення простору дозволяють лише методи, що базуються на фізиці процесу: вимірювання часу та відстані. Аналіз часу проходження сигналу (RTT) допомагає виявити підозріло швидку передачу, неможливу при стандартній маршрутизації. Також застосовується механізм «пакетних повідків» (packet leashes) – додавання до пакету часових міток або GPS-координат, що дозволяє приймачу відхилити з'єднання, яке подолало нереалістичну відстань за короткий час.

2.4.2 Виявлення атак на рівні MAC.

Рівень управління доступом до середовища MAC (Media Access Control) відіграє роль арбітра в архітектурі бездротових сенсорних мереж, регламентуючи правила використання спільного радіочастотного ресурсу. Саме вразливості популярних протоколів цього шару (S-MAC, B-MAC, IEEE 802.15.4) стають мішенню для атак, мета яких варіюється від саботажу цілісності даних до прихованого виснаження енергетичного бюджету вузлів. Складність детекції таких вторгнень полягає в тому, що аналіз доводиться проводити на мікросекундному рівні, оцінюючи часові таймінги та фізичні параметри сигналу, що вимагає від алгоритмів захисту неабиякої швидкодії.

Однією з найбільш підступних загроз тут є створення прицільних колізій. На відміну від примітивного глушіння всього діапазону, зловмисник діє точково: він синхронізується з передачею жертви і генерує короткий імпульс завади рівно в той момент, щоб зруйнувати контрольну суму пакету CRC (Cyclic Redundancy Check) у приймача. Така тактика є енергоефективною для нападника і вкрай складною для виявлення, адже колізії – це рутина бездротових мереж. Щоб відрізнити атаку від норми, системи моніторингу застосовують статистичний кореляційний аналіз. Головний маркер атаки – аномалія: якщо рівень помилок передачі залишається високим навіть при низькому завантаженні каналу, або ж збої мають підозрілу періодичність, прив'язану до конкретних транзакцій, це свідчить про штучне походження перешкод.

Інший вектор атаки – це гра не за правилами в механізмах конкурентного доступу (CSMA/CA). Поки доброчесні вузли, виявивши зайнятість ефіру, чекають випадковий інтервал часу, його також називають експоненціальною відстрочкою, скомпрометований пристрій може ігнорувати цей етикет. Встановлюючи таймер очікування на нуль, зловмисник захоплює канал, позбавляючи сусідів права голосу. Виявити таку «егоїстичну» поведінку можна шляхом пасивного вимірювання інтервалів між спробами передачі. Якщо розподіл затримок конкретного вузла різко відхиляється від рівномірного закону, передбаченого стандартом, це є прямим доказом маніпуляції протоколом.

Окремою загрозою є атаки на виснаження класу «Denial of Sleep», які б'ють по найвразливішому місцю сенсорів – батареї. Бомбардуючи жертву потоком службових запитів (RTS/CTS флуд) або фальшивими пакетами синхронізації, зловмисник не дає радіомодулю перейти в енергоощадний режим сну. Ефективна протидія тут базується на моніторингу робочого циклу (duty cycle). IDS зіставляє час активності вузла з обсягом реально виконаної корисної роботи. Кричуща диспропорція, коли енергія витрачається, а корисні дані не передаються, слугує надійним індикатором атаки, спрямованої на скорочення життєвого циклу пристрою.

2.4.3 Виявлення атак відмови в обслуговуванні (DoS, DDoS).

Атаки типу відмова в обслуговуванні DoS (Denial of Service) та їх розподілені варіації DDoS (Distributed Denial of Service) становлять одну з найбільш критичних загроз для бездротових сенсорних мереж через суттєву асиметрію ресурсів між нападником і цільовою системою. У той час як зловмисник може володіти потужним обладнанням та стабільним джерелом живлення, сенсорні вузли обмежені в обчислювальній потужності, пам'яті та енергії. Метою таких атак є не стільки перехоплення інформації, скільки порушення доступності сервісів мережі шляхом перевантаження каналів зв'язку, виснаження буферів пам'яті або повного розряду батарей ключових вузлів. Складність виявлення DDoS-атак у БСМ полягає у необхідності розрізнення зловмисного флудингу та легітимного сплеску трафіку, викликаного раптовою подією в зоні моніторингу (ефект «Flash Crowd»).

Найпоширенішим механізмом реалізації DoS у сенсорних мережах є флудинг різними типами пакетів, зокрема HELLO-флудинг, RREQ-флудинг на рівні маршрутизації або SYN-флудинг на транспортному рівні. Зловмисник генерує величезну кількість беззмістовних або службових запитів, змушуючи сусідні вузли витрачати ресурси на їх обробку та ретрансляцію. Для детекції таких аномалій застосовуються методи статистичного аналізу інтенсивності вхідного трафіку. Системи виявлення вторгнень встановлюють динамічні порогові значення для кількості пакетів, що надходять від одного джерела за одиницю часу. Якщо активність певного вузла перевищує ці ліміти, він тимчасово блокується. Для підвищення точності та зниження рівня помилкових спрацювань, сучасні алгоритми використовують кумулятивні суми (CUSUM) або методи експоненційного згладжування, що дозволяють адаптуватися до природних коливань навантаження мережі.

У випадку розподілених атак DDoS, де джерелом загрози виступає скоординована група скомпрометованих вузлів, прості методи блокування за IP-адресою або ідентифікатором є неефективними. Тут доцільним є використання методів, що базуються на теорії інформації, зокрема аналізі ентропії. Під час

нормальної роботи мережі потоки даних мають певний рівень випадковості атрибутів у заголовках пакетів (наприклад, IP-адрес призначення або портів). Під час DDoS-атаки ентропія цих атрибутів різко знижується, оскільки атакуючі вузли надсилають однотипні запити на одну ціль. Моніторинг змін ентропії дозволяє виявити початок атаки на ранніх стадіях навіть за умови, що трафік від кожного окремого зловмисного вузла не перевищує порогових значень.

Окрім об’ємного флудингу, серйозну небезпеку становлять логічні DoS-атаки, які експлуатують вразливості у програмному забезпеченні або протоколах для виведення вузлів з ладу. Прикладом є атака розсинхронізації Desynchronization Attack, коли зловмисник порушує часові цикли сну та пробудження вузлів, або атака на переповнення буфера, що призводить до відкидання легітимних пакетів. Для протидії таким загрозам застосовують методи глибокої інспекції пакетів DPI (Deep Packet Inspection) у полегшеному варіанті, адаптованому для БСМ, а також моніторинг стану черг повідомлень. Якщо черга на обробку пакетів постійно заповнена на 100% при відсутності ознак зовнішнього перевантаження мережі, це сигналізує про внутрішню атаку або наявність програмної помилки, що вимагає перезавантаження або ізоляції вузла.

2.5 Моделі розподіленого виявлення загроз.

Еволюція архітектури систем виявлення вторгнень у БСМ – це не просто зміна топології, а вимушена відповідь на зростання масштабів мереж та жорсткі ліміти комунікаційного середовища. Історично домінувала централізована модель: усі «сирі» логи стікалися на базову станцію для глобального аналізу. Такий підхід, безумовно, давав ідеальну видимість, адже сервер володів повною картиною подій. Проте ціна цієї точності виявилася зависокою: передача гігантських масивів службової інформації крізь усю мережу катастрофічно виснажувала батареї ретрансляторів, а біля шлюзу неминуче утворювалося «пляшкове горлечко». До того ж, наявність єдиної точки відмови робила всю систему вразливою: вихід з ладу

сервера означав миттєве засліплення мережі. Саме ці фактори змусили наукову спільноту змістити вектор досліджень у бік розподілених систем.

Філософія розподіленого виявлення Distributed Detection докорінно змінює роль окремого пристрою. У цій парадигмі сенсор перестає бути пасивним постачальником даних і перетворюється на активного агента безпеки, здатного самостійно аналізувати трафік та оцінювати дії сусідів. Вердикт про атаку тепер формується не одноосібно «зверху», а народжується «знизу» – через діалог та агрегацію думок безлічі локальних кластерів. Така децентралізація дає подвійний виграш. По-перше, радикально знижується навантаження на канали зв'язку, адже замість сирого трафіку передаються лише компактні звіти про інциденти. По-друге, система стає надзвичайно живучою: ізоляція або втрата окремого сегмента мережі більше не призводить до колапсу всього механізму захисту.

Втім, реалізація розподіленого інтелекту вимагає вирішення нетривіальних алгоритмічних завдань. Головна проблема – локальність сприйняття: окремий вузол, обмежений радіусом дії свого радіомодуля, бачить лише фрагмент загальної картини, тому його індивідуальні висновки часто бувають хибними. Щоб перетворити набір суб'єктивних спостережень на об'єктивну істину, необхідні надійні механізми кооперації та кореляції подій у просторі. Ключовим елементом тут стають протоколи досягнення консенсусу, які дозволяють групі вузлів прийняти правильне колективне рішення навіть в умовах, коли мережа інфільтрована зрадниками, що цілеспрямовано поширюють дезінформацію.

2.5.1 Локальні механізми детекції.

Локальні механізми детекції становлять фундамент розподіленої архітектури систем виявлення вторгнень, представляючи собою автономні програмні модулі, що інсталюються безпосередньо на кожному сенсорному вузлі мережі. Основна ідея цього підходу полягає в тому, що кожен вузол несе персональну відповідальність за безпеку власного периметра та моніторинг поведінки безпосередніх сусідів, що знаходяться в радіусі дії його радіопередавача. На цьому

рівні процес виявлення відбувається ізольовано, спираючись виключно на інформацію, яку вузол може отримати самостійно: власні системні логи, дані про споживання енергії, а також перехоплені пакети, що проходять через локальний сегмент ефіру. Така децентралізація дозволяє реагувати на загрози з мінімальною затримкою, оскільки рішення приймається в точці виникнення інциденту без необхідності тривалого обміну даними з віддаленими серверами.

