Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Система виявлення вторгнень у бездротових сенсорних мережах

(тема)

Виконав:
студент II курсу, групи КСМм-19-1
Попазов А.К.
(прізвище, ініціали)

Спеціальність
123 – Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп'ютерні системи та мережі
(повна назва освітньої програми)

Керівник: проф. Горбачов В.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 – Комп'ютерна інженерія
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Попазову Андрію Костянтиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система виявлення вторгнень у бездротових сенсорних мережах

затверджена наказом по університету від " 30 " жовтня 2020 р. № 1487 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 14 грудня 2020 р.

3. Вхідні дані до роботи

Бездротова мережа датчиків;

Виявлення вторгнень у бездротові сенсорні мережі.

IEEE 802.15.4 бездротові персональні мережі (LR-WPAN);

Система моделювання Opnet 14.5.

4. Перелік питань, що потрібно опрацювати в роботі

Бездротові сенсорні мережі;

Моделі загроз

Системи виявлення вторгнень;

Моделювання та аналіз

Бездротові сенсорні мережі;

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 13 арк. ф. А4

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз завдання	12.11.2020-16.11.2020	
2	Аналіз науково-технічної літератури	17.11.2020-23.11.2020	
3	Пошук моделі загроз системи	24.11.2020-28.11.2020	
4	Пошук аналітичних моделей комп'ютерних	29.11.2020-07.12.2020	
	систем та мереж		
5	Вивчення концепції імітаційного моделювання	08.12.2020-15.12.2020	
6	Визначення вторгнень	16.12.2020-20.12.2020	
7	Оформлення пояснювальної записки	08.12.2020-11.12.2020	
8	Оформлення графічної частини	08.12.2020-11.12.2020	
9	Представлення магістерської роботи	12.12.2020-13.12.2020	
	науковому керівнику		

Дата видачі завдання 3 листопада 2020 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Горбачов В.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 106 с., 34 рис., 2 дод., 34 джерела.

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, БЕЗДРОТОВА МЕРЕЖА ДАТЧИКІВ, OPNET, ЗАКЛИНЮВАННЯ, ВИБІРКОВА ПЕРЕАДРЕСАЦІЯ.

У цій роботі досліджується декілька атак та вразливостей мережі бездротових сенсорних мереж щодо схем управління топологією та оцінюємо їх ефективність у ворожих середовищах. Ми пропонуємо нову розподілену систему виявлення вторгнень (DIDS), яка включає кластерну топологію, що базується на правилах, що стосується бездротових сенсорних мереж (WSN), щоб визначити їх ефективність захисту в середовищах, специфічних для додатків. Наш DIDS робить висновки про вторгнення, порівнюючи аномальні шаблони зі слідів пакетів потужностей передачі та прийому сигналу, співвідношення швидкості надходження пакетів та аномалії в порогах потужності пакетів радіоприймача, використовуючи кількість вікон буфера. Підхід моделюється за допомогою симулятора OPNET. Результати моделювання показують, що можливості виявлення нашої схеми в умовах атаки відмови в обслуговуванні (DoS) (перешкода) збільшують частоту помилок в бітах, збільшують реакції затримки передачі та значне зменшення як потужності сигналу на шум, так і середньої пропускної здатності мережі до присутності атак глушителя, що є базовим для нашого аналізу, необхідного для підтримання енергоефективності та покращення безпеки в спеціальній мережі.

ABSTRACT

Master’s thesis: 106 pages, 34 figures, 2 appendices, 34 sources.

INTRUSION DETECTION SYSTEM, WIRELESS SENSOR NETWORK, OPNET, JAMMING, SELECTIVE FORWARDING.

In this thesis, we investigate few wireless sensor network security attacks and vulnerabilities relative to topology control schemes and evaluate their performance under hostile environments. We propose a novel Distributed Intrusion Detection System (DIDS) that incorporates rule based cluster topology relevant to Wireless sensor networks (WSNs) to determine their security performance in application specific environments. Our DIDS draws inferences of intrusion by comparing anomalous patterns from packet traces of transmit and receive signal powers, ratio of packet arrival rates and anomaly in radio receiver packet power thresholds using buffer window count. Our approach is simulated using the OPNET simulator. Simulation results show that the detection capabilities of our scheme under a denial of service (DoS) (jammer) attack, increases the bit error rates, increase in transmit delay responses and considerable decrease in both the signal to noise powers and the average network throughput due to the presence of jammer attack which forms the baseline for our analysis required to maintain energy efficiency and improve security in ad hoc network.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

WSN – Wireless Senosr Network (бездротова сенсорна мережа)

ВСТУП

Бездротова мережа датчиків (WSN) – це широко розподілена мережа з обмеженими ресурсами та бездротовими пристроями, що називається сенсорними вузлами. Кожен вузол датчиків контролює певне фізичне явище (наприклад, вологість, температуру, тиск, світло) всередині області дії. Зібрані вимірювання відправляються на базову станцію. Діапазон зв'язку сенсорних вузлів обмежений десятками метрів, отже, не всі вони можуть безпосередньо спілкуватися з базовою станцією. Тому дані надсилаються частинами від одного вузла датчика до іншого, поки вони не досягнуть базової станції.

Безпека стає важливою проблемою для WSN та приносить нові проблеми інженерам безпеки. Криптографічні методи можуть бути використані, щоб запобігти підслуховуванню зовнішнього зловмисника або зміни поточного зв'язку. Зона дислокації зазвичай не захищена фізично, і зловмисник може легко отримати доступ до області та захопити деякі вузли. Оскільки вони не стійкі до несанкціонованого доступу, зловмисник може модифікувати програмне забезпечення, що працює на вузлах, для запуску різноманітних внутрішніх атак. У цій дисертації розглянуто заїдання, hello flood, кротовину, вибіркову переадресацію, sinkhole, Sybil, виготовлення інформації та атаки зміною пакетів. Передбачається, що кількість захоплених вузлів значно менша, ніж загальна кількість сенсорних вузлів у мережі. Однак шкода, завдана внутрішніми атаками, може бути значною.

Системи виявлення вторгнень (IDSs) є належними механізмами захисту від внутрішніх атак і широко застосовуються у звичайних мережах. Однак ці IDS не можуть бути безпосередньо застосовані до WSN, в основному через сильні обмеження вузлів датчиків на енергію, пам'ять та обчислювальну потужність. Досить мати кілька зондів у звичайних мережах, якщо вони розміщені в точках концентрації руху. У WSN деякі напади можуть

спостерігати лише сусіди шкідливих вузлів. Отже, передбачається, що кожен вузол датчика запускає агент IDS і стежить за сусідами в безладному режимі. Зібрані дані, на нашу думку, повинні бути проаналізовані локально сенсорним вузлом або у співпраці лише з вузлами з близького сусідства, оскільки комунікаційна діяльність вимагає великих витрат енергії.

1 АКТУАЛЬНІСТЬ ПРОБЛЕМИ

1.1 Мотивація

Бездротова мережа - це розвиваюча технологія, яка набуває широкого визнання та популярності в комерційному секторі внаслідок стандартизованих протоколів та специфікацій. Потенціал технології бездротового зв'язку не був оминутий увагою у багатьох програмах, де важлива надійна комунікація. У таких програмах аспекти безпеки такі ж важливі, як продуктивність та низьке споживання енергії. Однак безпека все ще знаходиться на початковій стадії розвитку і є привабливою для дослідників. Було розроблено багато протоколів, однак обмеження ресурсів WSN робить пряме застосування цих рішень непридатним.

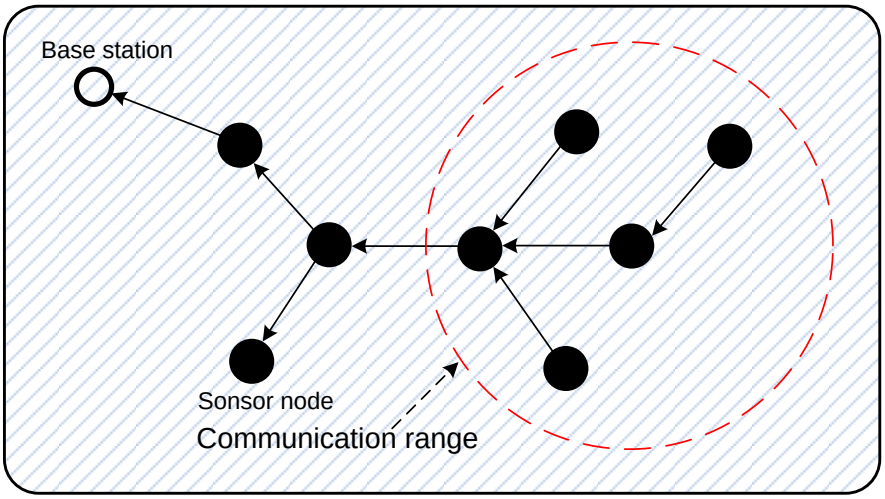


Рисунок 1.1 – Бездротова мережа датчиків

Протягом останніх років для сенсорних мереж було впроваджено декілька методів запобігання вторгнень [1]. Такі заходи профілактики, як шифрування та автентифікація, можуть використовуватися для зменшення

вторгнень, але не можуть їх усунути. Наприклад, шифрування та аутентифікація не можуть захищати від порушених сенсорних вузлів, які несуть приватні ключі. З досвіду досліджень безпеки, незалежно від того, скільки повідомлень про запобігання вторгнень вставлено в мережу, завжди є слабкі зв'язки, які можна було б використати для прориву. Таким чином, супротивник залишиться непоміченим, і це, ймовірно, призведе до збоїв у роботі нормальної роботи мережі, як зазначено на рисунку 1.2а.

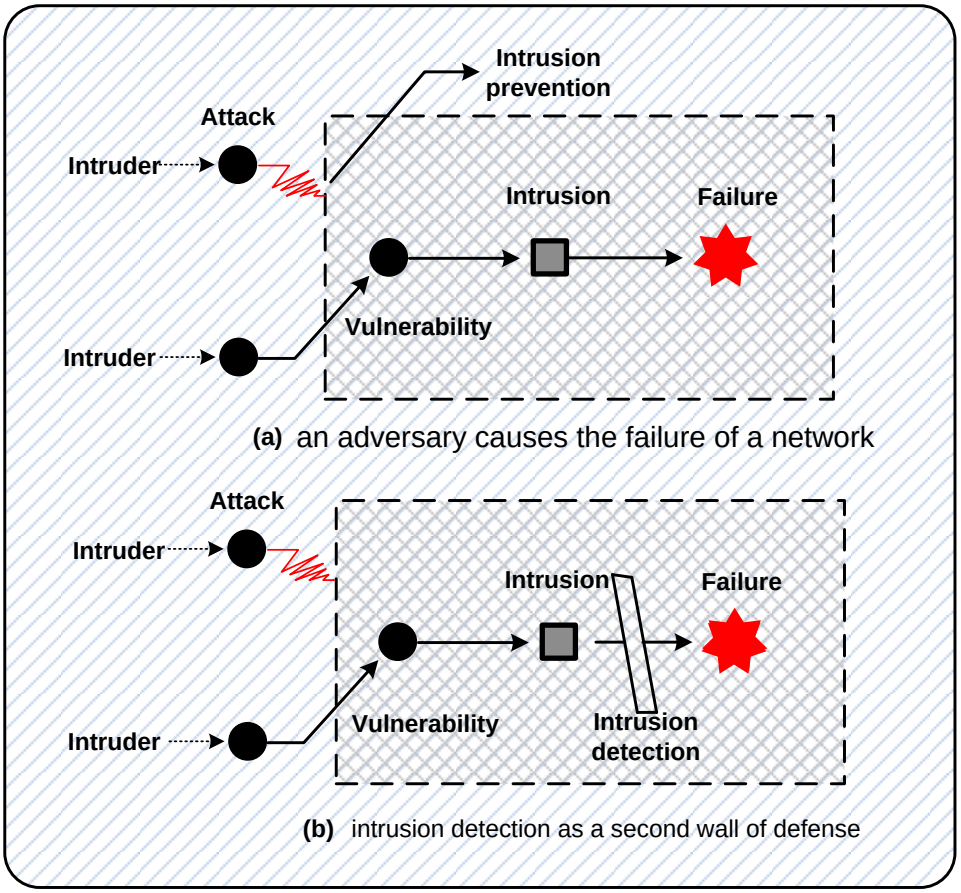


Рисунок 1.2 – Послідовність вторгнення

Для по-справжньому безпечних сенсорних мереж нам також потрібна друга лінія захисту: система виявлення вторгнень, яка може виявити третю сторону, яка намагається використовувати безпеку мережі, навіть якщо ця атака раніше не визначена. Якщо зловмисник виявиться досить швидко, ми

можемо вжити будь-які відповідні заходи до того, як буде завдана шкода або порушено будь-які дані (рисунок 1.2б). Таким чином, виявлення вторгнення представляє собою другу стіну захисту, і це необхідність у мережі високої живучості.

1.2 Здобутки роботи

У цій роботі ми запропонували механізм DIDS для виявлення аномалій вторгнення за наявності атаки заїдання в бездротовій сенсорній мережі. Запропонований DIDS використовує алгоритм для створення голови кластера, IDS встановлюється у кожному вузлі головки кластера, який служить вузлом монітора або шлюзу. Внутрішні вузли також служать точками доступу для взаємодії та розповсюдження оновлень маршрутів, контролюючи схожість у випадку загальних та підозрюваних збоїв проти будь-якої форми вторгнення.

Запропонований нами DIDs виявив ознаки аномалії вторгнення у спеціальній мережі через зміни в:

- Назви шаблонів внаслідок атаки видають себе,
- Потужності прийому пакетів,
- Таблиці між приходом пакетів вузлів,
- Мережі та розмірах пакетів за допомогою співвідношення вікна буфера пакетів.
- Передачі та прийняття сигналу повноважень як джамер-пакетів, так і законних вузлів.