Технічна реалізація локальної детекції зазвичай базується на використанні легковагових агентів моніторингу, які працюють у фоновому режимі. Ключовим інструментом тут виступає згаданий раніше механізм «прослуховування» (promiscuous listening), який дозволяє вузлу аналізувати заголовки та вміст пакетів, що передаються сусідами, навіть якщо вони не адресовані цьому конкретному вузлу. Агент порівнює спостережувані параметри (частоту передач, типи пакетів, затримки) із попередньо завантаженими правилами або нормативними профілями. Враховуючи жорсткі обмеження мікроконтролерів БСМ щодо обчислювальної потужності та пам’яті, локальні алгоритми зазвичай є спрощеними: вони використовують порогові методи або базові статистичні метрики, уникаючи складних математичних перетворень, які могли б перевантажити процесор та призвести до збоїв у виконанні основного завдання сенсора.

Попри очевидні переваги у швидкості реакції та масштабованості, локальні механізми мають суттєві обмеження, головним з яких є вузький «горизонт подій». Оскільки вузол бачить лише те, що відбувається у його безпосередньому оточенні, він не здатен ідентифікувати складні розподілені атаки, такі як скоординоване сканування мережі або DDoS-атака, що зароджується у віддаленому сегменті. Більше того, локальні рішення схильні до помилок в умовах зашумленого бездротового каналу: втрата пакету через природну інтерференцію може бути помилково інтерпретована ізольованим агентом як зловмисна дія. Тому в сучасних IDS результати роботи локальних детекторів розглядаються не як остаточний вердикт, а як попередні гіпотези або «голоси», що потребують подальшої верифікації на рівні кооперативної взаємодії.

2.5.2 Кооперативні та колективні схеми.

Усвідомлення обмежень локального моніторингу призвело до розробки кооперативних та колективних схем виявлення вторгнень, які базуються на принципі синергії та інформаційного обміну між вузлами мережі. Основна ідея цього підходу полягає в тому, що об’єднання спостережень від декількох просторово розподілених сенсорів дозволяє сформувати більш точну та об’єктивну картину мережевої активності, ніж це можливо зробити ізольовано. Кооперація дозволяє подолати проблему «сліпих зон» та неоднозначності інтерпретації подій, що виникають внаслідок нестабільності радіоканалу: якщо один вузол фіксує підозрілу поведінку сусіда, а інші вузли-свідки підтверджують це спостереження, ймовірність помилкового спрацювання системи суттєво знижується.

Архітектурно кооперативні схеми в бездротових сенсорних мережах найчастіше реалізуються в рамках кластерної ієрархії. У такій структурі мережа розбивається на логічні групи – кластери, кожен з яких очолює головний вузол (Cluster Head). Рядові сенсори виконують роль первинних агентів моніторингу, збираючи локальні дані та надсилаючи звіти або попередні вердикти головному вузлу. Головний вузол, у свою чергу, виступає як центр агрегації та аналізу: він співставляє отримані звіти, фільтрує суперечливі дані та приймає остаточне рішення про наявність атаки в межах свого кластера. Така організація дозволяє збалансувати навантаження, звільняючи рядові вузли від складних обчислень, та оптимізувати використання каналу зв’язку, оскільки передаються не «сирі» дані, а компактні індикатори загроз.

Альтернативою ієрархічному підходу є повністю розподілені однорангові (peer-to-peer) схеми взаємодії, де відсутній виділений арбітр. У цьому сценарії рішення приймається колективно групою сусідніх вузлів шляхом обміну «голосами» або оцінками репутації. Кожен вузол підтримує таблицю довіри до своїх сусідів, яка динамічно оновлюється на основі їхньої поведінки та рекомендацій від інших учасників мережі. Якщо репутація певного вузла падає нижче критичного рівня згідно з консенсусом сусідів, він автоматично ізолюється:

його пакети ігнорується, а маршрути перебудовуються в обхід скомпрометованої зони. Цей підхід забезпечує високу живучість мережі, оскільки відсутня єдина точка відмови, проте він генерує значний обсяг службового трафіку, що може негативно вплинути на енергоефективність.

Впровадження кооперативних схем також породжує нові вектори загроз, пов’язані з можливістю компрометації самих учасників процесу голосування. Зловмисник, захопивши декілька вузлів, може реалізувати атаку «поганого відгуку» (bad mouthing attack), надсилаючи неправдиві звіти з метою звинувачення легітимного вузла або, навпаки, виправдання зловмисних дій («good mouthing»). Для протидії таким маніпуляціям кооперативні системи повинні включати надійні алгоритми управління довірою та методи фільтрації аномальних голосів, що базуються на статистичному аналізі відхилень від середньої думки колективу. Таким чином, ефективність колективної безпеки прямо залежить від здатності алгоритму розрізняти чесну помилку спостереження та навмисну дезінформацію.

2.5.3 Узгодження рішень у сенсорних мережах.

Процес узгодження рішень є кульмінацією роботи розподілених систем виявлення вторгнень. Саме на цьому етапі розрізнена мозаїка суб'єктивних локальних спостережень трансформується в єдиний об'єктивний вердикт про стан безпеки мережі. Потреба у складних механізмах арбітражу продиктована самою природою БСМ: сенсори, дивлячись на одну й ту ж подію з різних точок простору та через призму нестабільного радіоканалу, часто генерують суперечливі звіти. Ситуацію критично ускладнює наявність скомпрометованих вузлів-зрадників, які цілеспрямовано вкидають дезінформацію. Це створює класичну проблему «візантійських генералів» [3], де досягнення консенсусу вимагає алгоритмів, математично стійких до брехні частини учасників.

Найпоширенішим інструментом вирішення цієї дилеми залишаються схеми голосування. У найпростішому і найшвидшому варіанті діє правило простої більшості: вузол визнається зловмисним, якщо понад 50% сусідів звинуватили його

у некоректній поведінці. Проте цей метод безсилий, якщо зловмисники контролюють чисельну перевагу в локальному кластері. Тому еволюція пішла шляхом зваженого голосування. Тут система переходить від демократії до своєрідної меритократії: голос кожного вузла має різну «вагу», що залежить від його репутації, запасу енергії та історії правдивих прогнозів. Це дозволяє фільтрувати шум від підозрілих новачків, надаючи пріоритет перевіреним ветеранам мережі.

Коли ж ситуація є надто невизначеною для бінарної логіки атака/норма, у гру вступає більш потужний математичний апарат – теорія доказів Демпстера-Шейфера або нечітка логіка. Перша дозволяє коректно комбінувати конфліктуючі докази, розраховуючи міру правдоподібності загрози, а не просто її факт. Нечітка логіка, у свою чергу, наближає машину до людського мислення, оперуючи лінгвістичними змінними, наприклад висока підозра чи низька ймовірність. Це додає системі гнучкості при обробці граничних випадків, які є нормою для динамічного середовища.

Головним інженерним викликом тут залишається баланс між надійністю консенсусу та його ціною. Класичні алгоритми візантійської відмовостійкості вимагають шквального обміну повідомленнями всі з усіма, що для сенсорних мереж є неприпустимою розкішшю через швидке виснаження батарей. Тому сучасний тренд – це легковагові протоколи, які звужують коло учасників голосування лише до найбільш компетентних вузлів, досягаючи прийнятного рівня безпеки за мінімальних енергетичних витрат.

Висновки до другого розділу

У другому розділі здійснено комплексний розгляд сучасних методів та алгоритмів виявлення вторгнень, що застосовуються для забезпечення інформаційної безпеки бездротових сенсорних мереж. Проведене дослідження підтвердило, що специфіка функціонування сенсорних мереж, яка полягає у суттєвих обмеженнях обчислювальних ресурсів, енергії та пропускної здатності каналів, робить неможливим пряме запозичення класичних механізмів захисту з традиційних дротових мереж. Натомість, ефективна система виявлення вторгнень у даному середовищі повинна бути адаптивною, легковаговою та здатною функціонувати в умовах децентралізації.

Аналіз базових підходів до виявлення загроз засвідчив, що використання виключно сигнатурних методів є недостатнім через їхню нездатність протистояти новим типам атак, тоді як аномалійні підходи, хоч і дозволяють виявляти невідомі загрози, страждають від високого рівня помилок другого роду. У зв’язку з цим найбільш перспективним напрямом визначено розробку гібридних систем, які поєднують точність сигнатурного аналізу з евристичними можливостями аномалійних детекторів. Встановлено, що для підвищення надійності детекції процес моніторингу має носити комплексний характер і спиратися на багатовимірний вектор ознак, що включає параметри мережевого трафіку, динаміку енергоспоживання вузлів та аналіз маршрутизаційної поведінки. Також було приділено увагу до інтелектуалізації систем захисту за допомогою методів машинного навчання. Результати свідчать про те, що алгоритми, такі як метод опорних векторів, випадкові ліси та нейронні мережі, забезпечують високу точність класифікації складних атак, однак їх імплементація на рівні сенсорних вузлів вимагає застосування спеціальних технік оптимізації або використання полегшених імовірнісних моделей, наприклад, наївного байєсівського класифікатора. Це підкреслює необхідність пошуку балансу між складністю математичної моделі та її енергоефективністю.

3 МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АЛГОРИТМУ ВИЯВЛЕННЯ АТАК

3.1 Вибір атаки для детекції.

Одним із ключових напрямів забезпечення безпеки в БСМ є протидія загрозам, спрямованим на спотворення результатів вимірювань та прийняття рішень на основі недостовірних даних. На відміну від атак, що порушують цілісність маршрутизації або доступність мережі, атаки на рівні інформаційного наповнення сенсорного трафіку є менш помітними, але можуть мати критичні наслідки для систем моніторингу та керування.

У даній роботі для дослідження обрано атаки типу data injection (інжекція даних), сутність яких полягає у навмисному внесенні в потік телеметричної інформації штучних, підмінних або спотворених значень. Зловмисник, отримавши доступ до сенсорного вузла або проміжного елемента обробки даних, може змінювати показники вимірювань таким чином, щоб приховати реальний стан об’єкта моніторингу, створити хибне уявлення про аварійну ситуацію або спрямувати систему керування до прийняття некоректних рішень.

3.2 Середовище для симуляції сценарію атаки на БСМ.

Для програмної реалізації експериментальної частини роботи та моделювання процесів у бездротовій сенсорній мережі було обрано екосистему мови програмування Python. Цей вибір обумовлений необхідністю забезпечення гнучкості розробки та наявністю потужного математичного апарату для наукових обчислень. Використання спеціалізованих бібліотек для статистичного аналізу, обробки масивів даних та машинного навчання дозволяє ефективно імплементувати складні алгоритми виявлення аномалій, а також забезпечує засоби для детальної візуалізації результатів експерименту. Такий інструментарій є

стандартом у сфері Data Science, що гарантує високу продуктивність обчислень та простоту інтеграції різнорідних компонентів моделі.

Функціонування підсистеми моніторингу БСМ відтворюється шляхом генерації синтетичних часових рядів, які емулюють реальну телеметрію сенсорних вузлів. Архітектура симуляційної моделі передбачає роботу системи у двох базових станах: штатному режимі функціонування та в умовах деструктивного впливу. У якості основного вектора загрози розглядається атака типу «ін'єкція даних» (data injection), яка передбачає внесення зловмисником несанкціонованих змін у потік вимірювань. Такий сценарій дозволяє дослідити стійкість алгоритмів детекції до спроб фальсифікації показників, коли скомпрометований вузол намагається приховати реальний стан об'єкта моніторингу або спровокувати хибну реакцію системи управління.

Структурно програмне середовище складається з кількох взаємопов'язаних модулів, що забезпечують повний цикл обробки даних. Первинною ланкою є генератор нормального трафіку, який формує квазіперіодичні послідовності значень, збагачені випадковим шумом для імітації природних флуктуацій вимірювального середовища та похибок датчиків. На цей потік накладається дія модуля емуляції атак, який у визначені моменти часу модифікує фрагменти телеметрії, вносячи аномальні відхилення. Модель загрози є варіативною та дозволяє генерувати як миттєві імпульсні сплески, так і поступовий дрейф параметрів, що ускладнює їх ідентифікацію простими пороговими методами.

Отриманий комбінований потік даних надходить на вхід алгоритму детекції, який виконує обробку сигналів у режимі реального часу, класифікуючи кожне спостереження як нормальне або аномальне. Для оцінки ефективності роботи системи передбачено модуль логування та візуалізації, який фіксує всі події, будує графіки часових залежностей та розраховує метрики точності виявлення. Реалізація моделі у середовищі Python забезпечує повну відтворюваність експериментів, дозволяє легко масштабувати обсяги тестових даних та, за необхідності, розширювати функціонал шляхом інтеграції нових типів атак або більш досконалих методів машинного навчання. Концептуальну блок-схему роботи

програмного комплексу, яка відображає послідовність зазначених етапів, наведено на рисунку 3.1.

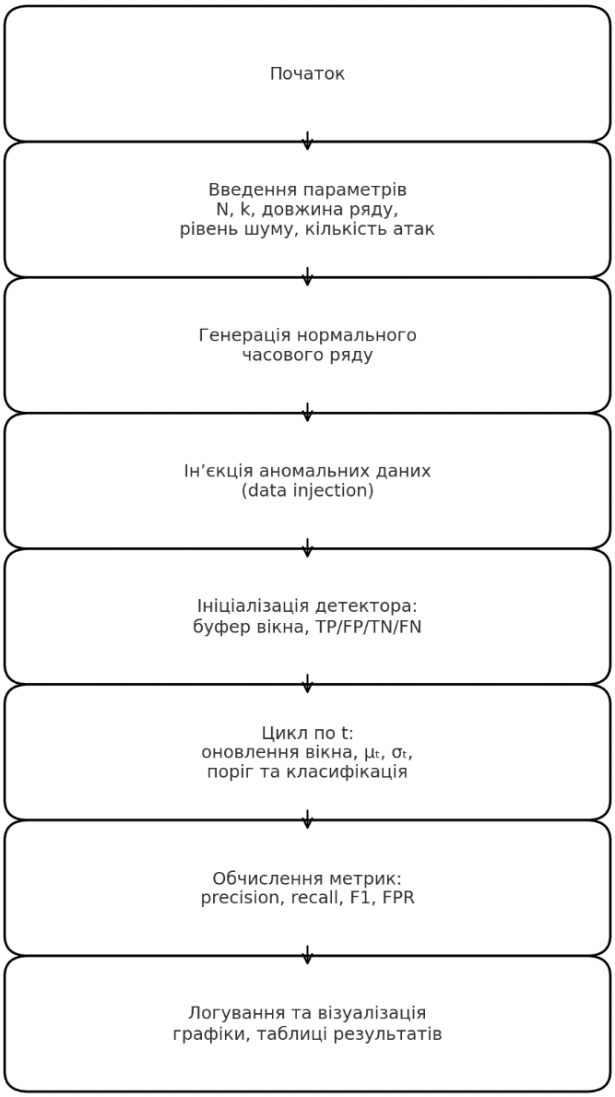


Рис. 3.1 Блок-схема роботи програмного коду симуляції та детекції атак типу data injection

3.3 Опис моделі алгоритму для виявлення загрози.

У даній роботі для виявлення аномалій у телеметричних даних БСМ було обрано алгоритм на основі ковзного статистичного порога, сформованого із використанням локальних параметрів вибірки. Такий підхід є одним з найбільш

інтерпретованих та водночас ефективних для задач детекції різких відхилень, характерних для маніпуляцій сенсорними даними.

Алгоритм ґрунтується на припущенні, що в нормальному режимі зміни параметрів телеметрії описуються стаціонарним або квазістаціонарним процесом із відносно низьким рівнем шуму. Тому статистичні характеристики невеликого вікна (ковзного сегмента) можуть використовуватися для прогнозування очікуваного діапазону значень.

Для кожної нової точки потоку даних обчислюється:

- ковзне середнє μ_t;
- ковзне стандартне відхилення σ_t;
- динамічний поріг відхилення

$$\mathrm{T}_t = \mu_t \pm k \cdot \sigma_t,$$

де k - коефіцієнт чутливості алгоритму.

Спостереження, що виходить за межі порогу, вважається аномальним.

Алгоритм складається з таких етапів:

1. Підготовка вхідного потоку.

   Дані надходять у реальному часі або генеруються в симуляції. Перед обробкою застосовується нормалізація та фільтрація високочастотного шуму (за потреби).

2. Формування ковзного вікна.

   Для останніх N спостережень зберігається буфер, на основі якого обчислюються статистичні параметри. Вибір розміру вікна визначає компроміс між чутливістю та стійкістю алгоритму.

3. Обчислення статистичних характеристик.

   Ковзне середнє та стандартне відхилення відображають локальну поведінку процесу, що дозволяє адаптувати пороги до динамічних умов.

4. Порівняння нового значення з порогами.

Якщо виконано умову:

$$x_t < \mu_t - k\sigma_t \qquad \text{або} \qquad x_t > \mu_t + k\sigma_t,$$

точка позначається як аномалія. Для зменшення кількості хибних спрацювань може застосовуватися фільтр послідовних аномалій. Усі аномальні значення фіксуються з часом їх появи та зберігаються для подальшого аналізу.

3.4 Оцінка обчислювальної складності та ресурсних витрат.

Однією з ключових вимог до алгоритмів є їхня обчислювальна та енергетична ощадливість. З огляду на обмежені обчислювальні ресурси сенсорних вузлів, алгоритми виявлення атак мають мати передбачувану та невисоку обчислювальну складність.

Нехай довжина оброблюваного часового ряду дорівнює T, а розмір ковзного вікна — N. У наївній реалізації для кожного нового вимірювання x_t обчислення ковзного середнього μ_t та стандартного відхилення σ_t передбачає проходження по всьому вікну розміру N, що потребує O(N) операцій на крок. У такому випадку загальна обчислювальна складність алгоритму для всього ряду має порядок O(T*N). Для невеликих значень N це може бути прийнятним, проте зі зростанням розміру вікна така реалізація стає менш ефективною.

Водночас ковзний характер вікна дозволяє застосувати інкрементальні обчислення, за яких для переходу від μ_t до $\mu_t + 1$ немає потреби повторно переглядати всі N елементів. Зберігаючи суму значень у вікні та суму їх квадратів, можна оновлювати відповідні статистики, лише віднімаючи вклад елемента, що «випадає» з вікна, та додаючи вклад нового елемента. За такого підходу кожен крок обробки вимагає сталої кількості операцій, тобто обчислювальна складність всього алгоритму знижується до O(T), що є лінійною відносно довжини часового ряду. Це робить алгоритм придатним для роботи в режимі потокової обробки даних на сенсорному вузлі або шлюзі.

Обсяг необхідної пам’яті також є критичним параметром. Запропонований алгоритм потребує зберігання поточного значення вимірювання, буфера останніх N вимірів (або еквівалентної структури для підтримки ковзних сум), а також невеликої кількості службових змінних (поточні μ_t, σ_t, показники TP, FP, TN, FN). Таким чином, вимоги до пам’яті мають порядок O(N). За типових значень N, які використовуються у роботі, розмір буфера є невеликим і може бути реалізований навіть на мікроконтролерах із обмеженою оперативною пам’яттю.

З енергетичної точки зору статистичний пороговий алгоритм є відносно ощадливим, оскільки не вимагає складних операцій, таких як матричні перетворення, ітераційні оптимізаційні процедури або операції з плаваючою комою високого порядку. Основними джерелами енергоспоживання є виконання нескладних арифметичних дій та, потенційно, передача результатів детекції по бездротовому каналу. Важливо, що використання локальної обробки на вузлі дає змогу істотно зменшити обсяг передаваних даних (надсилаються переважно індикатори аномалій, а не повні часові ряди), що додатково знижує енергетичні витрати мережі.

3.5 Методика проведення експерименту.

Методика проведення експерименту передбачає поетапне моделювання поведінки безпровідної сенсорної мережі в умовах нормальної роботи та під впливом аномального трафіку, створеного шляхом ін’єкції штучних атак типу data injection. У межах цього дослідження експериментальна процедура включає формування контрольованого середовища, генерацію даних, налаштування алгоритму виявлення та оцінювання результатів детекції.

На першому етапі створюється потік телеметричних вимірювань, який моделює поведінку типового сенсорного вузла. Потік складається з:

- нормальних даних, що змінюються відповідно до рівномірного або гаусового шуму;

- аномальних значень, що вставляються у визначені моменти часу та відображають вплив атаки.