1.3 Огляд існуючих WSN

Проведено багато досліджень у галузі виявлення вторгнень для бездротових спеціальних мереж. У своєму початковому дослідженні Жан та Лі [2] запропонували розподілені та спільні IDS на основі методів

статистичного виявлення аномалії, які використовують інформацію з усіх рівнів протоколів зв'язку та локальних для кожного вузла.

Однак виявлення вторгнень, характерних для WSN, є здебільшого невивченою областю. Є багато проблем, які роблять цю область цікавою. Перш за все важливо зауважити, що не кожен вузол може мати повний IDS-агент, пов'язаний з ним, через апаратні обмеження.

Інші міркування включають: справедливий розподіл завдання виявлення між вузлами мережі, вибір функцій, які не залежать від використовуваного протоколу маршрутизації, та своєчасного поширення сигналів тривоги від вузлів датчика до базової станції. Отже, схема виявлення вторгнень повинна бути здатна розпізнавати небачені атаки, створюючи при цьому мінімальну кількість помилкових сигналів тривоги. Далі - короткий підсумок деяких робіт, які були зроблені в спробі вирішити вищезазначені проблеми:

Loo та ін. [3] представили схему виявлення вторгнень для сенсорних мереж на основі виявлення аномалії. Зокрема, вони використовують алгоритм кластеризації з фіксованою шириною, щоб забезпечити виявлення раніше небачених атак. Вони також запропонували 12 загальних особливостей для виявлення раковин і періодичних атак помилок на маршруті на основі протоколу AODV [4], що не є чистим протоколом маршрутизації WSN. Однак запропонована ними схема виявлення не вимагає зв'язку між вузлами, отже зменшує енергію, необхідну для роботи. Вони досягають до 100% точності для активних атак на раковину. У цьому дослідженні ми також слідуємо за шляхом виявлення аномалії.

Алгоритм на основі правил був запропонований в [5] для виявлення аномалій у WSNS. Вузли моніторів перевірять трафік своїх сусідів і порівнюють із деякими заздалегідь визначеними правилами. Якщо правило не виконується, виникає збій. Повідомляється про аномалію, якщо кількість відмов перевищує очікуване значення, яке динамічно обчислюється вузлом монітора. Однак деякі правила непрості у здійсненні та витрачають ресурси.

Більш важливо, що ефективність та точність виявлення залежать від розміру буфера, який суворо обмежений у WSNS.

2 БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ

Бездротова мережа датчиків - це спеціальна мережа, що складається з великої кількості невеликих недорогих пристроїв, позначених як вузли (моти). Ці вузли - пристрої, що працюють на батареях, здатні спілкуватися між собою, не покладаючись на будь-яку фіксовану інфраструктуру.

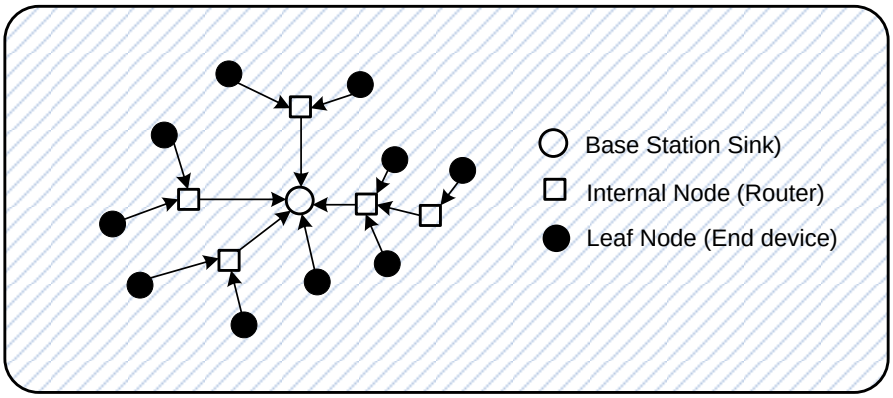


Рисунок 2.1 – Бездротові сенсорні мережі

Типовий WSN (рисунок 2.1) складається з базової станції та вузлів, які сприймають середовище та передають дані на базову станцію. Базова станція (також позначається як раковина або шлюз) є більш потужною, ніж інші вузли і служить інтерфейсом для зовнішнього світу. Коли будь-якому вузлу необхідно надіслати повідомлення на базову станцію, яка знаходиться поза його радіодіапазоном, він надсилає його через внутрішні вузли. Внутрішні вузли такі ж, як і інші, але крім місцевого зв‘язку вони також надають змогу переадресації для інших.

Типовий бездротовий сенсорний вузол оснащений одним або декількома датчиками, здатними контролювати фізичні або екологічні умови, такі як температура, вологість, тиск, вібрації або інтенсивність світла. Крім того, кожен вузол оснащений радіопередавачем, енергоефективним

мікроконтролером та джерелом енергії, як правило, акумулятором. Через енергетичні обмеження, вузли здатні лише до обмеженої кількості обчислень та обробки сигналів.

У порівнянні зі звичайним підходом, який використовує кілька дорогих і складних датчиків, WSN здійснює мережеви зв‘язок, використовуючи велику кількість відносно непрофілізованих і дешевих датчиків. Ми можемо узагальнити переваги підходу WSN як більше охоплення, точність та надійність при можливо меншій вартості [6].

Як тільки люди зрозуміють можливості бездротової сенсорної мережі, сотні прикладних програм стануть можливими. Це здається прямим поєднанням сучасних технологій.

Однак фактично поєднання датчиків, радіостанцій та процесора в ефективну бездротову сенсорну мережу вимагає детального розуміння як можливостей, так і обмежень кожного з основних апаратних компонентів, а також детального розуміння сучасних мережевих технологій та теорії розподілених систем. Кожен окремий вузол повинен бути розроблений таким чином, щоб забезпечити набір примітивів, необхідних для синтезу взаємопов’язаного полотна, яке з’явиться під час їх розгортання, дотримуючись суворих вимог щодо розміру, вартості та енергоспоживання. Основним завданням є зіставлення загальних системних вимог до можливостей та дій окремих пристроїв.

2.1 Застосування WSN

WSN – це сукупність компактних розмірів, відносно недорогі обчислювальні вузли, які вимірюють місцеві умови навколишнього середовища або інші параметри та передають таку інформацію в центральну точку для відповідної обробки. Вузли WSN можуть сприймати оточення, можуть спілкуватися із сусідніми вузлами і, у багатьох випадках, можуть виконувати основні обчислення даних, що збираються.

WSN підтримують широкий спектр корисних програм, включаючи безпеку та спостереження, контроль, спрацьовування та обслуговування складних систем та точний моніторинг внутрішніх та зовнішніх середовищ. Деякі приклади цих додатків пояснюються нижче:

- Військові програми: бездротові сенсорні мережі можуть бути невід'ємною частиною військових систем управління, управління, зв'язку, комп'ютерів, систем розвідки, спостереження, розвідки та націлювання. Швидке розгортання, самоорганізація та відмовні характеристики сенсорних мереж роблять їх дуже перспективною технікою зв‘язку для військових. Оскільки сенсорні мережі ґрунтуються на щільному розгортанні одноразових і недорогих сенсорних вузлів, руйнування деяких вузлів ворожими діями не впливає так само на військову операцію, як на знищення традиційного датчика. Деякі з військових застосувань - це спостереження за силою, спостереження за боєм, розвідка, прицілювання, оцінка ураження боїв та хімічне, біологічне, радіологічне та ядерне виявлення.

- Екологічні програми: деякі екологічні програми сенсорних мереж включають стеження за переміщенням видів, тобто моніторинг середовища проживання, моніторинг умов навколишнього середовища, які впливають на сільськогосподарські культури та худобу, зрошення, макроінструменти для широкомасштабного моніторингу Землі та вивчення планети і хіміко-біологічне виявлення.

- Комерційні програми: існує багато потенційних та нових комерційних програм WSN, таких як управління запасами, моніторинг якості продукції, розумні офіси, моніторинг пацієнтів та людей похилого віку, моніторинг стан матеріалів та контроль навколишнього середовища в офісних будівлях. Існує також кілька футуристичних WSN-застосувань, таких як послуги з медичних імплантацій, де численні датчики та виконавчі механізми імплантуються в організм людини для різних цілей, таких як постійний моніторинг, створення штучної імунної системи та стимуляція паралізованих м’язів.

2.2 Проблеми, пов'язані з WSN

WSN багато в чому відрізняються від звичайних мережевих систем. Зазвичай вони включають велику кількість просторово розподілених, обмежених енергією, самоконфігуруючих і самосвідомих вузлів. Крім того, вони, як правило, автономні і вимагають високого ступеня взаємодії та адаптації для виконання бажаних скоординованих завдань та функцій мереж. Таким чином, вони створюють нові проблеми на додаток до тих, які впроваджуються звичайними бездротовими мережами.

2.2.1 Зміни топології

Вузли можуть статично розміщуватися в деяких WSN. Однак поломка пристрою є звичайною подією через виснаження енергії. Можливо також наявність сенсорних мереж з високомобільними вузлами. Крім того, вузли та досвід роботи мережі відрізняються в динаміці завдань, і вони можуть бути цілями для навмисного заїдання. Тому топологія сенсорної мережі може бути схильні до більш частих змін, ніж звичайні спеціальні мережі.

2.2.2 Допуски до відмов

Сенсорні мережі повинні мати можливість підтримувати свої функції без будь-яких перерв через збої вузла. Протоколи та алгоритми можуть бути розроблені для задоволення рівня відмовостійкості, необхідної для сенсорних мережних додатків. Вимоги додатків зазвичай відрізняються одна від одної. Наприклад, вимоги до відмов у тактичній мережі датчиків можуть вважатися набагато вищими, ніж вимоги для домашнього додатка, оскільки вузли схильні до більш високих показників у тактичних сенсорних мережах, а вплив несправності сенсорної мережі в тактичному полі може бути набагато важливішим, ніж вплив відмови мережі домашнього датчика. Відмінності в

потребах різних застосувань сенсорних мереж можна спостерігати майже для кожного фактора, що впливає на розробку сенсорних мереж. Більше того, компроміси зазвичай потрібні серед цих факторів, оскільки існують суворі обмеження, пов'язані з ними. Тому один розмір, який відповідає всім загальним конструкціям, неможливий для багатьох завдань в сенсорних мережах. Як правило, для виконання вимог різних застосувань потрібні різні схеми.

2.2.3 Масштабованість

Кількість вузлів, розгорнутих у сенсорному полі, може досягати мільйонів у деяких програмах. Більше того, щільність вузла може досягати 20 вузлів на м3 в деяких додатках. Усі схеми, розроблені для сенсорних мереж, повинні бути достатньо масштабованими, щоб справлятися з щільністю та номерами вузлів, які за порядком величин вищі за всі інші типи мережі.

2.3 Апаратне забезпечення WSN

Вузол складається з чотирьох основних компонентів: датчики, процесор, блок приймання та блок живлення. Вони також можуть мати додаткові компоненти, що залежать від застосування, такі як система пошуку місцезнаходження, генератор електроенергії.

Одиниці чутливості зазвичай складаються з двох субодиниць: датчиків та аналого-цифрових перетворювачів (ADCs). Аналогові сигнали, що виробляються датчиками на основі спостережуваного явища або подразників, перетворюються в цифрові сигнали ADC і потім подаються в блок обробки. Зауважте, що вузол може бути приєднаний до декількох датчиків. Наприклад, датчик температури і вологості може бути приєднаний до одного і того ж вузла.

Блок обробки, який, як правило, пов'язаний з невеликим блоком зберігання даних, як показано на малюнку 2.2 нижче, управляє процедурами, які змушують вузол співпрацювати з іншими вузлами для виконання призначених завдань з‘язку.

Приймач з'єднує вузол з мережею. Одним з найважливіших компонентів вузла є блок живлення.

Блоки живлення можуть підтримуватися за допомогою енергозберігаючих інструментів, таких як сонячні батареї. Існують також інші субодиниці, які залежать від програми. Більшість методів маршрутизації сенсорних мереж та завдань з‘язку вимагають знання місця з високим ступенем точності. Таким чином, для вузла прийнято мати систему пошуку місцезнаходження.

Іноді може знадобитися мобілізація для переміщення вузлів, коли це потрібно для виконання покладених завдань. Усі ці субодиниці, можливо, знадобляться для модуля розміром з сірникової коробки. Необхідний розмір буде навіть меншим за кубічний сантиметр у деяких програмах.

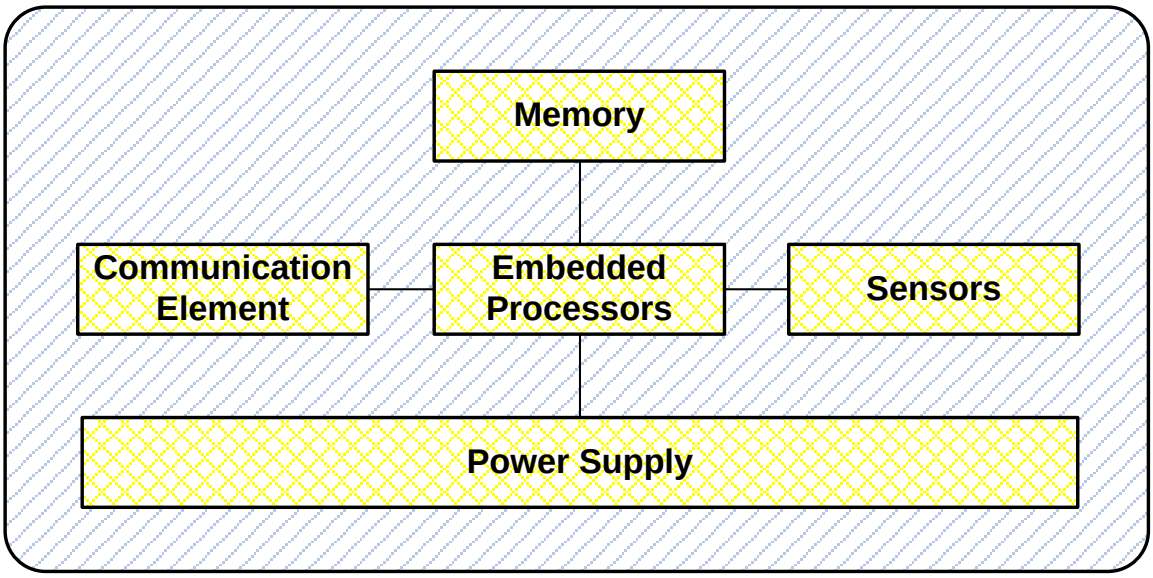


Рисунок 2.2 – Апаратний елемент бездротового сенсорного вузла

2.4 Вимоги до WSN

Зважаючи на характеристики та обмеження WSN, вимоги щодо побудови додатків у цих мережах наведені нижче [7].

- Бездротовий зв'язок: при використанні проміжних вузлів зв'язок на великі відстані може зменшити енергію, необхідну для передачі пакетів. Цей механізм є елементарним для багатьох застосувань.

- Енергоефективність: термін експлуатації вузла визначається терміном служби акумулятора; тим самим він вимагає мінімальних витрат енергії.

- Ефективне використання малої пам’яті: необхідно враховувати відповідні структури даних, щоб вмістити невеликий об'єм пам'яті у вузлах датчика.

- Агрегація даних: величезна кількість чутливих вузлів може переповнювати мережу інформацією. Щоб вирішити цю проблему, деякі датчики можуть агрегувати дані, зробити деякі обчислення, а потім транслювати узагальнену нову інформацію.

- Мережева самоорганізація: враховуючи велику кількість вузлів та їх потенційне розміщення у ворожих місцях, важливо, щоб мережа могла самоорганізовуватися. Більше того, вузли можуть вийти з ладу (або через брак енергії, або через фізичне знищення), і нові вузли може знадобитися приєднати до мережі. Тому мережа повинна мати можливість періодично перенастроюватися, щоб вона могла продовжувати функціонувати. Окремі вузли можуть бути відключені від решти мережі, але високий ступінь підключення повинен підтримуватися.

- Спільне прийняття рішень: однією з цілей WSN є виявлення / оцінка деяких подій, а не лише спілкування. Для підвищення продуктивності вияється часто буває досить корисним датчик взаємодії один з одним, щоб вийти в загальний стан. Це може затримати передачі повідомлень управління та даних.

2.5 Проблеми безпеки в WSN

Захист іноді розглядається як окремий компонент архітектури системи, де окремий модуль забезпечує безпеку. Однак це розмежування є хибним підходом до безпеки мережі. Для досягнення захищеної системи безпеку необхідно інтегрувати в кожен компонент, оскільки компоненти, розроблені без захисту, можуть стати точкою нападу. У будь-якому випадку потреба в безпеці в сенсорних додатках очевидна. WSN ідеально підходять для виявлення хімічних, біологічних чи екологічних загроз на великих територіях, однак зловмисні сигнали, що викликаються, можуть повністю знищити значення системи. Якщо захист слабкий, сенсорні мережі будуть придатні лише для обмежених, керованих середовищ, що значно не відповідають їхнім потребам. Широке розповсюдження та загальний успіх сенсорних мереж буде безпосередньо пов’язано з їхньою безпекою.

У розділах нижче ми опишемо деякі проблеми безпеки у WSN та необхідні вимоги для сенсорної мережі.

2.5.1 Виклики щодо безпеки в WSN

Мережевий характер великих, спеціальних, бездротових сенсорних мереж створює нові загрози та значні проблеми при розробці схем безпеки. Сенсорні мережі дозволяють збирати дані, координувати аналіз та автоматизоване співвідношення подій. Таким чином, вони вразливі до атак безпеки через багато причин, таких як характер трансляції носія. Крім того, сенсорні вузли часто поміщаються у вороже або небезпечне середовище, де вони фізично не захищені. Нижче ми представимо п'ять відомих проблем у бездротових сенсорних мережах [8].

2.5.2 Бездротовий носій

Поширені програми, запропоновані для сенсорних мереж, потребують бездротового зв'язку. Крім того, спеціальне розгортання сенсорних мотивів робить провідне спілкування абсолютно недоцільним. Бездротовий носій по суті є менш захищеним, оскільки його характер трансляції робить підслуховування простим. Будь-яка передача може легко перехоплюватися, змінюватися або відтворюватися противником. Бездротовий носій дозволяє зловмиснику легко перехоплювати дійсні пакети та легко вводити шкідливі. Хоча ця проблема не характерна лише для сенсорних мереж, традиційні рішення повинні бути адаптовані для ефективного виконання в сенсорних мережах.

2.5.3 Спеціальне розгортання

Спеціальний характер сенсорних мереж означає, що жодна структура не може бути заздалегідь статично визначена. Топологія мережі завжди піддається змінам через збій вузла, додавання або мобільність. Вузли можуть розгортатися повітрям, тому нічого невідомо про топологію розгортання. Оскільки вузли можуть виходити з ладу або замінюватися, мережа повинна підтримувати самоконфігурацію. Схеми безпеки повинні мати можливість працювати в цьому динамічному середовищі. Постійно мінливий характер сенсорних мереж вимагає більш надійних конструкцій для технік безпеки, щоб впоратися з такою динамікою.

2.5.4 Вороже середовище

Ще одним складним фактором є вороже середовище, в якому функціонують сенсорні вузли. Моти стикаються з можливістю знищення або (можливо, гірше) захоплення зловмисниками. Компроміс із вузлом

відбувається, коли зловмисник за допомогою деяких підривних засобів отримує контроль над вузлом в мережі після розгортання. Оскільки вузли можуть перебувати у ворожій обстановці, зловмисники можуть легко отримати фізичний доступ до пристроїв. Отримавши контроль над вузлом, зловмисник може змінити вузол для прослуховування інформації в мережі, введення шкідливих даних або здійснення різноманітних атак. Зловмисник також може розібрати вузол і витягти важливу для безпеки мережі інформацію, таку як протоколи маршрутизації, дані та криптографічні ключі. Як правило, компроміс відбувається, коли зловмисник знайшов вузол, а потім безпосередньо підключає вузол до свого комп'ютера за допомогою якогось дротового з'єднання. Після підключення зловмисник контролює вузол шляхом вилучення даних та / або розміщення нових даних або елементів управління на цьому вузлі. Підсумовуючи, дуже вороже середовище представляє серйозну проблему для дослідників безпеки.

2.5.5 Дефіцит ресурсів

Надзвичайні обмеження ресурсів сенсорних пристроїв створюють значні труднощі для механізмів захисту ресурсів. Представницьким прикладом сенсорного пристрою є мот Tmote Sky. Він має мікроконтролер 8 МГц TI MSP430 з 16-бітовим процесором RISC разом з 10 КБ оперативної пам’яті для даних. Радіо працює на пропускній здатності до 40 Кбіт / с на відстані в кілька десятків метрів. Такі обмеження обладнання вимагають надзвичайно ефективних алгоритмів захисту з точки зору пропускної здатності, складності обчислень та пам'яті. Це не тривіальне завдання. Хоча енергія є чи не найціннішим ресурсом для сенсорних мереж, попередні роботи приділяли мало уваги енергоефективності. Спілкування особливо дороге з точки зору потужності. Кожен переданий біт споживає стільки ж енергії, скільки виконує 800-1000 інструкцій. Очевидно, що механізми

безпеки повинні докладати особливих зусиль, щоб бути ефективними у спілкуванні і бути енергоефективними.

2.5.6 Величезна шкала

Отже, запропонована шкала сенсорних мереж створює значну проблему для механізмів безпеки. Сенсорні мережі популярні завдяки їх можливості розгортатися у великих районах з тисячами або мільйонами сенсорних вузлів. Просто мережеве з'єднання десятків до сотень тисяч вузлів виявилося важливим завданням. Забезпечення безпеки через таку мережу однаково складно. Механізми безпеки повинні бути масштабованими до дуже великих мереж, зберігаючи високу ефективність обчислень та зв'язку.

2.5.7 Вимоги безпеки

Безпека - це широко вживаний термін, що включає характеристики аутентифікації, цілісності, конфіденційності, невідхилення та відтворення. Що стосується сенсорної мережі, вимоги до безпеки (і, зрештою, поведінки), необхідні для досягнення захищеної мережі, обговорюються нижче [9]:

- Конфіденційність даних: конфіденційність означає збереження інформації в таємниці від сторонніх сторін. Сенсорна мережа не повинна просочувати показання датчика до сусідніх мереж. У багатьох програмах (наприклад, розподіл ключів) вузли передають високочутливі дані. Стандартний підхід до збереження конфіденційних даних у таємниці полягає в шифруванні даних секретним ключем, який мають лише призначені приймачі, завдяки чому досягається конфіденційність. Оскільки криптографія відкритого ключа є надто дорогою, щоб використовувати її в сенсорних мережах, обмежених ресурсами, більшість запропонованих протоколів використовують симетричні методи шифрування ключів. Однак, хоча шифрування захищає від зовнішніх атак, воно не захищає від

внутрішніх атак / компрометацій вузлів.

- Автентичність даних: у сенсорній мережі зловмисник може легко вводити повідомлення, тому приймач повинен переконатися, що дані, які використовуються в будь-якому процесі прийняття рішень, походять з правильного джерела. Аутентифікація даних не дозволяє стороннім сторонам брати участь у мережі, а законні вузли повинні мати можливість виявляти повідомлення від несанкціонованих вузлів та відхиляти їх. Однак аутентифікація сама по собі не вирішує проблему захоплення вузлів, оскільки компрометовані вузли все ще можуть автентифікувати себе в мережі. Отже, механізми аутентифікації повинні бути колективними та спрямовані на забезпечення всієї мережі. Використання методів виявлення вторгнень може допомогти знайти компрометовані вузли та розпочати відповідні процедури відкликання.

- Цілісність даних: цілісність даних гарантує одержувачеві, що отримані дані не змінюються противником під час транзиту. Зауважте, що аутентифікація даних також може забезпечувати цілісність даних.

- Свіжість даних: свіжість даних означає, що дані недавні, і це гарантує, що противник не повторив жодного старого повідомлення. Поширений захист полягає в тому, щоб включити порядкові номери у повідомлення та відхилити ті зі старими значеннями. У роботі [10] автори виділили два типи свіжості: слабку свіжість, яка забезпечує часткове впорядкування повідомлень, але несе інформацію про затримку, та сильну свіжість, яка забезпечує загальний порядок на пару відповідей на запит, та дозволяє оцінити затримку. Слабка свіжість необхідна вимірюванням датчиків, тоді як сильна свіжість корисна для синхронізації часу в мережі.

- Доступність: мережа датчиків повинна бути надійною проти різних атак безпеки, і якщо атака буде успішною, її вплив слід звести до мінімуму. Компроміс одного вузла не повинен порушувати безпеку всієї мережі. Все це обговорення говорить про те, що сенсорні мережі повинні демонструвати безперебійну роботу навіть у сценаріях атаки. Важливо, щоб їх

функціональність деградувала передбачувано та стабільно, незважаючи на наявність компромісів чи збоїв у вузлах.

2.6 Стандарт IEEE 802.15.4: LR-WPAN

Стандарт IEEE 802.15.4 [11] визначає характеристики фізичного та MAC-шарів для низькошвидкісних бездротових персональних мереж (LR-WPAN). Перевагами LR-WPAN є легка установка, надійна передача даних, короткий діапазон роботи, надзвичайно низька вартість, використання неліцензованих радіодіапазонів (діапазон ISM), гнучкі та розширювані мережі, інтегрована розвідка для налаштування мережі та маршрутизації повідомлень, а також розумний ресурс акумулятора, зберігаючи простий і гнучкий протокол.

2.6.1 Мережеві топології

Зіркова топологія: зоряна мережа має центральний вузол, який пов'язаний з усіма іншими вузлами в мережі. Усі повідомлення проходять через центральний вузол.

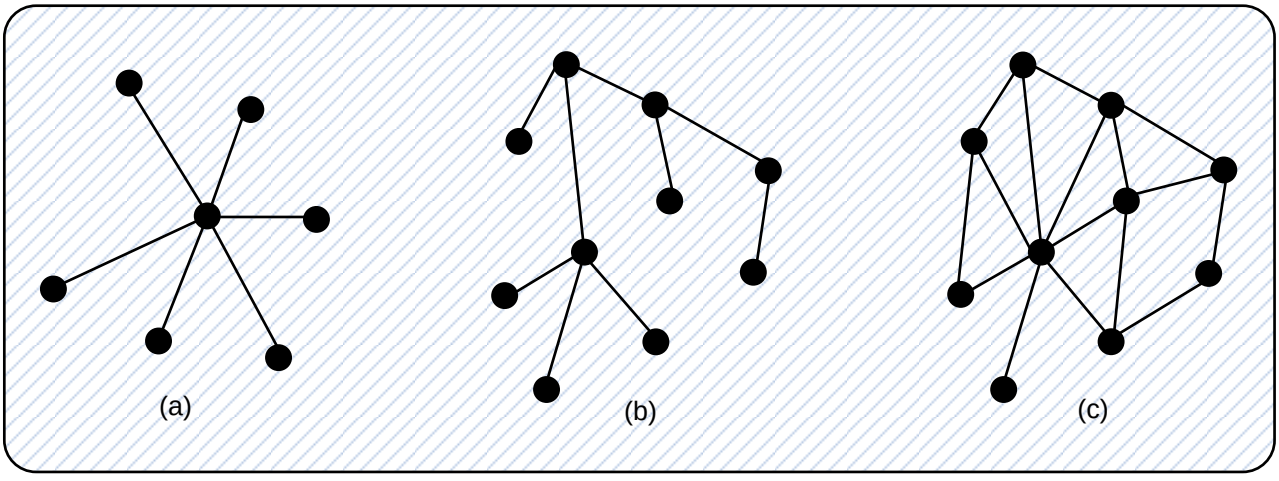


Рисунок 2.3 – Мережеві топології: (а) Зірка, (б) Дерево, (в) Сітка

Топологія дерева: мережа дерева має верхній вузол із структурою гілки / листя внизу. Щоб досягти місця призначення, повідомлення рухається вгору по дереву (наскільки це необхідно), а потім вниз по дереву.