Для забезпечення репрезентативності експерименту використовуються такі параметри:

- довжина всього потоку даних – від 500 до 5000 вимірювань;
- інтенсивність шуму – невелика (5–10 % від базового значення);
- точки атаки – поодинокі сплески, групові ін’єкції або короткі періоди некоректної поведінки.

На другомі етапі (рисунок 3.1) реалізується симуляція у середовищі Python з використанням базових бібліотек numpy та matplotlib. Тут перевіряється коректність структури даних та відсутність неконтрольованих пропусків.

```
np.random.seed()  # нова симуляція при кожному запуску

data_length = 600
baseline = 10
noise_level = 0.5

# нормальні дані
normal_data = baseline + np.random.normal(0, noise_level, data_length)

# копія з ін'єкціями атаки
data = normal_data.copy()

# випадкові позиції атак
attack_positions = np.random.choice(range(100, 500), size=5, replace=False)
for pos in attack_positions:
    data[pos] += np.random.uniform(5, 12)  # spike-атаки

# ground truth
ground_truth = np.zeros(data_length)
ground_truth[attack_positions] = 1
```

Рис. 3.2 Перший та другий етап експериментального дослідження

На третьому етапі ініціалізуються та налаштовуються параметри алгоритму: ромір ковзного вікна N, коефіцієнт чутливості k та режим фыльтрацыъ аномалій.

Також задається структура змінних для збереження позначок «аномалія/норма» та накопичується статистика для подальшої оцінки точності алгоритму.

На четвертому етапі (рисунок 3.2) програма послідовно обробляє кожне нове значення потоку: додає його до ковзного буфера, обчислює поточні статистики μ_t, σ_t, визначає статус нової точки, фіксує проміжні дані.

```
34  window_size = 20
35  k = 3  # чутливість порога
36
37  mu_list = []
38  sigma_list = []
39  anomaly = np.zeros(data_length)
40
41  for t in range(data_length):
42
43      if t < window_size:
44          mu_list.append(0)
45          sigma_list.append(0)
46          continue
47
48      window = data[t - window_size:t]
49      mu = np.mean(window)
50      sigma = np.std(window)
51
52      mu_list.append(mu)
53      sigma_list.append(sigma)
54
55      upper = mu + k * sigma
56      lower = mu - k * sigma
57
58      if data[t] > upper or data[t] < lower:
59          anomaly[t] = 1
60
```

Рис. 3.3 Третій та четвертий етап експериментального дослідження

На пятому етапі (рисунок 3.3) для підбиття підсумків експерименту визначаються такі метрики:

- True Positive (TP) – атакуючі точки, які були правильно виявлені;
- False Positive (FP) – нормальні точки, помилково позначені як аномальні;
- True Negative (TN) – правильно ідентифіковані нормальні значення;
- False Negative (FN) – атаки, які детектор не розпізнав.

На основі цих значень вираховуються:

$$Precision = \frac{TP}{TP+FP}, \qquad Recall = \frac{TP}{TP+FN}, \qquad F1score = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall}$$

Precision, recall і F1-score це стандартні метрики якості для задач бінарної класифікації “норма” vs “атака/аномалія”. Вони описують, наскільки добре алгоритм знаходить атаки і наскільки мало він помиляється. Усі три метрики безрозмірні, тобто це частки ймовірності в діапазоні [0;1] або ті самі значення у відсотках.

Precision (точність спрацювань) описує те, як часто спрацювання аглоритму на вияв загрози є правильним, тобто серед усіх знайдених аномалій яка частка справді є атаками.

Метрика recall (повнота або чутливість) відображає скільки реальних атака знайшов алгоритм.

F1-score - гармонічне середнє precision і recall, вона описує один узагальнений показник якості, який “штрафує”, якщо хоча б одна з метрик низька. На цю метрику особливо зручно дивитись, якщо precision високий, а recall низький або навпаки, F1 буде низьким. У задачах оцінки ефективності алгоритмів виявлення вторгнень F-міра виступає своєрідним «арбітром», що дозволяє знайти баланс між двома конфліктуючими цілями: мінімізацією хибних тривог precision та максимізацією виявлених загроз recall. Вибір саме гармонічного, а не звичайного арифметичного середнього як математичної основи цієї метрики є принциповим моментом. Гармонічне середнє має унікальну властивість: воно завжди тяжіє до меншого з двох значень. Це означає, що F1-score діє як жорсткий фільтр — якщо хоча б один із показників є низьким, підсумкова оцінка також буде низькою, навіть якщо другий показник дорівнює 100%.

```
TP = np.sum((anomaly == 1) & (ground_truth == 1))
FP = np.sum((anomaly == 1) & (ground_truth == 0))
TN = np.sum((anomaly == 0) & (ground_truth == 0))
FN = np.sum((anomaly == 0) & (ground_truth == 1))

precision = TP / (TP + FP + 1e-9)
recall = TP / (TP + FN + 1e-9)
f1 = 2 * precision * recall / (precision + recall + 1e-9)

print("\n--- РЕЗУЛЬТАТИ ---")
print("TP:", TP)
print("FP:", FP)
print("TN:", TN)
print("FN:", FN)
print(f"Precision: {precision:.3f}")
print(f"Recall:    {recall:.3f}")
print(f"F1-score:  {f1:.3f}")
```

Рис. 3.4 П’ятий етап експериментального дослідження

На фінальному, шостому етапі (рисунок 3.4) формується наглядна графічна візуалізація отриманих результатів та отримуються дані значень для кожної з метрик у вигляді текстового виводу в термінал (рисунок 3.5).

```
plt.figure(figsize=(14, 6))
plt.plot(data, label="Дані сенсора", linewidth=1)

# істинні атаки
plt.scatter(attack_positions, data[attack_positions],
            color="red", s=80, label="Атаки (ground truth)", zorder=6)

# виявлені аномалії (зміщення +0.15)
plt.scatter(np.where(anomaly == 1), data[anomaly == 1] + 0.15,
            color="orange", s=60, label="Виявлені аномалії", zorder=7)

# ковзне середнє
plt.plot(mu_list, linestyle="--", color="tab:orange", label="Ковзне середнє", linewidth=1.5)

plt.title("Симуляція атаки та її виявлення", fontsize=14)
plt.xlabel("Часовий індекс")
plt.ylabel("Значення вимірювання")
plt.grid(True)
plt.legend()
plt.tight_layout()
plt.show()
```

3.5 Шостий етап експериментального дослідження

```
PS C:\Users\Acorn\Desktop\sim> python main.py

--- РЕЗУЛЬТАТИ ---
TP: 5
FP: 2
TN: 593
FN: 0
Precision: 0.714
Recall:    1.000
F1-score:  0.833
PS C:\Users\Acorn\Desktop\sim>
```

Рис. 3.6 Текстовий вивід значень основних метрик

Після обчислення метрик якості (TP, FP, TN, FN та похідних показників precision, recall, F1-score) виконується побудова графіка (рисунок 3.6), який забезпечує наочне представлення як вихідного сенсорного сигналу, так і результатів роботи алгоритму детекції.

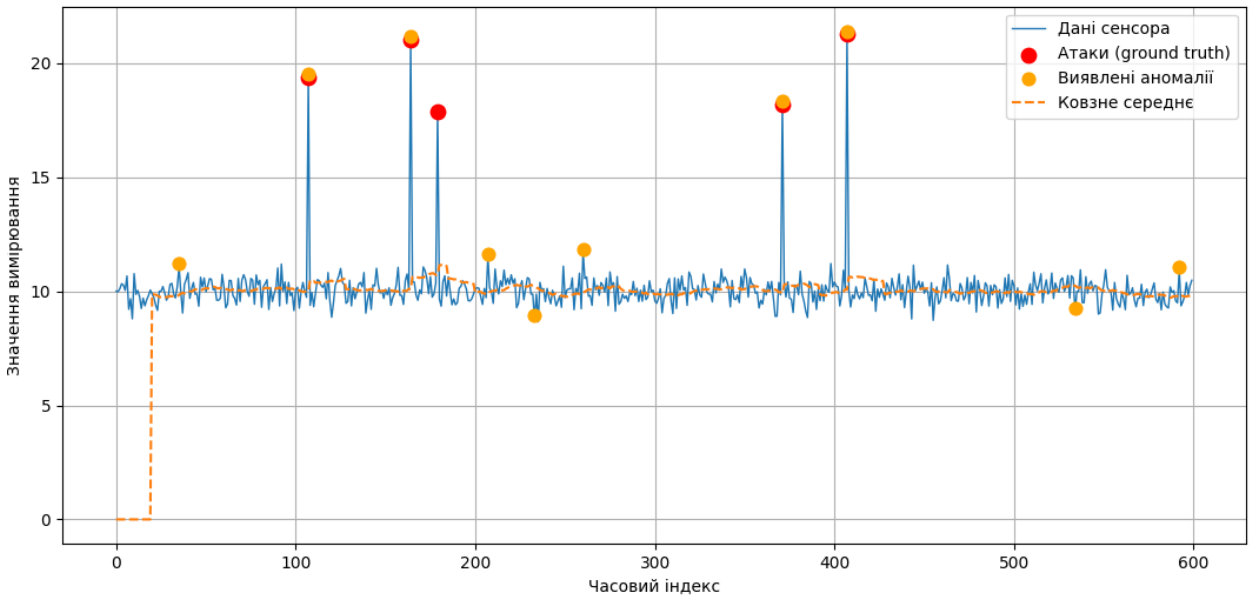


Рис. 3.7 Симуляція атаки та її виявлення

На графіку відображаються такі елементи:

- часовий ряд вимірювань сенсора як основна крива, що демонструє нормальні коливання сигналу та можливі аномальні відхилення;
- точки атак (ground truth), нанесені маркерами у відповідних часових індексах, що відображають моменти інжекції спотворених значень у дані;
- точки, позначені алгоритмом як аномалії, які відображають фактичні спрацьовування детектора;
- ковзне середнє (або інші оцінки локальної тенденції), що демонструє адаптацію алгоритму до нормального рівня сигналу та слугує основою для формування динамічного порога.

3.6 Аналіз результатів експерименту.