Мережа топології: мережа має деревоподібну структуру, в якій деякі листя безпосередньо пов'язані. Повідомлення можуть подорожувати по дереву, коли є відповідний маршрут.

2.6.2 Фізичний рівень

Фізичний рівень бездротової бездротової персональної мережі складається з 27 каналів. Доступні канали розділені на три діапазони частот: діапазон 2450 МГц (з 16 каналами), діапазон 915 МГц (з 10 каналами) і діапазон 868 МГц (1 канал), всі вони використовують спектр прямого розповсюдження прямої послідовності (DSSS) режим доступу. Швидкість передачі даних дуже низька порівняно з іншими типами WPAN. Крім роботи радіо вмикання / вимкнення, фізичний рівень підтримує функціональні можливості для вибору каналу, оцінки якості зв'язку, вимірювання виявлення енергії та чіткої оцінки каналу для сприяння вибору каналу. Фізичний рівень забезпечує інтерфейс між підрівнем MAC та фізичним радіоканалом.

Фізичний рівень виконує такі завдання:

- Активація/деактивація радіопередавача: перетворення радіопередавач в один з трьох станів, тобто передачу отримання або вимкнення (сну) відповідно до запиту від підрівня MAC.

- Виявлення енергії (ED): це оцінка потужності прийнятого сигналу в межах пропускної здатності каналу. Результат від виявлення енергії може бути використаний мережевим рівнем як частина алгоритму вибору каналу або з метою чіткої оцінки каналу (CCA) (окремо або в поєднанні з носієм).

- Індикація якості зв'язку (LQI): вимірювання проводиться для кожного прийнятого пакету. Рівень PHY використовує детектор енергії приймача (ED), співвідношення сигнал / шум (SNR) або їх комбінацію для

вимірювання міцності та якості зв'язку, з якої приймається пакет.

- Вибір каналу: як обговорювалося вище, посилання бездротового зв’язку в діапазоні 802.15.4 можуть працювати в 27 різних каналах, але певна мережа може вибрати підтримку частини каналів. Отже, рівень PHY повинен бути в змозі налаштувати свій приймач у певний канал після отримання запиту від підрівня MAC.

- Чітка оцінка каналу (CCA) для багаторазового доступу оператора через чутливість до зіткнення (CSMA-CA): Рівень PHY необхідний для виконання CCA, використовуючи виявлення енергії, відчуття носія або комбінацію цих двох. У режимі сенсорного носія середовище вважається зайнятим, якщо виявлено сигнал із характеристиками модуляції та розповсюдження IEEE 802.15.4.

- Передача/прийом пакетів на фізичному носії: тут використовуються методи модуляції та розповсюдження.

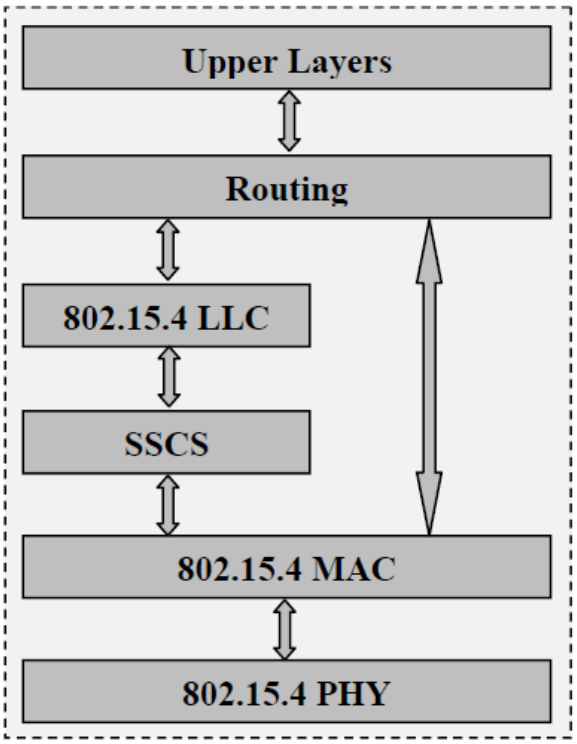


Рисунок 2.4 – Шаровий підхід IEEE 802.15.4

2.6.3 Підрівень MAC

Підрівень MAC забезпечує інтерфейс між конвергенцією специфічного підрівня для послуги (SSCS) та рівнем PHY, як показано на рисунку 2.4. Підрівень MAC забезпечує дві послуги, а саме службу передачі даних MAC та службу управління MAC. Він відповідає за наступні завдання:

- Створення та управління маяками: якщо пристрій є координатором, то координатор може визначити, чи працювати в режимі включеного маяка, в якому використовується супер кадрова структура.
- Асоціація та дисоціація з координаторами персональної зони (PAN): Для підтримки самоконфігурації 802.15.4 вбудовує функції асоціації та роз'єднання у свій підрівень MAC. Це не лише дозволяє автоматично налаштовувати зірку, але також дозволяє створити мережу, що самоконфігурується, однорангову.
- Доступ до каналу: використовуючи механізм багаторазового доступу оператора з уникненням зіткнень (CSMA-CA) для доступу до каналу. Як і більшість інших протоколів, призначених для бездротових мереж, 802.15.4 використовує механізм CSMA-CA для доступу до каналу. Однак новий стандарт не включає механізм запиту на надсилання (RTS) та чіткого механізму відправки (CTS), враховуючи низьку швидкість передачі даних, що використовується в LR-WPAN.
- Гарантоване управління тимчасовими слотами: обробка та підтримка механізму гарантованого часового інтервалу (GTS). Працюючи в режимі з включеним маяком, координатор може виділити частини активного суперкадру для пристрою. Ці частини називаються GTS і містять період вільного змісту (CFP) суперкадру.
- Перевірка кадру та підтвердження доставки: забезпечує різні механізми підвищення надійності зв’язку між двома одноранками, серед них: підтвердження та повторна передача кадру, перевірка даних за допомогою 16-бітної CRC, а також CSMA-CA.

2.6.4 Супер структура кадру

Суперкадр обмежений мережевими маячками і поділений на декілька слотів Super frame (значення за замовчуванням 16). Координатор періодично надсилає маячки для синхронізації приєднаних пристроїв та для інших цілей. Пристрій, приєднаний до координатора, що працює в режимі маяка, може відслідковувати маяки для синхронізації з координатором. Ця синхронізація важлива для опитування даних, енергозбереження та виявлення одиночок. Супер кадр ділиться на дві частини: неактивний та активний період. У неактивний період всі станції сплять, тоді як активний період буде розділений на 16 слотів. Ці слоти є слотами MACRO. Ці 16 слотів можна додатково розділити на дві частини: період доступу до конфлікту (CAP) та вільний період (CFP). CFP є необов'язковим і може містити до семи так званих гарантованих часових інтервалів (GTS), а GTS може займати більше одного періоду слотів. Однак достатня частина CAP залишається для доступу на основі суперечок інших мережевих пристроїв або нових пристроїв, які бажають приєднатися до мережі.

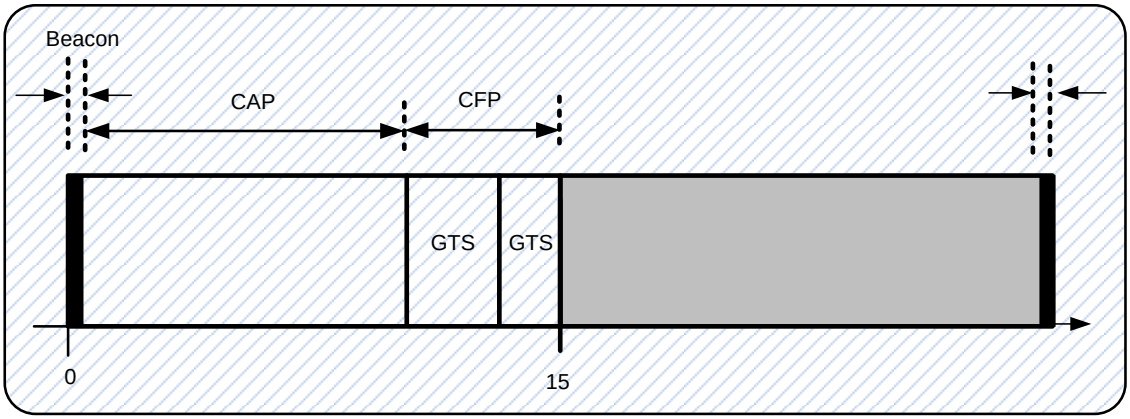


Рисунок 2.5 – Супер кадрова структура

Прорізний механізм CSMA-CA використовується для доступу до каналу під час CAP. Усі транзакції, що базуються на суперечках, повинні

бути завершені до початку CFP. Також усі транзакції з використанням GTS повинні бути здійснені до часу наступного GTS або до кінця CFP.

2.6.5 Багаторазовий доступ – запобігання зіткнення

CSMA-CA [12] дає рішення проблеми прихованого вузла в CSMA-CD, що вузол не може виявити інший вузол, який також хоче передати пакет в результаті зіткнення. Алгоритм CSMA-CA буде використовуватися перед передачею даних кадрів команд MAC, переданих в рамках CAP. Протокол CSMA-CA використовує чотиристоронній режим.

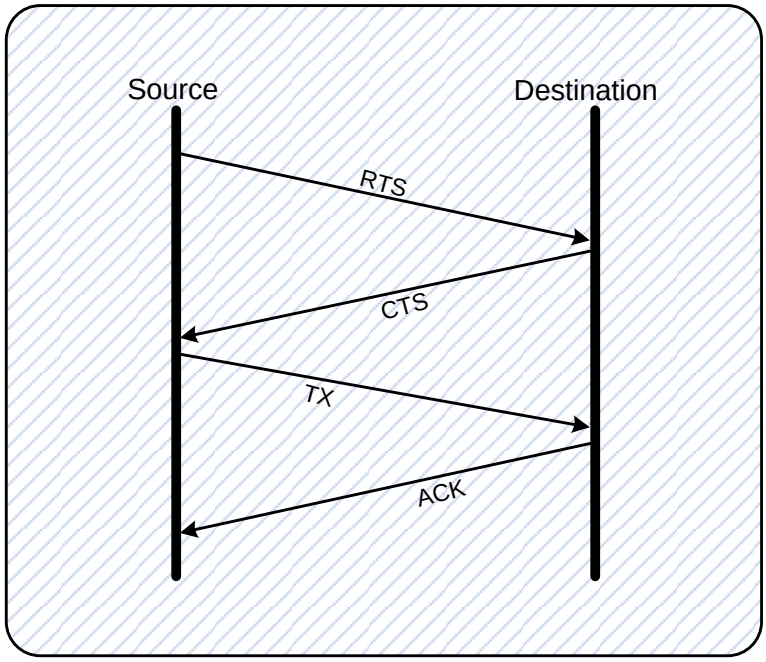


Рисунок 2.6 – Діаграма часу для CSMA-CA

Вузол прослухає (відчує рівень напруги), перш ніж передавати будь-який пакет. Якщо він виявить сигнал, він буде чекати випадкового періоду, перш ніж знову слухати мережу. Якщо сигнал не виявлений, вузол надішле готове до відправки повідомлення (RTS) на всі вузли. RTS містить адресу призначення та період передачі. Місце призначення відповість

повідомленням для відправки (CTS), яке позначає, що вузол може надсилати повідомлення без зіткнення. Місце призначення / підтвердження одержувач надішле для кожного отриманого пакету. Якщо CAP не отримано, пакет вважається втраченим або пошкодженим і буде повторно відправляти, поки CAP не буде отриманий. IEEE 802.15.4 використовує два типи механізму доступу до каналу, залежно від конфігурації мережі.

2.6.6 Прорізний CSMA-CA

Мережі з включеними маяками використовують цей механізм доступу до каналу, де відсічні слоти вирівнюються з початком передачі маяка. Кожен раз, коли пристрій хоче передавати кадр даних під час CAP, він повинен знаходити межу наступного слота для зворотного відключення, а потім чекати випадкової кількості відступаючих слотів. Якщо канал зайнятий, після цього випадкового зворотного відключення, пристрій повинен дочекатися ще одного слота зворотного відключення випадкового числа, перш ніж знову спробувати отримати доступ до каналу. Якщо канал в режимі очікування, пристрій може почати передачу на наступну доступну межу зворотного відключення.

2.6.7 Нерозрізнений CSMA-CA

Мережі без маяка використовують цей механізм доступу до каналу. Якщо пристрій хоче передавати кадри даних або команди MAC, воно буде чекати випадкового періоду. Якщо канал виявляється непрацюючим, після випадкового відключення пристрій передає свої дані. Якщо канал виявляється зайнятим після випадкового відключення, пристрій повинен чекати іншого випадкового періоду, перш ніж знову спробувати отримати доступ. Нерозкладений CSMA-CA - це метод доступу до каналу передачі даних.

2.6.8 Передача даних

Модель передачі даних може відбуватися трьома різними способами: (1) від пристрою до координатора; (2) від координатора до пристрою; і (3) від одного однорангового до іншого в багатокористувацькій мережі однорангових. Модель передачі даних також класифікується як пряма передача, непряма передача даних та передача даних GTS.

Пряма передача даних стосується всіх передач даних - від пристрою до координатора, від координатора до пристрою або між двома одноранками. Для передачі даних використовується нерозрізна CSMACA або прорізна CSMA-CA, залежно від того, чи використовується режим без маяка або режим включеного маяка. Тоді як непряма передача даних стосується лише передачі даних від координатора до її пристроїв. Інколи непряма передача даних може відбуватися і в режимі без маяка. Хоча передача даних GTS стосується лише передачі даних між пристроєм та його координатором, або від пристрою до координатора, або від координатора до пристрою. Жодна CSMA-CA не потрібна для передачі даних GTS.

3 МОДЕЛІ ЗАГРОЗ

Напади можна віднести до внутрішніх та сторонніх. У сторонній атаці вузол не є уповноваженим учасником сенсорної мережі. Коли сенсорні мережі спілкуються по бездротовому каналу, зловмисник може легко підслуховувати радіочастотний діапазон мережі, намагаючись викрасти приватну або конфіденційну інформацію. Також може змінювати або підробляти пакети, щоб порушити справжність зв'язку або вводити заважаючі бездротові сигнали, щоб заглушити мережу. Ще одна форма сторонніх атаки - відключення сенсорних вузлів. Зловмисник може вводити непотрібні пакети для зливання акумулятора приймача, або він може захоплювати та фізично знищувати вузли. Невдалий вузол - це те саме, що відключений вузол.

На відміну від сторонніх, внутрішні виконуються компрометованими вузлами в WSN. При компромісі у вузах супротивник може здійснити внутрішню атаку. На відміну від заборонених вузлів, компрометована діяльність вузлів прагне порушити або паралізувати мережу. Компрометований вузол може бути порушеним сенсорним вузлом або більш потужним пристроєм, як ноутбук, з більшою обчислювальною потужністю, пам'яттю та потужним радіо. Він також визначається як атака класів ноутбука, де зловмисники можуть володіти більш потужним обладнанням, таким як швидкий процесор, більша батарея, радіопередавач високої потужності або чутлива антена. Це обладнання дозволяє більш широкий спектр атак, які важче зупинити. Їх метою може бути запуск деякого шкідливого коду та прагнення викрасти секрети з сенсорної мережі або порушити її нормальні функції.

Отже, ще одним головним класом нападів є напади класу mote. Зловмисники класу mote користуються обмеженням процесора, потужності, пропускної здатності та діапазону платформи mote. У більшості випадків

вони мають доступ до кількох сенсорних вузлів, що мають аналогічні можливості, але не набагато більше цих. Вони можуть спробувати заглушити радіозв'язок, але лише в безпосередній близькості від вузла датчика. Однак ці атаки є більш обмеженими, оскільки зловмисники намагаються використовувати вразливості мережі, використовуючи лише вузлові можливості датчика.

3.1 Типи атак у WSN

WSN – це еволюційний розвиток в області розумних середовищ. Сенсорні дані можуть надходити від декількох датчиків різних модальностей у розподілених місцях. Їх можливості зробили їх досить популярними та широко використовувались у різноманітних програмах. Такі характеристики, як бездротове спілкування або агрегація даних, надають їм потенціал, який неможливо знайти в традиційних мережах.

Незважаючи на те, що було проведено багато досліджень з вивчення цих мереж, безпека є проблемою, яка все ще залишається на початковій стадії. Як правило, безпека мережі датчиків характеризується тими ж властивостями, що і традиційна мережева безпека. Однак WSN вразливі до нових методів експлуатації у багатьох шарах їх функціональності [13]. Наприклад, атаки на фізичний рівень включають заглушення радіосигналів та підробку фізичних пристроїв.

Інші проблемні питання виникають із рівня зв'язку, який обробляє зв‘язок між сусідом та канальний арбітраж. Якщо противник може породжувати зіткнення навіть частини передачі, він може порушити весь пакет. Одинарна бітова помилка призведе до невідповідності CRC і, можливо, вимагатиме повторної передачі. Крім того, він може мати на меті вичерпання енергії акумулятора мережі. Виснаження може бути викликане нападом. Наприклад, у протоколах IEEE 802: 15.4, запит на відправку (RTS) та очищення для відправлення (CTS) пакетів використовується для

резервування пропускної здатності перед передачею даних. Компрометований вузол міг неодноразово надсилати пакети RTS з метою отримання пакетів CTS від цільового сусіда, з часом споживаючи заряд акумулятора обох вузлів. Іншою формою цієї атаки є додавання до мережі вузла, який подає недостовірні дані або перешкоджання проходженню правдивих даних (позбавлення режиму сну). Більш тонкою метою для нападника може бути несправедливість на рівні MAC. Компрометований вузол може бути змінений для переривчастої атаки на мережу таким чином, що викликає несправедливість у пріоритетах щодо надання доступу до середовища. Наприклад, ця слабка форма відмови у наданні послуг може збільшити затримку, щоб протоколи в реальному часі пропустили свої терміни.

Крім описаних вище атак, щодо яких існують деякі контрзаходи, найважливіші та важкі для виявлення порушення безпеки націлені на мережевий рівень. Мережевий рівень відповідає за маршрутизацію пакетів по декількох вузлах. Бездротові сенсорні вузли не потребують зв’язку безпосередньо з найближчою контрольною баштою високої потужності або базовою станцією, а лише з місцевими. Натомість, спираючись на попередньо розгорнуту інфраструктуру, кожен окремий датчик або привід стає частиною загальної інфраструктури. Протоколи однорангових мереж забезпечують сітчастий взаємозв'язок для передачі даних між тисячами крихітних вбудованих пристроїв в режимі мульти-хоп. Таким чином, кожен вузол сенсорної мережі повинен взяти на себе обов'язки щодо маршрутизації. WSN є особливо вразливим для атаки маршрутизації, оскільки кожен вузол по суті є маршрутизатором. Запропоновано багато протоколів маршрутизації сенсорних мереж, але жоден з них не був розроблений з метою безпеки.

3.1.1 Глушення системи

Заглушення заважає радіочастоті, яка використовується вузлами для їх зв'язку. Вона виконується шляхом навмисної передачі радіосигналів. Використовується для здійснення атаки відмови в обслуговуванні, оскільки вузли взагалі не можуть спілкуватися, поки триває атака заглушенням (рисунок 3.1). Вузли вважають, що їх носій зв'язку використовується, або вважають, що якийсь вузол передає, і тому вони весь час залишаються в режимі прийому. Атака заглушенням викликається пристроєм, який зазвичай називають джамером. Це може бути сенсорний вузол або якийсь інший пристрій, здатний перешкоджати радіочастоті бездротової сенсорної мережі. Ми можемо виділити різні типи атак. Серед тих, які можуть бути найефективнішими, є постійні, оманливі, випадкові та реактивні глушники [14].

3.1.2 Класифікація заглушення

Постійне: випромінює радіочастотні сигнали, що інформують про випадкові згенеровані пакети, позбавлені будь-якого протоколу або правил на рівні MAC. Високочастотний сигнал, що випромінюється в бездротовий канал, створює зайнятий канал таким чином, що відправник сприймає носій як зайнятий. Постійне заглушення конкретно не передбачає схеми відчуття носія; це означає, що він чекає, поки канал почне працювати перед передачею. На підставі базового протоколу MAC [14] рівень визначає, чи є канал непрацюючим чи ні, порівнюючи вимірювання сили сигналу з фіксованим порогом, меншим від сили сигналу, що генерується постійним заглушення, таким чином, постійне заглушення може ефективно запобігти потраплянню через канал законних джерел трафіку.

Оманливий глушник: Як випливає з назви, оманливий виконує свою діяльність шляхом обману, він постійно вводить регулярні пакети в канал

між послідовними передачами без інтервалу часу, замість того, щоб відправляти випадковий біт. Оманливе заглушення передає напівправдиві пакети, які містять дійсні заголовки, але є марними. Це створює оманливе середовище, так що законні вузли сприймають канал як передачу дійсного трафіку. Через послідовну передачу заглушення без будь-якого розриву, законні вузли змушені переходити в режими прослуховування і не зможуть передавати жодний пакет, отже вони відступають.

Випадковий глушник: Ця форма іншими словами називається сном і пробудженням, це означає, що випадковий глушник чергує свій процес між сплячим режимом і режимом глушника замість того, щоб постійно надсилати радіосигнали. Під час режиму глушника він може вести себе як постійний або оманливий, як описано раніше, і переходить у сплячий режим, вимикаючи радіо. Ця форма враховує енергоефективність та збереження, дотримуючись режиму сну, що чітко розрізняє інші форми глушників.

Реактивний глушник: Ця форма спрямована на націлювання на приймальний канал, надсилаючи його радіосигнал лише тоді, коли канал відчутий зайнятим. Іншими словами, реактивний глушник враховує схему руху трафіку на відміну від попередньо описаних, які активні і спрямовані на виснаження енергоресурсів всієї мережі. Таким чином, ми зазначимо, що [14] реактивні глушники не обов'язково економлять енергію, оскільки радіопередавач повинен постійно знаходитись для того, щоб відчути канал.

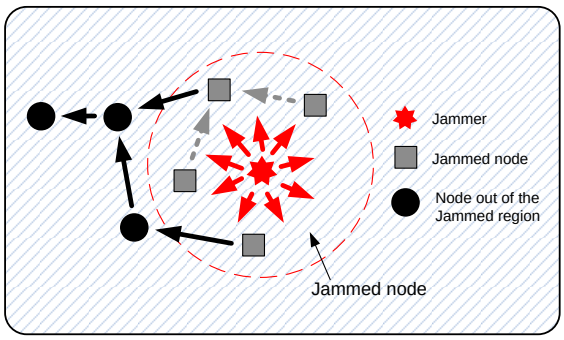


Рисунок 3.1 – Атака заглушенням

Для виявлення глушника може використовуватися кілька ознак. Короткий огляд цих методів наведено в наступному параграфі. Однак вони не завжди підходять для кожного типу. Більш детальну інформацію про виявлення атак глушника можна знайти в [10].

Отриманий індикатор сили сигналу може бути використаний для виявлення глушника, оскільки на розподіл сили сигналу впливає його активність. Основний підхід, коли середнє значення сили сигналу порівнюється з порогом, обчисленим із рівня шуму навколишнього середовища, є досить обмеженим. Більш зручна методика використовує спектральну дискримінацію по силі сигналу. На жаль, статистика, заснована на величині сили сигналу, підходить лише для виявлення постійних та оманливих глушників. На розподіл сили сигналу таким чином не впливають реактивні та випадкові заглушки, оскільки вони змінюють сплячий і випромінюючий стан, який імітує поведінку нормального вузла.

Протокол зондування використовується для того, щоб визначити, чи дозволений вузол для передачі через носій. Якщо вузол ніколи не знаходить медіа-режим очікування, він не може передавати і може припустити, що мережа заглушена. Метричний показник часу зондування підходить лише тоді, коли протокол доступу до носія сенсорної мережі повідомляє, чи не працює канал у встановленому порозі.

Коефіцієнт доставки пакетів раптово падає майже до нуля, коли вузол заглушена. У випадку перевантаженості воно не падає так раптово, і хоча коефіцієнт доставки дуже низький у перевантаженій мережі, він не наближається до нуля, як у випадку із забитою мережею. Коефіцієнт подачі може виявити перевантаженість від заглушення і корисний для розкриття всіх сценаріїв втручання. Однак він схильний до неточності через збій акумулятора або іншу мережеву динаміку, що може раптом призвести до неможливості доставки пакетів. Коефіцієнт доставки можна оцінити як отримані підтвердження / відправлені пакети на стороні відправника, або як кількість пакетів, які пройшли циклічну перевірку надмірності отримання

пакету на стороні одержувача.

Для усунення помилково оголошеного заглушення можна використовувати комбінацію описаних вище методів. Виснаження енергії може призвести до помилкової тривоги у випадку показника коефіцієнта доставки пакетів. Якщо метод співвідношення доставки пакетів поєднується з перевіркою стійкості сигналу, помилкові позитивні показники зменшуються. Дуже низький коефіцієнт доставки пакетів і низька потужність сигналу означають, що сусід вузла несправно працює через виснаження акумулятора. Однак, коли коефіцієнт доставки пакетів близький до нуля, а з іншого боку, сила сигналу висока, в бездротовій сенсорній мережі триває атака заглушенням з найбільшою ймовірністю.

Швидкість передачі пакетів (PSR) легко контролювати, і просте припущення дозволило б дізнатися, що вузол, який надсилає ненормальну кількість пакетів, є тим, який створює заглушення [15]. Ми можемо точно виявити оманливі глушники, контролюючи PSR сусідніх вузлів. Однак, від того, наскільки реалізовано заглушення, та мережевий протокол, можна виявити випадкові та реактивні дметамери, це залежить від того, чи є можливим виявлення дроселів. Врешті-решт, ми використовуємо дуже простий і обмежений підхід, щоб виявити постійне заглушення. Якщо під час спілкування з іншими вузлами існує вузол, що видає надзвичайно сильний сигнал, підозрюється, що це можливий глушитель, який міг би заглушити досить велику частину мережі.

3.1.3 Атака типа червоточини

Атака черв‘яком - це вид зовнішньої атаки, при якому противник може здійснити атаку, не порушуючи ключ шифрування або не потребуючи допомоги компрометованого вузла. Під час нападу противник встановлює два вузли в мережі та створює зв'язок між ними з низькою затримкою та високою якістю. Посилання згадується як атакуючий тунель і доступне лише

для цих двох вузлів. Один вузол, іменований шкідливим вузлом, підслуховує пакети і посилає їх через атакуючий тунель в інший вузол, який називається узгодженим вузлом. Узгоджений вузол відтворює пакети у своєму положенні.

Тож вузли в радіодіапазоні узгодженого вузла можуть чути вузли, радіодіапазон яких охоплює шкідливий вузол, і приймати ці вузли як своїх сусідів. Модель нападу зображена на рисунку 3.2. Відстань між злісним вузлом та узгодженим вузлом становить D. Співіснуючий вузол відтворює всі пакети від шкідливого вузла в каналі датчиків радіодіапазону Rw. Передбачається, що узгоджувальний вузол не пересилає жодних пакетів із вузлів датчика назад до шкідливого вузла. Ми визначаємо ділянку, що знаходиться один або два кроки від узгодженого вузла, як область впливу нападу черв‘яка. Вузли датчиків у зоні впливу називаються отруєними вузлами.