Для оцінювання ефективності розробленого алгоритму детекції атак типу data injection було виконано серію симуляцій із варіюванням ключових параметрів методу: розміру ковзного статистичного вікна $\boldsymbol{N} \in \{\mathbf{10}, \mathbf{20}, \mathbf{30}\}$ та коефіцієнта чутливості порога $\boldsymbol{k} \in \{\mathbf{2.0}, \mathbf{2.5}, \mathbf{3.0}, \mathbf{3.5}, \mathbf{4.0}\}$**.** Зміна параметра N дозволяє оцінити вплив “інертності” статистичних оцінок (середнього та стандартного відхилення) на результати детекції, тоді як параметр k визначає жорсткість порога та, відповідно, баланс між пропусками атак і кількістю хибних спрацьовувань. Таким чином, обрана схема експерименту дає змогу дослідити компроміс між чутливістю детектора до відхилень у даних та його стійкістю до природного шуму сенсорних вимірювань.

Загалом виконано 48 незалежних прогонів симуляції, структурованих таким чином: для кожного значення N було проведено по 16 прогонів, які додатково поділено на 4 групи відповідно до значень k, по 4 прогони для кожної пари параметрів (N,k). У кожному прогоні формувався часовий ряд сенсорних значень із шумом, після чого у випадково обраних позиціях виконувалася інжекція аномальних значень (сплесків), що моделюють атаку. Алгоритм детекції обробляв

дані послідовно, формував адаптивний поріг на основі локальних статистик та приймав рішення щодо належності кожного нового значення до класу “норма” або “аномалія”.

У таблиці 3.1 наведено результати для кожного окремого прогону: номер прогону та параметри (N,k), а також значення елементів матриці помилок – правильно виявлені атакуючі точки (TP), хибно позначені нормальні точки (FP), правильно ідентифіковані нормальні значення (TN) та атаки, які детектор не розпізнав (FN). На основі цих величин обчислено основні показники якості: метрику точності спрацьовувань (precision), метрику повноти виявлення (recall), інтегральний показник F1-score, а також частоту хибних спрацювань (FPR), що характеризує ймовірність помилкового сигналу тривоги в умовах відсутності атаки. Представлені дані слугують основою для подальшого аналізу впливу параметрів алгоритму на якість детекції та формування висновків щодо оптимальних налаштувань для розглянутого сценарію атак.

Таблиця 3.1

Метрики алгоритму детекції для різних параметрів N та k

№	Розмір вікна **N**	Коефіцієнт чутливості **k**	**TP**	**FP**	**TN**	**FN**	**Precision**	**Recall**	**F1score**	**FPR**
1	10	2.5	4	29	566	1	0.121	0.8	0.211	0.049
2			4	29	566	1	0.121	0.8	0.211	0.049
3			5	33	562	0	0.132	1.0	0.233	0.055
4			5	27	568	0	0.156	1.0	0.27	0.045
5		3.0	4	16	579	1	0.2	0.8	0.32	0.027
6			4	15	580	1	0.211	0.8	0.333	0.025
7			4	18	577	1	0.217	1.0	0.357	0.03

Продовження таблиці 3.1

№	Розмір вікна **N**	Коефіцієнт чутливості **k**	**TP**	**FP**	**TN**	**FN**	**Precision**	**Recall**	**F1score**	**FPR**
8	10	3.0	4	17	578	0	0.227	1.0	0.37	0.029
9		3.5	4	8	580	1	0.333	0.8	0.471	0.013
10			4	5	577	1	0.444	0.8	0.571	0.008
11			5	8	578	0	0.385	1.0	0.556	0.013
12			5	9	587	0	0.357	1.0	0.526	0.015
13		4.0	4	4	591	1	0.5	0.8	0.615	0.007
14			4	2	593	1	0.667	0.8	0.727	0.003
15			5	5	590	0	0.5	1.0	0.667	0.008
16			5	4	591	0	0.556	1.0	0.714	0.007
17	20	2.5	4	17	578	1	0.19	0.8	0.308	0.029
18			4	13	582	1	0.235	0.8	0.364	0.022
19			5	13	582	0	0.278	1.0	0.435	0.022
20			5	18	577	0	0.217	1.0	0.357	0.03
21		3.0	4	7	588	1	0.364	0.8	0.5	0.012
22			4	4	591	1	0.5	0.8	0.615	0.007
23	20		5	8	587	0	0.385	1.0	0.556	0.013

Продовження таблиці 3.1

№	Розмір вікна **N**	Коефіцієнт чутливості **k**	**TP**	**FP**	**TN**	**FN**	**Precision**	**Recall**	**F1score**	**FPR**
24		3.0	5	5	590	0	0.5	1.0	0.667	0.008
25			3	3	592	2	0.5	0.6	0.545	0.005
26		3.5	4	1	594	1	0.8	0.8	0.8	0.002
27			5	3	592	0	0.625	1.0	0.769	0.005
28	20		5	2	593	0	0.714	1.0	0.833	0.003
29			3	3	592	2	0.5	0.6	0.545	0.005
30		4.0	4	0	595	1	1.0	0.8	0.889	0.0
31			5	1	594	0	0.833	1.0	0.909	0.002
32			5	1	594	0	0.833	1.0	0.909	0.002
33		2.5	5	19	576	0	0.208	1.0	0.345	0.032
34			5	7	588	0	0.417	1.0	0.558	0.012
35			5	10	585	0	0.333	1.0	0.5	0.017
36	30		5	11	584	0	0.312	1.0	0.476	0.018
37			4	3	592	1	0.571	0.8	0.667	0.005
38		3.0	5	2	593	0	0.714	1.0	0.833	0.003
39	30		5	2	593	0	0.714	1.0	0.833	0.003

Продовження таблиці 3.1

№	Розмір вікна **N**	Коефіцієнт чутливості **k**	**TP**	**FP**	**TN**	**FN**	**Precision**	**Recall**	**F1score**	**FPR**
40		3.0	5	6	589	0	0.455	1.0	0.625	0.01
41			4	1	594	1	0.8	0.8	0.8	0.002
42		3.5	4	1	594	1	0.8	0.8	0.8	0.002
43			5	0	595	0	1.0	1.0	1.0	0.0
44	30		5	1	594	0	0.833	1.0	0.909	0.002
45			3	0	595	2	1.0	0.6	0.75	0.0
46		4.0	4	0	595	1	1.0	0.8	0.889	0.0
47			5	0	595	0	1.0	1.0	1.0	0.0
48			5	0	595	0	1.0	1.0	1.0	0.0

На основі 48 прогонів можна зробити кілька чітких висновків про поведінку алгоритму та вплив його налаштувань.

По-перше, у результатах добре видно компроміс між точністю та повнотою. Зі збільшенням коефіцієнта чутливості порога k алгоритм стає “обережнішим”: кількість хибних спрацьовувань зменшується, тому точність зростає, а FPR падає. Наприклад, для N=10 перехід від k=2.5 до k=4.0 зменшив середню кількість FP приблизно з 29.5 до 3.75, що підняло precision з ∼0.133 до ∼0.556 і збільшило F1 з ∼0.231 до ∼0.681. При цьому recall у цих серіях залишався приблизно на рівні 0.90, тобто сплескові інжекції даних загалом виявлялися, але головною проблемою при малих k була саме велика кількість “зайвих тривог”.

По-друге, суттєвий вплив має розмір ковзного вікна N. При збільшенні N оцінки μ_t та σ_t стають стабільнішими, тому поріг менше реагує на випадковий шум, а отже зменшується FP і покращується precision та F1. У середньому по всіх k маємо зростання якості при переході від N=10 до N=30: середній F1 підвищився приблизно з 0.447 до 0.751, а середній FPR знизився приблизно з 0.024 до 0.007. Це означає, що більші вікна є більш придатними для сигналів із шумом, де потрібно відокремити нормальні флуктуації від справжніх інжекцій.

У таблиці можна виділити конфігурації, що дають найкращий баланс. Найвищі значення F1 отримано для великих N і високих k: зокрема, при N=30, k=4.0 середній precision = 1.0 (тобто FP практично відсутні), F1≈0.91 але recall знижується до ~0.85 (частина атак може бути пропущена через “жорсткий” поріг). Якщо ж потрібен більш збалансований варіант із вищою повнотою при все ще низькому рівні FP, показовою є конфігурація N=30, k=3.5: precision ~0.858, recall ~0.90, F1 ~0.877, FPR ~0.001. Отже, з отриманих прогонів видно, що для сплескових data injection атак оптимальними є N≈30 та k≈3.5–4.0k залежно від того, що критичніше: мінімум хибних тривог (більший k) чи мінімум пропусків атак (трохи менший k).

Зобразимо залежність метрики F1score від k з таблиці у вигляді графіку для подальшого аналізу.

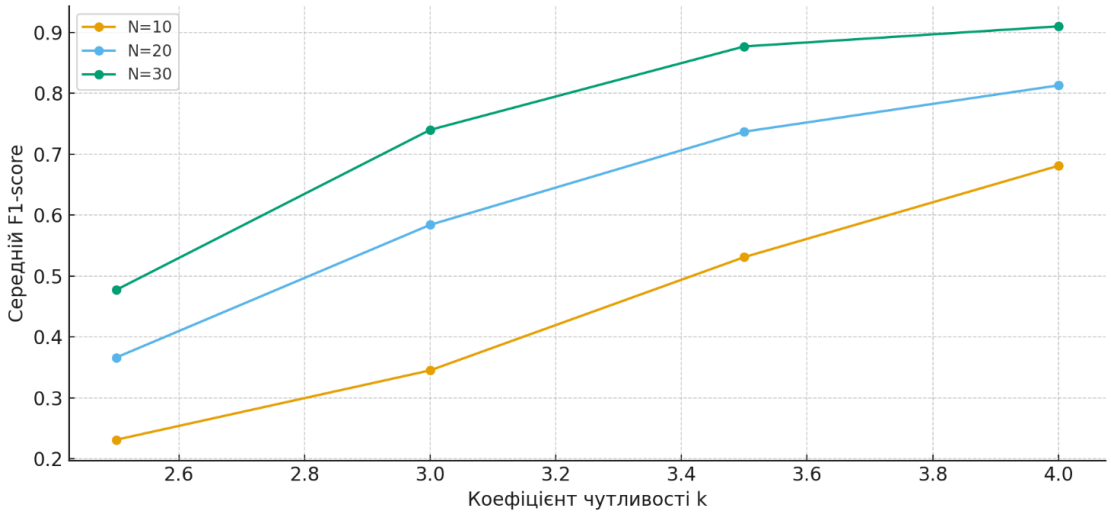


Рис. 3.8 Графік залежності F1-score від k при різних розмірах ковзного вікна N

Бачимо чітку тенденцію, по-перше, F1-score монотонно зростає зі збільшенням зі збільшенням k для всіх досліджених розмірів вікна. Це означає, що у нашому сценарії основним джерелом погіршення якості при малих k є саме хибні спрацювання (FP), які «псують» precision і відповідно F1. Фактично при малих k алгоритм надто чутливий до природного шуму сигналу, а при більших k шумові відхилення все рідше виходять за поріг.