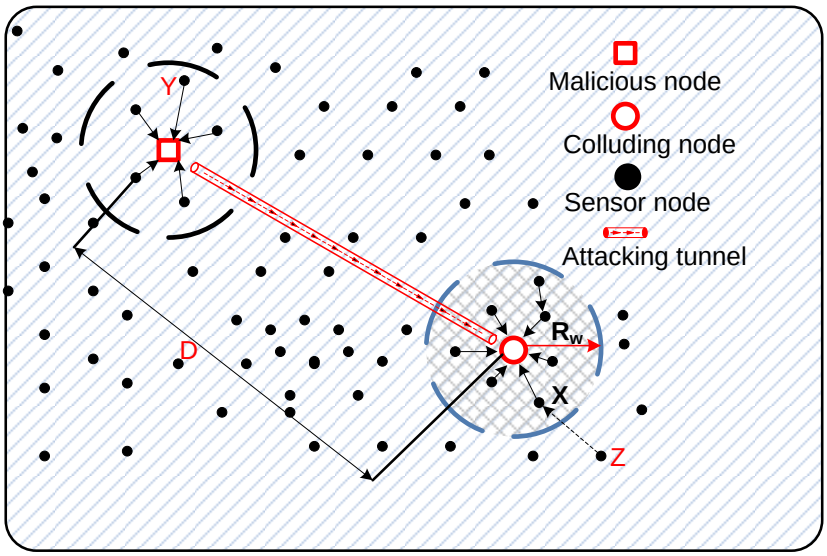


Рисунок 3.2 – Модель атаки черв'яком

Шлях маршрутизації, що використовує тунель, що атакує, здається, більш привабливим для отруєних вузлів, оскільки він має низьку затримку, мало стрибків, і відрізняється високою якістю. Наприклад, отруєний вузол X

може чути вузол датчика, радіодіапазон якого охоплює шкідливий вузол Y, і може приймати Y як наступний стрибковий вузол через перевагу атакуючого тунелю (рис. 3.2). Однак X і Y не є справжніми сусідами. Пакети, призначені для Y з X, не можуть досягти Y, оскільки атакуючий тунель є однонаправленим. В результаті нападу таке защемлення трафіку може зазнати не тільки отруєний вузол, але й вузли поблизу зони впливу.

Z, який приймає X як наступний стрибковий вузол, буде зазнавати такого ж заповнення трафіку, що і X. Таким чином, з'явиться зона плутанини маршрутизації, де вузли датчиків можуть неправильно адресувати свої пакети і не можуть надсилати свої пакети. Така зона плутанини маршрутизації може поширюватися на декілька рівнів поза межами узгодженого вузла. Однак, якщо отруєний вузол може самостійно ідентифікувати атаку черв‘яка та транслювати пакет попередження, щоб повідомити своїх сусідів не сприймати його як наступний вузол рівня, розширення області плутанини маршрутизації може бути ефективно обмежено, і тоді шкода, заподіяна нападу можна мінімізувати.

3.1.4 Hello flood атака

Атака Hello flood Протоколи маршрутизації зазвичай віддають перевагу найкоротшому або найнадійнішому шляху до базової станції. Початкові пакети (іноді їх також називають рекламними або маяками) надсилаються новим вузлом в мережі, щоб повідомити інші вузли, що вони, можливо, можуть спрямовувати свої повідомлення через новий вузол. Якщо шкідливий вузол має антену великого діапазону, він може транслювати початкові пакети, які вимагають гарного з'єднання з базовою станцією. Ці пакети отримають вузли, які не можуть дістатися до супротивника назад, оскільки у них немає такої сильної антени (рис. 3.3). Уражена частина мережі стає паралізованою, оскільки жодне повідомлення не виводиться з неї.

Вузли, близькі до зловмисника, можуть помітити, що значення

показників сили сигналу повідомлень, що надходять від зловмисника, аномально високі. Цей спосіб виявлення може бути реалізований за допомогою методики виявлення сусідів. Вузли зберігатимуть статистику середньої сили сигналу отриманих повідомлень від своїх сусідів та порівнюватимуть їх із усередненим значенням цих статистичних даних. Вузол із середньою силою сигналу, значно більшим, буде оголошено як нападник.

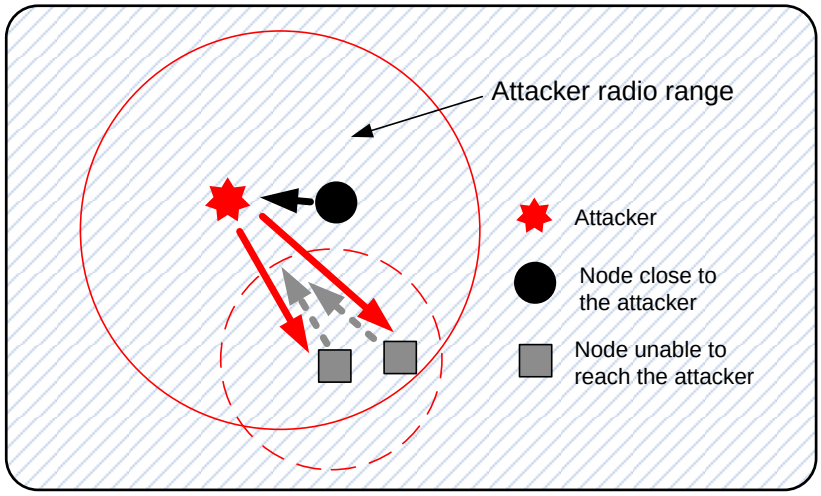


Рисунок 3.3 – Модель атаки Hello flood

3.1.5 Вибіркове пересилання

Компрометований вузол (зловмисник) скидає пакети замість того, щоб пересилати їх далі в системі багаторівневої маршрутизації у разі вибіркової атаки переадресації (рис. 3.4). Зловмисник може скинути всі вхідні пакети (також називають як атака чорної діри) або вибірково відкинути лише конкретні пакети (що надходять із конкретного джерела, мають певне призначення, містять певні дані про корисне навантаження тощо). У другому випадку виявити важче, і IDS має зберігати кілька статистичних даних для перевірки.

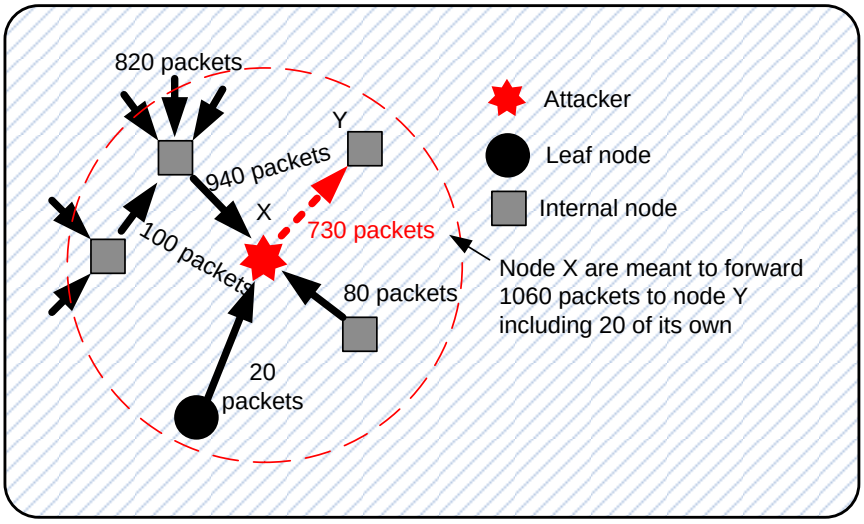


Рисунок 3.4 – Селективна атака переадресації

Висока швидкість випадання пакетів (PDR) може використовуватися для ідентифікації вузлів, які проводять селективне пересилання [16]. Він оцінюється як співвідношення між кількістю відправлених пакетів та кількістю отриманих пакетів за певний проміжок часу. Це співвідношення може зберігатися як загальна кількість переданих пакетів або просто для пакетів, що надходять із конкретного джерела, мають певне призначення тощо.

Підхід [17] не враховує лише пакети, скинуті шкідливим вузлом. У той же час система виявлення вторгнень перевіряє, чи передається пакет законному сусіду моніторизованого вузла. В іншому випадку передбачається, що пакет був спрямований зловмисним вузлом у невідповідне місце розташування. Для того, щоб ця методика працювала, форма початкового пакету (використовується для встановлення таблиць маршрутизації, коли в мережу додається новий вузол) має бути змінена, щоб кожен вузол міг вивести з нього своїх двох стрибків. Ця вимога робить цей механізм складнішим у застосуванні, ніж у випадку моніторингу швидкості зникнення пакетів. Протокол для виявлення двосхилих сусідів вузла означав би ще одні комунікаційні та обчислювальні витрати для крихітних вузлів.

3.1.6 Тип атаки Воронка

Вузол sinkhole – коли відображається більша частина трафіку (рисунок 3.5). Відповідно до протоколу маршрутизації, він вимагає надзвичайно гарного зв’язку з базовою станцією в своєму районі. Зловмисник намагається створити вузол sinkhole того, хто захоплений ними. Після цього за допомогою цього вузла можна запустити більш серйозні атаки. Залежно від того, який алгоритм маршрутизації використовується, зловмисник намагається підробити показники протоколу маршрутизації, які визначають найкращий шлях до шлюзу, тому більшість його сусідів, бажано всі, встановлюють захоплений вузол як свій батьківський вузол.

IDS може ідентифікувати вузли, які заявляють про підозріло високоякісне з'єднання із шлюзом і є єдиними такими вузлами у своєму районі. Ця методика не може визначити sinkhole, запущений на початку існування мережі, оскільки сусіди також вимагатимуть хорошого зв’язку через нього. Різниця у видимій якості зв'язку не буде помітна.

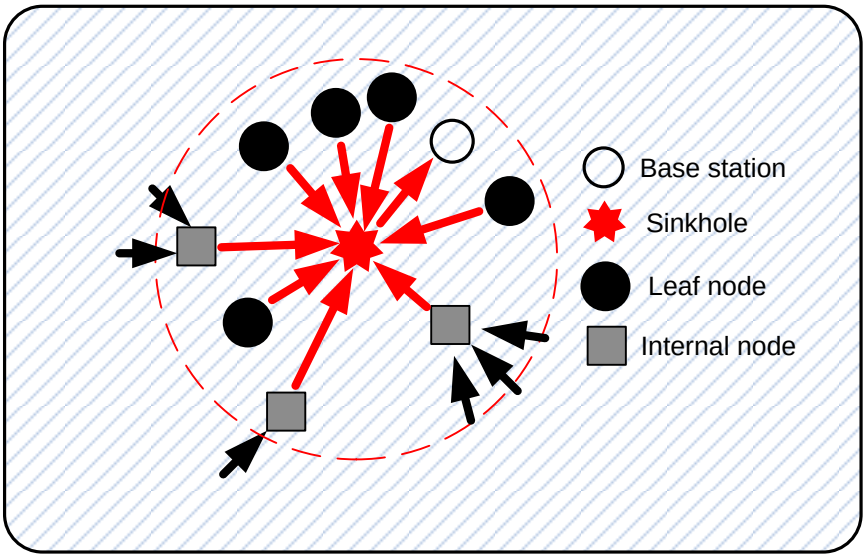


Рисунок 3.5 – Атака Sinkhole

Якщо швидкість прийому пакетів у певному вузлі надзвичайно висока, можливо, це буде підозрою, що він є зловмисником [15]. Однак цей симптом не розділяє sinkhole, які можуть існувати залежно від топології мережі. Крім того, швидкість прийому пакетів з навколишніх вузлів також стане високою, оскільки вони отримають дуже гарне з'єднання з базовою станцією через нього. Цей підхід вважається дуже обмеженим і не підходить для методів виявлення вторгнень.

Хоча шкідливий вузол може стверджувати, що його підключення до шлюзу краще, ніж є насправді, вузли в сусідньому районі не повинні відразу змінювати батьків. У цьому випадку зловмисник повинен знизити якість підключення інших вузлів. Шкідливий вузол може сфабрикувати підроблені пакети оновлення кореневих файлів, видаючи себе за своїх сусідів. Автори роботи [18] припускають, що ця форма атаки sinkhole може бути виявлена IDS, яка спостерігає, чи є передавач кореневих пакетів оновлення в околиці вузла, на якому працює IDS. Якщо ні, або якщо вони навіть надіслані вузлом, на якому працює сам IDS (можливо, коли заголовок пакета змінено), деякий вузол виконує атаку sinkhole в мережі.

Ця методика ефективно виявляє зловмисників, які намагаються знизити якість підключення інших вузлів. Якщо якийсь вузол виявить, що інший вузол підробляє пакети, він повинен негайно попередити інші вузли про це. Не має значення, яка спільна поведінка сусідства.

3.1.7 Сибільська атака

Вузол Sybil - це той, який вимагає кілька ідентифікаційних даних.. Зловмисник, який володіє цим, може скористатися протоколами голосування або створити маршрути для власних вигод. Зв'язок із вузлами може бути прямим або непрямим. Під час прямого зв'язку компрометований вузол зв'язується з іншими вузлами, відповідальними за всі його ідентичності. При непрямому спілкуванні вузол sybil стверджує, що він спілкується з вузлами,

які насправді не існують. Посвідчення можуть бути сфабриковані або викрадені. Атака sybil може бути здійснена одночасно або неодночасно, залежно від того, чи використовується вузол sybil одночасно або протягом часу.

Вузол може бути виявлений за допомогою тестування локації, заснованого на принципі, що деяка кількість взаємодіючих вузлів здатна оцінити місце розташування іншого вузла на основі деяких вимірювань. Якщо вони дізнаються, що два вузли розташовані в одній і тій же позиції, атака Sybil, швидше за все, проводиться зловмисником.

Техніка використання прийнятого сигналу (RSSI) описана в [19]. Три співпрацюючі вузли вимірюють силу сигналу після отримання повідомлення (рисунок 3.6). Після обміну отриманими значеннями співвідношення вимірюється від них і зберігається у записі відправника повідомлення в базі даних сусідів. Унікальне значення співвідношення визначає унікальне положення вузла. Аналогічний підхід опублікований і в [20]. Тестування локації базується на вимірюванні різниці у часі надходження (TDOA) пакетів між взаємодіючими вузлами замість потужності прийнятого сигналу.

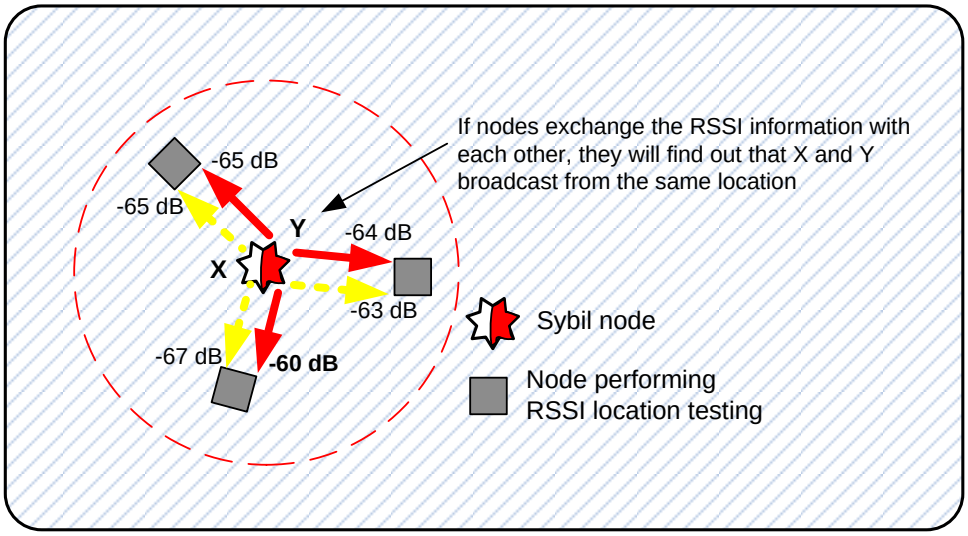


Рисунок 3.6 – Тестування RSSI локальної атаки sybil

І тести розташування RSSI, і TDOA потребують групи вузлів для обміну деякою інформацією. Ця інформація використовується для простого обчислення, результатом якого є визначення місця вузла, про який вони обмінювались інформацією. Кожен вузол має таблицю таких розташувань вузлів у своєму районі. Обидві методи не шукають властивості мережевої поведінки, яка не повинна помітно відрізнятися для вузла в деякій групі сусідніх вузлів.

3.1.8 Підміна пакета

Зловмисник може бути зацікавлений у підробці або зміні пакетів інших вузлів (рисунок 3.7), щоб неправильно використовувати алгоритм маршрутизації, мати перевагу в протоколах голосування або зміні вимірюваних значень, що надсилаються вузлами датчиків на базову станцію.

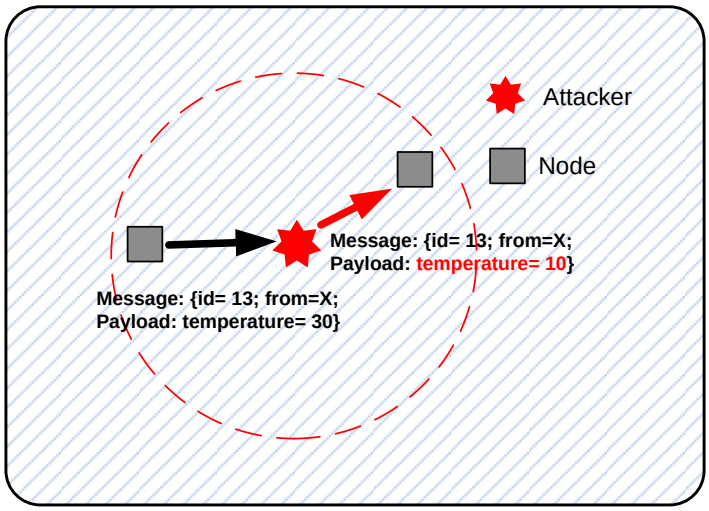


Рисунок 3.7 – Зміна пакетів

Моніторинг підроблених пакетів може бути передбачений аналогічно тому, як описано в цій главі в розділі, присвяченому атакам sinkhole і виявленню фальшивих маяків (розділ 3.1.5). Основне припущення полягає в

тому, що вузол повинен мати можливість сприймати лише пакети, що виникли в його сусідстві. Якщо вони виникли в іншому місці, підробка пакетів.

Для того, щоб виявити зміну даних, IDS повинен зберігати пакети в буфері, чекати, поки відповідні вузли переправлять їх, і порівняти, чи корисні навантаження однакові для пересланих пакетів і пакетів, що зберігаються в буфері. Відразу помічається присутність зловмисника, який змінює або підробляє пакети. Немає необхідності використовувати методи, такі як метод виявлення на основі сусідів, щоб з'ясувати, чи не є це звичайною зміною пакетів у сусідньому районі. Навмисна зміна завжди повинна розглядатися як напад.

3.1.9 Сфабрикована інформаційна атака

Шкідливий вузол може надсилати помилкові виміряні значення, які не відображають дійсність його оточення на базову станцію. Існує припущення, що ці значення, що надаються вузлами з близького сусідства, зазвичай мають незначно змінюватися (рисунок 3.8). Коли значення в оточенні вузла порівнюються і IDS виявляє, що вузол забезпечує надзвичайно різні результати, підозрюється, що зловмисник захопив його.

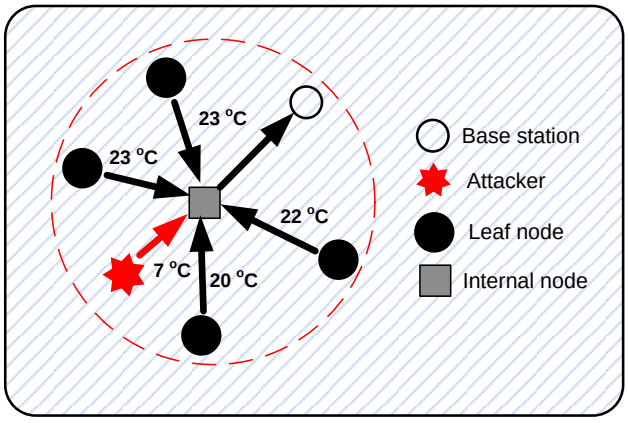


Рисунок 3.8 – Сфабрикована інформаційна атака

4 СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Бездротова мережа сеносорів пов'язана з вразливими характеристиками, такими як передача під відкритим небом та самоорганізація без фіксованої інфраструктури або централізованого управління. Отже, бездротові сенсорні мережі більш сприйнятливі до атак, а проблеми безпеки в них складніші. В якості першого напряму захисту від зловмисників можуть використовуватися методи запобігання вторгнень, такі як шифрування та автентифікація. Однак, навіть у стаціонарної мережі, активний захист недостатній для уникнення усіх проникнень. Друга лінія захисту потрібна для виявлення поточної атаки в мережі. Якщо таке виявлення доступне, пошкодження можуть бути мінімізовані.

Система виявлення вторгнень (IDS) контролює діяльність в системі, а потім аналізує отримані дані, щоб визначити, чи є порушення правил безпеки. Повідомлення надсилається, якщо виявлено порушення, яке, як відомо, є шкідливим. Відповіді на атаку також можуть ініціювати IDS. Доступні методи включають виявлення атаки, неправильного використання та визначення специфікацій, описаних у наступному підрозділі.

4.1 Методи виявлення вторгнень

Для виявлення нам потрібно використовувати модель вторгнення. Потрібно знати, на що слід звертати увагу на IDS. Зокрема, IDS повинен вміти розрізняти нормальну та ненормальну діяльність, щоб вчасно виявити спроби атаки. Однак це може бути складно, оскільки багато моделей поведінки можуть бути непередбачуваними та неясними. Існує три основні методи, які система виявлення вторгнень може використовувати для класифікації дій [21]:

4.1.1 Виявлення атаки

У системах виявлення атаки системах виявлення сигнатур [22] поведінка порівнюється з відомими схемами атаки (сигнатурою). Отже, моделі дій, які можуть становити загрозу безпеці, повинні бути визначені та надані системі. Система виявлення намагається визнати будь-яку погану поведінку відповідно до цих зразків. Дозволено будь-які дії, які чітко не заборонені. Основним недоліком таких систем є те, що вони не можуть виявити нові атаки. Хтось повинен постійно оновлювати базу даних атаки. Ще одна складність полягає в тому, що сигнатури повинні бути написані таким чином, щоб вони охоплювали всі можливі варіанти відповідного нападу, але все ж уникали хибного виявлення.

4.1.2 Виявлення аномалії

Виявлення аномалій [23] долає обмеження виявлення атак, орієнтуючись на нормальну поведінку, а не на поведінку нападу. Ця методика спочатку описує, що являє собою нормальна поведінку (як правило, встановлюється за допомогою автоматизованого визначення), а потім позначає як спроби вторгнення будь-які дії, що відрізняються від такої поведінки на статистичну кількість. Таким чином існує значна можливість виявити нові атаки. З цим підходом пов'язані дві проблеми: По-перше, система може проявляти законну, але раніше небачену поведінку. Це призведе до значної помилкової частоти тривоги, коли аномальні дії, які не є вторгненням, позначаються як шкідливі. По-друге, і ще гірше, вторгнення, яке не проявляє аномальної поведінки, може бути не виявлено, що призводить до помилок.

4.1.3 Виявлення на основі специфікації

Визначення на основі специфікацій [24] намагається поєднати сильні сторони неправильного використання та виявлення аномалії. Воно засноване на відхиленнях від нормальної поведінки. Однак у цьому випадку нормальна поведінка не визначається методами машинного навчання. Визначення засноване на введених вручну специфікаціях, які описують, що таке правильна операція, і стежать за поведінкою щодо цих обмежень. Таким чином, законна, але раніше небачене поведінка не спричинить високу помилкову частоту тривоги, як у підході до виявлення аномалії. Крім того, оскільки це засновано на відхиленнях від законної поведінки, все ще можливо виявити невідомі раніше напади. З іншого боку, розробка детальних специфікацій людьми може забирати багато часу і нести в собі притаманний ризик того, що певні напади можуть пройти непоміченими.

Слід бути обережними, застосовуючи техніку виявлення аномалії в сенсорних мережах. Визначити, що таке нормальна поведінка в таких мережах, непросто, оскільки вони зазвичай пристосовуються до змін у навколишньому середовищі або за іншими параметрами, наприклад, залишковим рівнем акумулятора. Отже, ці законні зміни поведінки можуть бути легко сприйняті IDS як спроби вторгнення. Більше того, сенсорні мережі не можуть перенести витрати на автоматичне навчання через низькі енергоресурси. Виявлення на основі специфікацій видається найбільш підходящим у цьому випадку, якщо можна розробити відповідні правила, що охоплюють якомога ширший спектр атак.

4.2 Архітектура системи виявлення вторгнень

Традиційно системи виявлення вторгнень для фіксованих мереж поділяються на дві категорії: на базі хоста та на основі мережі. Хост-архітектура була першою архітектурою, яку досліджували при виявленні

вторгнень. Система виявлення вторгнень на основі хоста (HIDS) призначена для контролю, виявлення та реагування на активність системи та атаки на даний хост (вузол). Будь-яке прийняте рішення ґрунтується на інформації, зібраній у цього хоста шляхом перегляду журналів на предмет підозрілої діяльності. Це суперечить розподіленому характеру сенсорних мереж і унеможливлює виявлення мережевих атак. Тут явно більше підходить мережева архітектура.

Мережеві системи виявлення вторгнень (NIDS) використовують вихідні мережеві пакети як джерело даних. Вони слухають в мережі, фіксують та вивчають окремі пакети в режимі реального часу. Аналіз всього пакету, а не лише заголовока. У провідних мережах активне сканування пакетів із мережі, заснованої на системі виявлення вторгнень, зазвичай проводиться в конкретних точках концентрації трафіку, таких як комутатори, маршрутизатори або шлюзи. З іншого боку, бездротові сенсорні мережі не мають таких вузьких місць. Будь-який вузол може виконувати роль маршрутизатора, а трафік зазвичай розподіляється з метою збалансування навантаження. Отже, неможливо контролювати рух в певних точках.

Оскільки вся комунікація у WSN ведеться по повітрю і вузол може перекривати трафік, що проходить від сусіднього вузла, вузли можуть взаємно перевіряти мережевий трафік. Наприклад, в [25] запропонована архітектура для спеціальних мереж, де вузли розподілені в кластерах, і лише голови кластерів відповідають за моніторинг трафіку в них. Однак один вузол монітору не відповідає вимозі "довіра вузлу", оскільки він може бути захоплений противником і може змусити мережу ізолювати інший законний вузол. Натомість певна частка вузлів у зоні повинна узгодити спостереження. Якщо кількість вузлів, які можуть сформувати таке виявлення, перевищує кількість вузлів, які можуть бути захоплені противником у певній області, для формування рішення може бути використана проста більшість голосів.

Характер WSN робить їх дуже вразливими для нападу. Перш за все, мобільні вузли є незалежними, а їх переміщення не контролюється системою,

тому їх можна легко захопити, скомпрометувати та викрасти. По-друге, оскільки в бездротових мережах немає фізичних перешкод для супротивника, атаки можуть надходити з усіх боків і вибирати будь-який вузол. По-третє, у бездротових спеціальних мережах противники можуть використовувати децентралізоване управління для нових типів атак, розроблених для порушення алгоритмів спільної роботи. Для вирішення цих додаткових проблем існує декілька можливих архітектур, включаючи окремі IDS, розподілені та спільні IDS та ієрархічні.

4.2.1 Автономний IDS

Кожен вузол працює незалежно від IDS, який відповідає за виявлення атак. Окремі представники не співпрацюють з іншими і не діляться жодною інформацією. Перевагою такого підходу є його простота і той факт, що зловмисник не в змозі зробити дезінформацію, оскільки вузли не покладаються на інших. Хоча ця архітектура недостатньо ефективна, але також може бути використана в мережах, де не кожен вузол здатний запускати IDS.

4.2.2 Розподілені та кооперативні IDS

Оскільки бездротові сенсорні мережі розподіляються та базуються на співпраці між вузлами, система виявлення та реагування на вторгнення повинна розподілятися та спільно працювати. У цій архітектурі кожен вузол має агент IDS і сам приймає локальні рішення щодо виявлення. При цьому всі вузли беруть участь у глобальному процесі виявлення. Як і окрема архітектура IDS, розподілена та спільна структура IDS більше підходить для конфігурації плоскої мережі, ніж багатошарова на основі кластера.