По-друге, вплив розміру ковзного вікна є системним: криві на графіку показують, що більші вікна (20–30) забезпечують більш високі значення F1 майже для всіх k. Це можна інтерпретуватитак: при більшому N локальні оцінки μ_t та σ_t стають стабільнішими, зменшується випадкове «пересмикування» порога, а отже знижується кількість FP і підвищується узгодженість спрацьовувань саме з інжекціями.

Отже, для моделі атак data injection у вигляді сплесків оптимальна робота алгоритму досягається при помірно великому ковзному вікні (близько 20–30) і достатньо високому порозі (приблизно k=3.5–4.0). У цих умовах алгоритм забезпечує кращий баланс між точністю і повнотою виявлення більшості атак, що підтверджується зростанням F1-score та зменшенням FPR.

3.7 Оцінка ефективності алгоритму та висновки експерименту.

У межах виконаного експерименту проведено оцінювання ефективності алгоритму виявлення атак типу data injection на основі ковзного статистичного порога. Ефективність розглядалася комплексно: з позицій якості детекції (через precision, recall та F1-score), частоти хибних спрацьовувань (FPR), чутливості до випадкового шуму сенсорних вимірювань, а також практичної придатності алгоритму до використання в ресурсно-обмежених середовищах, характерних для безпровідних сенсорних мереж. Оскільки в експерименті моделювалися інжекції у вигляді короткотривалих різких відхилень, основним об’єктом оцінювання був

сценарій spike injection, для якого статистичні порогові методи є інтерпретованими та обчислювально доступними.

Результати підтверджують, що запропонований алгоритм є дієвим для виявлення сплескових інжекцій за умови коректного підбору параметрів N і k. Згідно з таблицею 3.2, зі зростанням параметра чутливості k спостерігається стійка тенденція зменшення кількості хибних спрацьовувань, що відображається у зниженні FPR і зростанні точності. Така поведінка є очікуваною: більші значення k формують ширший допустимий інтервал навколо локального середнього, а отже алгоритм рідше реагує на випадкові шумові флуктуації. При цьому recall у більшості конфігурацій зменшується відносно помірно, тобто детектор зберігає здатність виявляти значну частину атак, але робить це "обережніше". У підсумку інтегральний показник F1-score, який балансує точність і повноту, зазвичай покращується при переході до більш консервативних порогів.

Окремо слід відзначити вплив розміру ковзного вікна N. Як видно з рисунка 3.3, збільшення N приводить до систематичного підвищення F1-score для всіх перевірених значень k. Це пояснюється стабілізацією оцінок μ_t та σ_t: при більшому вікні статистичні параметри менш чутливі до одиничних шумових викидів, а отже зменшується кількість FP і підвищується точність. Для малих вікон поріг формується на основі меншої кількості даних, що робить алгоритм значно більш чутливим до випадкових відхилень, а тому збільшує кількість хибних тривог, знижуючи загальну якість у сенсі F1. Таким чином, у розглянутому сценарії spike injection використання помірно великого вікна (20–30 значень) є більш доцільним, оскільки підвищує стійкість алгоритму до шуму без критичної втрати чутливості до атаки.

З практичної точки зору, результати дозволяють сформувати рекомендації щодо вибору параметрів. Конфігурації з N=30 та $k \in [3.5, 4.0]$ демонструють найвищі середні значення F1-score і мінімальні значення FPR, тобто забезпечують найкращий баланс між виявленням атак та обмеженням помилкових спрацьовувань. Водночас надмірне збільшення k може призводити до зниження чутливості, що є критичним у задачах, де пропуск атаки має вищу "вартість", ніж

хибна тривога. Тому остаточний вибір параметрів має здійснюватися з урахуванням пріоритетів системи: мінімізація FP (безпека/стабільність тривог) або максимізація виявлених атак (мінімізація FN).

Важливою перевагою запропонованого підходу є його низька обчислювальна складність та придатність до реалізації у вбудованих середовищах. У базовому вигляді для кожного нового вимірювання виконуються операції обчислення середнього та стандартного відхилення на вікні розміру N, що є прийнятним для невеликих N. За необхідності метод може бути оптимізований до ковзних обчислень із підтримкою сум і сум квадратів, що зменшує обчислювальні витрати на крок та потребує лише буфера фіксованого розміру. Отже, алгоритм є перспективним як легковаговий механізм контролю достовірності телеметричних даних на вузлах або шлюзах БСМ.

Проведений експеримент має природні обмеження, які визначають напрямки подальшого розвитку. По-перше, оцінювання виконувалося для сплескових інжекцій, тоді як поступові атаки типу drift можуть бути менш помітними для простих порогових схем. По-друге, модель використовує синтетичний шум і один тип сенсорного сигналу; у реальних системах можливі нестаціонарність, зміни режимів роботи, сезонність та корельовані багатовимірні вимірювання. Перспективним є розширення підходу шляхом додавання накопичувальних критеріїв, наприклад EWMA (Exponentially Weighted Moving Average) чи CUSUM (Cumulative Sum), або комбінування статистичної детекції з методами машинного навчання для підвищення стійкості до складніших сценаріїв атак і змін середовища.

3.8 Практичні рекомендації щодо сценаріїв інтеграції алгоритму в БСМ.

Результати моделювання та аналізу, дають змогу сформулювати низку практичних рекомендацій щодо використання розробленого алгоритму в реальних безпровідних сенсорних мережах, а також окреслити типові сценарії його інтеграції в архітектуру системи моніторингу. З огляду на обмежені ресурси сенсорних вузлів

і специфіку трафіку БСМ, особливу увагу приділено питанням розподілу обчислювального навантаження, мінімізації службового трафіку та узгодженню параметрів алгоритму з вимогами до якості виявлення атак.

Один із базових варіантів передбачає розгортання алгоритму безпосередньо на сенсорних вузлах. У такому сценарії вузол самостійно виконує локальний аналіз власних вимірювань, підтримуючи ковзне вікно розміру N та обчислюючи статистичні пороги. У разі виявлення аномалій він генерує сигнал тривоги або позначає підозрілі вимірювання спеціальним маркером. Перевага такого підходу полягає в тому, що в мережу не передаються надлишкові обсяги «сирих» даних: замість цього надсилаються лише стислі повідомлення про інциденти, що знижує енерговитрати на радіоканал і підвищує масштабованість системи. Обмеженням є необхідність дуже ощадливого використання пам’яті та обчислювальних ресурсів, що накладає додаткові вимоги на реалізацію алгоритму, зокрема на ефективність обчислень μ_t та σ_t.

Альтернативним підходом є розміщення модуля детекції на пограничних вузлах або шлюзі, які збирають дані від групи сенсорних вузлів. У цьому випадку окремі сенсори передають свої вимірювання у відносно стисненому вигляді, а аналіз виконується на вузлі з більшими обчислювальними можливостями. Така архітектура відкриває можливість поєднувати статистичний пороговий метод з додатковими механізмами, наприклад, кореляційним аналізом даних від кількох сенсорів, що вимірюють споріднені параметри. Водночас збільшується обсяг трафіку всередині кластера, тому доцільним є застосування адаптивних режимів передачі, наприклад надсилання даних з меншою частотою у відсутності аномалій.

Окрему увагу слід приділити можливості кооперативного використання алгоритму в розподілених системах виявлення загроз. Навіть за умови локального аналізу на вузлах, їх індивідуальні рішення можуть об’єднуватися на рівні кластера або шлюзу для зменшення впливу випадкових помилок і підвищення достовірності колективного вердикту. Наприклад, рішення про наявність атаки у певному регіоні мережі може прийматися лише у випадку, якщо аномалії одночасно зафіксовано на кількох сусідніх вузлах. Такий підхід дозволяє зменшити чутливість системи до

одиничних помилкових спрацьовувань та підвищує стійкість до локальних відмов сенсорів.

Загалом, результати моделювання свідчать, що запропонований алгоритм є перспективним для інтеграції в реальні системи на основі БСМ як легковаговий модуль детекції інжекційних атак. Його простота й низькі ресурсні вимоги поєднуються з можливістю гнучкого налаштування параметрів під конкретні умови експлуатації. Водночас практична реалізація такого підходу потребує подальших досліджень у напрямі адаптації до нестаціонарних режимів роботи сенсорів, багатовимірних сигналів, а також поєднання описаного методу з іншими механізмами моніторингу та кореляційного аналізу подій у мережі.

ВИСНОВКИ

У даній магістерській роботі розглянуто проблему виявлення атак та підвищення рівня безпеки безпровідних сенсорних мереж, які широко застосовуються в системах моніторингу та керування і є вразливими через обмежені ресурси, бездротове середовище передавання та можливість компрометації вузлів. У першому та другому розділах роботи систематизовано основи функціонування БСМ, їх архітектуру та типові компоненти, окреслено модель загроз і основні класи атак, а також узагальнено механізми захисту, зокрема криптографічні підходи та захищені протоколи маршрутизації. Це створило підґрунтя для аргументованого вибору підходу до виявлення загроз, орієнтованого на практичну реалізацію в умовах ресурсних обмежень.

Основну увагу в роботі зосереджено на атаках типу data injection, які полягають у навмисному спотворенні телеметричних даних і здатні призводити до прийняття помилкових рішень навіть за формально коректної роботи мережі. Для дослідження було сформовано симуляційне середовище в Python, що відтворює нормальну поведінку сенсорного сигналу з шумом і контрольовано вводить інжекційні аномалії у вигляді сплесків. На цій основі реалізовано алгоритм виявлення на базі ковзного статистичного порога, який використовує локальні оцінки середнього та стандартного відхилення для адаптивного формування меж “нормальної” поведінки даних.

Експериментальні дослідження показали, що обраний алгоритм є ефективним для виявлення сплескових інжекцій за умови коректного налаштування параметрів, зокрема розміру ковзного вікна та коефіцієнта чутливості порога. Аналіз результатів за метриками precision, recall та F1-score підтвердив наявність характерного компромісу між чутливістю до відхилень і кількістю хибних спрацьовувань: підвищення порогового параметра зменшує частоту FP та підвищує precision, при цьому recall для сплескових атак знижується несуттєво. Візуалізація часових рядів додатково дозволила інтерпретувати

причини помилок детекції та продемонструвала узгодженість між моментами інжекції і спрацьовуваннями алгоритму.

Отримані результати свідчать, що запропонований підхід може бути використаний як легковаговий механізм контролю достовірності телеметрії у безпровідних сенсорних мережах, оскільки він є інтерпретованим і не потребує значних обчислювальних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Butun I. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures / Ismail Butun, Patrik Österberg, Houbing Song // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, no. 1. – 616–644 стор.
2. Karlof C. Secure routing in wireless sensor networks: Attacks and countermeasures / Chris Karlof, David Wagner // Ad hoc networks. – 2003. – Vol. 1, no. 2–3. – 293–315 стор.
3. Mitchell R. A survey of intrusion detection techniques for cyber-physical systems / Robert Mitchell, Ing-Ray Chen // ACM Computing Surveys (CSUR). – 2014. – Vol. 46, no. 4. – 1–29 стор.
4. Khan M. A. A survey of security issues for WSNs / M. A. Khan, K. Salah // IEEE Communications Surveys & Tutorials. – 2018. – Vol. 20, no. 2. – 1044–1067 стор.
5. Otoum S. An adaptively supervised and intrusion-aware deep learning-based approach for WSNs / Safa Otoum, Burak Kantarci, Hussein T. Mouftah // IEEE Transactions on Cognitive Communications and Networking. – 2019. – Vol. 5, no. 2. – 367–379 стор.
6. Cortes C. Support-vector networks / Corinna Cortes, Vladimir Vapnik // Machine learning. – 1995. – Vol. 20, no. 3. – 273–297 стор.
7. Breiman L. Random forests / Leo Breiman // Machine learning. – 2001. – Vol. 45, no. 1. – 5–32 стор.
8. Goodfellow I. Deep Learning / Ian Goodfellow, Yoshua Bengio, Aaron Courville. – Cambridge: MIT Press, 2016. – 800 стор.
9. WebRTC 1.0: Real-Time Communication Between Browsers [Електронний ресурс] // w3.org. – 2024. – Режим доступу до ресурсу: https://www.w3.org/TR/webrtc/.

10. Rescorla E. WebRTC Security Architecture (RFC 8827) [Електронний ресурс] // ietf.org. – 2021. – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc8827.
11. Newsome J. The sybil attack in sensor networks: analysis & defenses / James Newsome, Dawn Song, David Wagner // Proceedings of the 3rd international symposium on Information processing in sensor networks. – ACM, 2004. – 259–268 стор.
12. Ngai E. C. H. Intruder detection for sinkhole attacks in wireless sensor networks / E. C. H. Ngai, J. Liu, M. R. Lyu // IEEE International Conference on Communications. – 2006. – Vol. 5. – 2383–2388 стор.
13. Sommer R. Outside the closed world: On using machine learning for network intrusion detection / Robin Sommer, Vern Paxson // 2010 IEEE symposium on security and privacy. – 2010. – 305–316 стор.
14. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks (RFC 6550) [Електронний ресурс] // ietf.org. – 2012. – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc6550.
15. Zarpelão B. B. A survey of intrusion detection in Internet of Things / B. B. Zarpelão, R. S. Miani, C. T. Kawakani // Journal of Network and Computer Applications. – 2017. – Vol. 84. – 25–37 стор.
16. Lorenc A. Intrusion detection system for wireless sensor networks based on machine learning / A. Lorenc, M. Kaczmarek // Przegląd Elektrotechniczny. – 2020. – Vol. 96, no. 9. – 120–124 стор.
17. WebRTC concepts and usage [Електронний ресурс] // developer.mozilla.org. – 2024. – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/WebRTC_concepts_and_usage.
18. STUN [Електронний ресурс] // wikipedia.org. – 2024. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/STUN.
19. Grigorik I. High Performance Browser Networking / Ilya Grigorik. – Sebastopol: O'Reilly Media, 2013. – 400 стор.

20. Gunning D. Explainable artificial intelligence (XAI) / David Gunning // Defense Advanced Research Projects Agency (DARPA). – 2017. – Vol. 2, no. 2. – 1–2 стор.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Державний університет
інформаційно-комунікаційних
технологій

Державна атестаційна робота
на здобуття ступеня магістра на тему:
«*Алгоритми виявлення атак і забезпечення безпеки в бездротових сенсорних мережах*»

Виконав:
студент VI курсу,
гр. ТСДМ-62
Головаш С. О.
Керівник:
к.т.н., доцент
Домрачева К. О.

1

Об’єкт та предмет дослідження

Об’єктом дослідження є **бездротові сенсорні мережі** (БСМ).

Предметом дослідження є алгоритми виявлення атак.

Метою роботи є дослідження та розробка ефективного алгоритму виявлення атак.

2

Структура роботи

Розділ 1. Аналіз принципів роботи БСМ, класифікація загроз та вразливостей.

Розділ 2. Систематизація методів виявлення атак та підходів до захисту.

Розділ 3. Розробка моделі, програмна симуляція атаки Data Injection та експериментальна оцінка алгоритму.

3

Вразливі складові БСМ

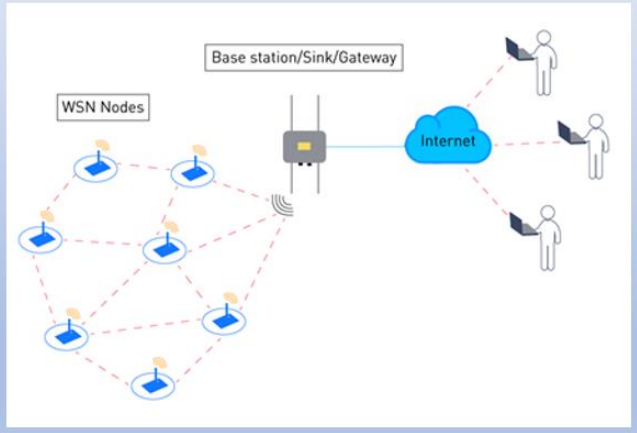


Рис. 1.1 Типова схема безпровідної сенсорної мережі

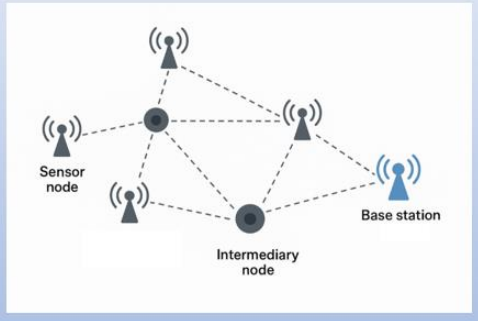


Рис. 1.3 Приклад конфігурації БСМ з проміжними вузлами

4

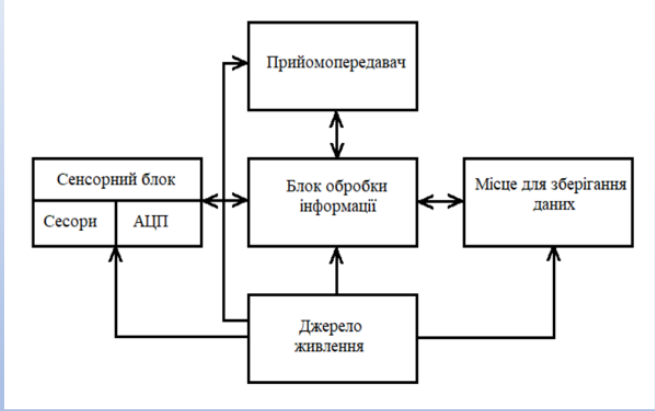


Рис. 1.2 Блок-схема нода (сенсорного вузла)

5

Таблиця 1.1 Порівняльна характеристика пасивних та активних атак

Ознака	Пасивні атаки	Активні атаки
Втручання в передачу даних	Відсутнє	Присутнє
Можливість виявлення	Дуже низька	Порівняно висока
Основна мета	Отримання інформації	Порушення роботи мережі
Рівень загрози	Інформаційний	Деструктивний
Приклади	Eavesdropping, Traffic Analysis	Jamming, Sinkhole, Data injection, Sybil

6

Власна реалізація алгоритму детекції

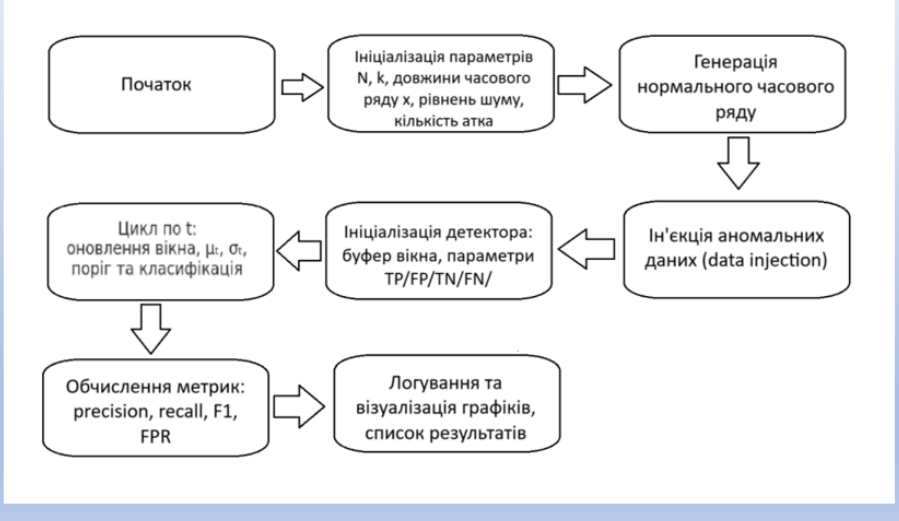


Рис. 3.1 Блок-схема роботи програмної симуляції аглоритму

7

Складові алгоритму виявлення

Вхід:

- часовий ряд x_t;
- ковзне вікно розміру N;
- Коефіцієнт чутливості k;

Поріг:

$T_t = \mu_t \pm k \cdot \sigma_t$;

Перевірка:

- якщо $x_t \in [T_t^-, T_t^+]$ => аномалія
- інакше => норма

Вихід:

послідовність міток «норма/атака»

8

```python
np.random.seed()  # нова симуляція при кожному запуску

data_length = 600
baseline = 10
noise_level = 0.5

# нормальні дані
normal_data = baseline + np.random.normal(0, noise_level, data_length)

# копія з ін'єкціями атаки
data = normal_data.copy()

# випадкові позиції атак
attack_positions = np.random.choice(range(100, 500), size=5, replace=False)
for pos in attack_positions:
    data[pos] += np.random.uniform(5, 12)  # spike-атаки

# ground truth
ground_truth = np.zeros(data_length)
ground_truth[attack_positions] = 1
```

Рис. 3.2 Перший та другий етап симуляції

```python
window_size = 20
k = 3  # чутливість порога

mu_list = []
sigma_list = []
anomaly = np.zeros(data_length)

for t in range(data_length):

    if t < window_size:
        mu_list.append(0)
        sigma_list.append(0)
        continue

    window = data[t - window_size:t]
    mu = np.mean(window)
    sigma = np.std(window)

    mu_list.append(mu)
    sigma_list.append(sigma)

    upper = mu + k * sigma
    lower = mu - k * sigma

    if data[t] > upper or data[t] < lower:
        anomaly[t] = 1
```

Рис. 3.3 Третій та четвертий етап симуляції


```python
TP = np.sum((anomaly == 1) & (ground_truth == 1))
FP = np.sum((anomaly == 1) & (ground_truth == 0))
TN = np.sum((anomaly == 0) & (ground_truth == 0))
FN = np.sum((anomaly == 0) & (ground_truth == 1))

precision = TP / (TP + FP + 1e-9)
recall = TP / (TP + FN + 1e-9)
f1 = 2 * precision * recall / (precision + recall + 1e-9)

print("\n--- РЕЗУЛЬТАТИ ---")
print("TP:", TP)
print("FP:", FP)
print("TN:", TN)
print("FN:", FN)
print(f"Precision: {precision:.3f}")
print(f"Recall:    {recall:.3f}")
print(f"F1-score:  {f1:.3f}")
```

Рис. 3.4 П’ятий етап симуляції

```python
plt.figure(figsize=(14, 6))
plt.plot(data, label="Дані сенсора", linewidth=1)

# істинні атаки
plt.scatter(attack_positions, data[attack_positions],
            color="red", s=80, label="Атаки (ground truth)", zorder=6)

# виявлені аномалії (зміщення +0.15)
plt.scatter(np.where(anomaly == 1), data[anomaly == 1] + 0.15,
            color="orange", s=60, label="Виявлені аномалії", zorder=7)

# ковзне середнє
plt.plot(mu_list, linestyle="--", color="tab:orange", label="Ковзне середнє", linewidth=1.5)

plt.title("Симуляція атаки та її виявлення", fontsize=14)
plt.xlabel("Часовий індекс")
plt.ylabel("Значення вимірювання")
plt.grid(True)
plt.legend()
plt.tight_layout()
plt.show()
```

Рис. 3.5 Шостий етап симуляції

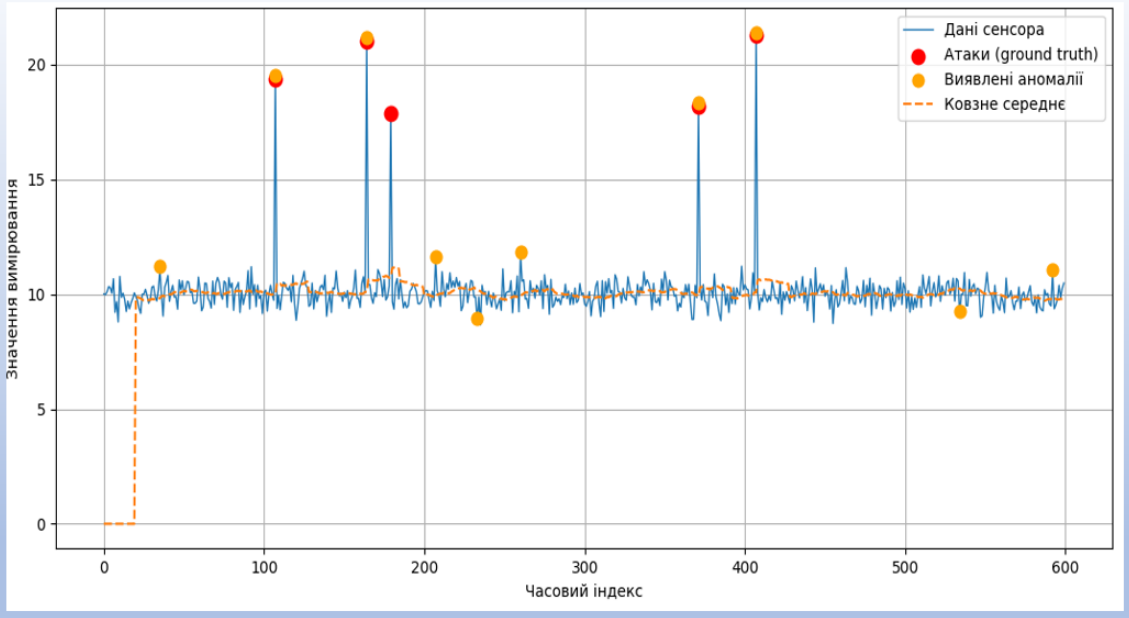


Рис. 3.8 Графік залежності F1-score від k при різних розмірах ковзного вікна N


```
PS C:\Users\Acorn\Desktop\sim> python main.py

--- РЕЗУЛЬТАТИ ---
TP: 5
FP: 2
TN: 593
FN: 0
Precision: 0.714
Recall:    1.000
F1-score:  0.833
PS C:\Users\Acorn\Desktop\sim>
```

Рис. 3.6 Текстовий вивід значень основних метрик

№	Розмір вікна N	Коефіцієнт чутливості k	TP	FP	TN	FN	Precision	Recall	F1score	FPR
8	10	3.0	4	17	578	0	0.227	1.0	0.37	0.029
9		3.5	4	8	580	1	0.333	0.8	0.471	0.013
10			4	5	577	1	0.444	0.8	0.571	0.008
11			5	8	578	0	0.385	1.0	0.556	0.013
12			5	9	587	0	0.357	1.0	0.526	0.015
13		4.0	4	4	591	1	0.5	0.8	0.615	0.007
14			4	2	593	1	0.667	0.8	0.727	0.003
15			5	5	590	0	0.5	1.0	0.667	0.008
16			5	4	591	0	0.556	1.0	0.714	0.007

Частина таблиці 3.1. Метрики алгоритму детекції для різних параметрів N і k

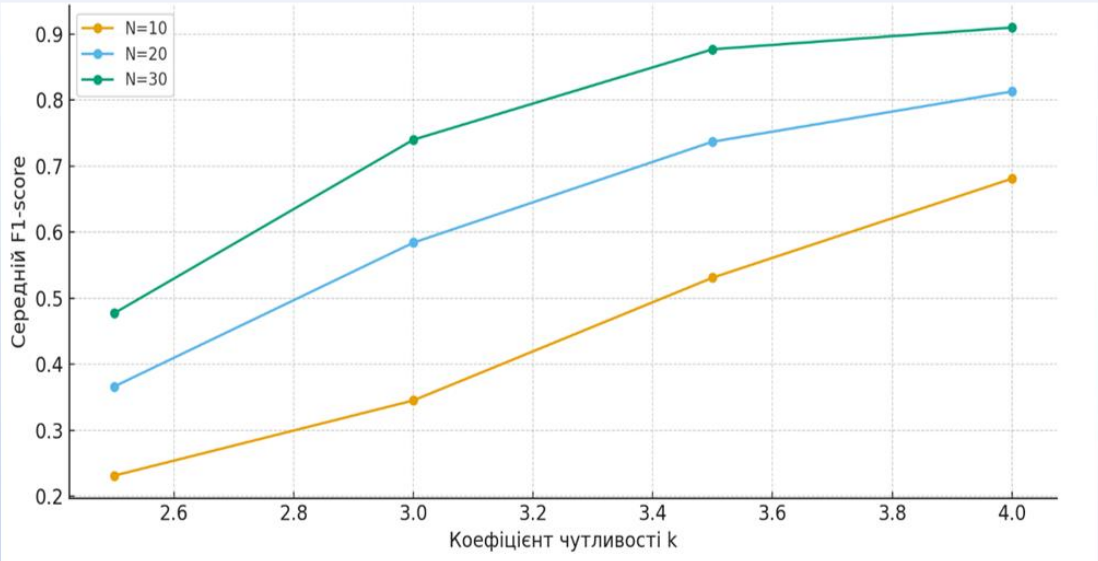


Рис. 3.8 Графік залежності F1-score від k при різних розмірах ковзного вікна N

13

Результати симуляції

Оптимальні параметри: N = 30, k=3.5-4.0

Алгоритм ефективний для виявлення сплескових інжекцій.

Є "легковаговим" (низька обчислювальна складність), що ідеально для БСМ.

Рекомендовано для інтеграції на рівні сенсорних вузлів або шлюзів.

15

Висновки

- Проаналізовано архітектуру та загрози БСМ, обґрунтовано актуальність виявлення атак типу data injection.
- Запропоновано й реалізовано в Python алгоритм детекції на основі ковзного вікна та порога $\mu_t \pm k \cdot \sigma_t$.
- Експериментально досліджено вплив параметрів алгоритму на точність виявлення атак та визначено область оптимальних налаштувань.

16

Дякую за увагу!

17