Як правило, головним завданням такого підходу є питання, як боротися з компрометованими сусідами. Ми не хочемо, щоб шкідливий вузол міг

плутати інших із дезінформацією. У роботі [26] автори представили алгоритм голосування, який ґрунтується на презумпції, що зловмисник не в змозі перевищувати кількість законних вузлів.

4.2.3 Ієрархічна IDS

У цій категорії мережа поділяється на кластери з утворенням кластерних вузлів. Ці вузли відповідають за маршрутизацію всередині кластера і приймають усі повідомлення про звинувачення від інших членів кластера, що вказують на зловмисну діяльність. Крім того, вузли головки кластера можуть також виявляти атаки на інші вузли мережі, оскільки вони складають основу інфраструктури маршрутизації. У п'ятій главі ми пропонуємо методику DIDS, засновану на керуванні кластерними вузлами. Ми впроваджуємо алгоритм кластера, що використовує розподілений та спільний механізм виявлення, необхідний для виявлення аномалій серед мережевих вузлів.

4.2.4 Ідентифікатор мобільного агента

IDS на основі мобільних агентів може розглядатися як розподілена і спільна техніка виявлення вторгнень, або вона може використовуватися в поєднанні з ієрархічною IDS. Агент мобільний завдяки своїй здатності рухатися по мережі та взаємодіяти з вузлами, збирати з них інформацію. Завдання на виявлення вторгнень розповсюджуються та призначаються цим мобільним агентам. Кожному мобільному агенту призначено конкретне завдання і дія на інформацію, яку він збирає по своєму рухомому шляху.

Є багато переваг використання мобільних агентів. Перш за все, енергоспоживання мережі зменшується, оскільки завдання розподіляються, і кожен вузол вміщує лише деякі завдання, а не всі. По-друге, загальне відношення до відмов у системі збільшується, оскільки завдання IDS

розподіляються по різних частинах мережі; коли одні агенти руйнуються або частини мережі відокремлюються, інші можуть залишатися функціональними. По-третє, оскільки мобільний агент може бути незалежним від платформи, IDS може працювати в різних середовищах операційної системи.

Крім того, коли центральний процесор замінюється розподіленими мобільними агентами, обчислювальне навантаження поділяється між машинами, а навантаження на мережу зменшується. Однак цих мобільних агентів все ще потрібно запускати в захищеному модулі на кожному вузлі, щоб захистити себе на віддалених хостах.

4.3 Вимоги до системи виявлення вторгнень для WSN

Для того, щоб детальніше розглянути вимоги, яким повинна відповідати система IDS для сенсорних мереж, слід переглянути конкретні характеристики цих мереж. Кожен вузол датчика має обмежені комунікаційні та обчислювальні ресурси та короткий радіодіапазон. Крім того, кожен вузол - це слабкий підрозділ, який може бути легко порушений противником, який може завантажувати зловмисне програмне забезпечення для запуску внутрішньої атаки.

У цьому контексті та беручи до уваги обговорення в розділі 5.2, розподілена архітектура, заснована на співпраці між вузлами, є бажаним рішенням. Зокрема, ми вимагаємо, щоб IDS для сенсорних мереж відповідало наступним властивостям:

- локальний аудит. IDS для сенсорних мереж повинен працювати з даними локалізованого та часткового аудиту. У таких мережах немає централізованих точок (крім базової станції), які можуть збирати дані для всієї мережі, тому такий підхід відповідає парадигмі мереж. Робота з частковими даними означає, що IDS також має вирішити проблему високої помилкової частоти.

- Мінімізація ресурсів. IDS для сенсорних мереж повинен використовувати невелику кількість ресурсів. Бездротова мережа не має стабільних з'єднань, а фізичні ресурси мережі та пристроїв, такі як пропускна здатність та потужність, обмежені. Відключення може статися в будь-який час. Крім того, зв'язок між вузлами для виявлення вторгнень не повинен займати занадто багато доступної пропускної здатності.

- Не довіряти жодному вузлу. У спільних IDS вузлах не можна вважати, що іншим вузлам учасників можна довіряти. На відміну від дротових мереж, сенсорні вузли можуть бути легко порушені. Ці вузли можуть поводитись нормально щодо маршрутизації інформації, щоб уникнути виявлення IDS. Однак вони можуть виявити зловмисну поведінку, щоб перешкодити успішному виявленню іншого зловмисного вузла. Тому в алгоритмах співпраці IDS повинен припускати, що жодному вузлу не можна повністю довіряти.

- Розподілення. Процес збору та аналізу даних повинен здійснюватися в декількох місцях, щоб розподілити навантаження виявлення вторгнень. Розподілений підхід також застосовується до виконання алгоритму виявлення та кореляції попередження.

- Підтримка додавання нових вузлів. На практиці ймовірно, що сенсорна мережа буде заповнена більшою кількістю вузлів після її розгортання. IDS має бути в змозі підтримати цю операцію та відрізнити її від нападу (наприклад, нападу черв'яка), що має той самий ефект.

- Безпека. IDS повинен мати можливість протистояти ворожій атаці проти себе. Компрометація вузла моніторингу та контроль поведінки вбудованого агента IDS не повинні дозволяти противнику відкликати законний вузол з мережі або залишати невизнаним інший вузол противника.

5 РОЗПОДІЛЕНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ

Системи виявлення вторгнень (IDS) у бездротових сенсорних мережах пропонуються відповідно до характеристик бездротового середовища. Архітектура IDS для бездротової сенсорної мережі може залежати від самої мережевої інфраструктури. Бездротові мережі можуть бути налаштовані як в плоскій, так і в багаторівневій мережевій інфраструктурі. У багаторівневій інфраструктурі всі вузли вважаються неоднорідними, тоді як у плоській всі вузли вважаються однорідними (рівними і можуть брати участь у функціях маршрутизації) [27]. Ідентифікатори можуть бути класифіковані на чотири категорії, які можуть бути відрегульовані і підходити для систем WSN (четвертий розділ).

5.1 Кластерна архітектура

Кластеризація - метод, за допомогою якого вузли розміщуються в групи, які називаються кластерами. Для кожного кластера обирається голова, яка підтримує перелік вузлів, що належать до цього ж кластеру, а також шлях до кожного, який оновлюється [28]. Кластер може бути сформований на основі багатьох критеріїв, таких як дальність зв'язку, потужність передачі, кількість та тип датчиків, локалізація тощо. У цій роботі голови кластерів спільно розташовують розгорнуті датчики та перегрупують їх, щоб мінімізувати енергію передачі датчика при збереженні підключення. Виходячи з нашого механізму, ми припускаємо статичні датчики з датчиками головки кластера.

Зокрема, вся мережа поділена на зони, що не перекриваються (кластери), як показано на рисунку 5.1, із внутрішніми кластерними вузлами (також називаються вузлами шлюзу, тобто тими вузлами, які мають віддалене з'єднання з різними кластерами), з кожного кластера, які

відповідають за агрегацію та співвіднесення локально сформованих сповіщень всередині кластера. Внутрішні головки кластерів після виявлення локальної аномалії генерують попередження і транслюють свої сповіщення в кластери. У DIDS вузли шлюзу можуть також використовувати сповіщення для генерування тривог, які можуть ефективно знижувати помилковий коефіцієнт тривоги та покращувати показник виявлення. C означає ступінь агрегації даних (кількість відсутніх сусідів / переходів) між головкою кластера (CH) та вузлами датчика (Node-to Sink) завдяки типу протоколу маршрутизації. Для заданого значення K вузли в k-симетричному діапазоні передачі організовуються в кластер, повторно вибирається головка кластера (CH) для поширення інформації про маршрутизацію та для підтримки двонаправленого зв'язку з кожним вузлом датчика, інакше вузли в межах k-асиметрично виключаються з кластера або відключаються від зв‘язку.

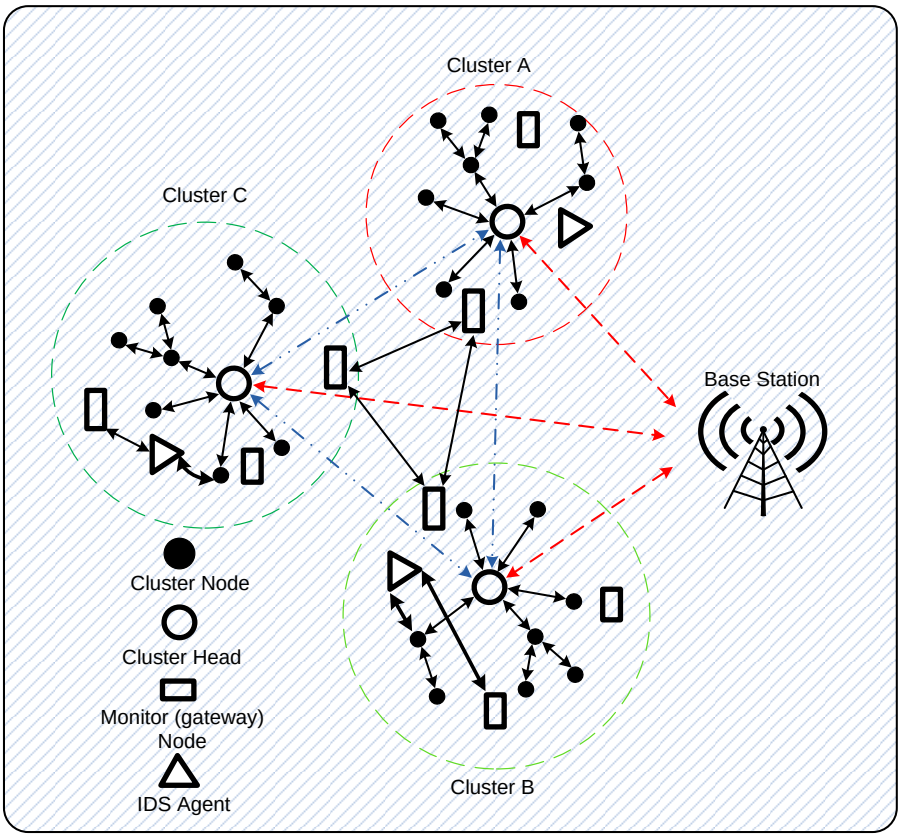


Рисунок 5.1 – Запропонована архітектура на основі кластера WSN DIDS

5.2 Модель вузла головного кластера DIDS

IDS є розповсюдженим та кооперативним за своєю природою. Кожен вузол головного кластера відповідає за виявлення ознак вторгнення, за обробку інформації, отриманої від одиниць збору даних IDS в межах домену кластера локально та незалежно. Базовій станції в її автономії присвоюється привілей контролювати та виявляти ознаки вторгнення, реакцій всередині віртуального кластера поза середовищем.

Наш DIDS складається з різних підсистем: мобільний агент (MA), статичний агент (SA), агент вузла (NA) та список компромісних вузлів (CNL) (також називається списком вузлів жертви).

Статичний агент встановлюється у кожному вузлі головки кластера та локально. SA на базовій станції працює автономно, отримує звіти про виявлення вторгнень від головних вузлів кластера та здійснює моніторинг діяльності (включаючи трасування даних вузла, зміну маршруту (щільність вузла), середню довжину шляху, потужність передачі). SA налаштований на підтримку декількох функцій, коли кожна діяльність контролюється вузлом жертви для різних класів нападу. Ці функції виконуються через регулярний налаштований інтервал часу для перевірки файлів журналу на наявність слідів атаки. Рисунок 5.2 демонструє роботу головного вузла DIDS-кластера.

Мобільні агенти, що перебувають у голові кластера, відповідають за збір доказів нападу з усіх компрометованих вузлів та подальший аналіз зібраних даних. Кілька MA пов'язаних з кожною головою кластера і утворюють блок живлення сервера IDS. CNL містить перелік усіх скомпрометованих вузлів та усі підозри аномалії у мережі.

NA є найпоширенішими агентами сервісного обслуговування і находяться у кожному сенсорному вузлі мережі та допомагають сигналізувати SA про можливі атаки шляхом моніторингу локальних подій (звичайне прослуховування) через IDS, що працює на сервері прикладних програм, а також повідомляючи MA на основі щільності вузла та зміни

маршруту, що супроводжується контролем потоку пакетів. Також в голові кластера DIDS модуль обслуговування кластерів активно оновлює інформацію про маршрути всіх членів кластера в кожному кластері на основі змін топології (тобто комутатор вузла, оновлення зв'язку, втрата зв'язку та ін.) Усі дані передаються в IDS для перевірки та класифікації. Модель DIDS (CH) була поділена на три основні функціональні одиниці:

5.2.1 Блок аналізу даних

У цьому блоці всі повідомлення та вхідні дані, зібрані з контрольованого блоку, прослуховуються в безладному режимі, а важлива інформація фільтрується і зберігається в кеші для подальшого аналізу. Ця інформація може включати поля повідомлень, необхідні для процесів застосування програм на основі правил. Для цілей наших механізмів інформація включає сліди атаки з потужністю передачі пакетів, швидкістю надходження пакетів, розмірами даних, кількістю переходів і т.д. Дані, витягнуті з повідомлень, надсилаються до вузлів для подальшої обробки відповідно до заздалегідь визначених правил протягом заданого часу кадру або після закінчення буферного простору.

5.2.2 Прикладний блок

Цей блок містить в собі програми, засновані на правилах, що керують схемою виявлення, що стало можливим завдяки різним заходам в межах кластера та поза ним. Процеси маршрутизації та схеми передачі пакетів використовуються для визначення неминучої поведінки чи вторгнення у разі нападу. Технічне обслуговування кластерів є основою, для якої застосовуються правила. У цьому підрозділі кожен запис у структурі даних масиву оцінюється відповідно до послідовності правил, визначених для повідомлення, згідно з нашим визначеним набором правил вторгнення.

Відмова повідомлення, застосоване до певного правила, вимагає збільшення лічильника відмов з подальшим відкиданням такого повідомлення без будь-якого іншого застосованого до нього правила, яке отримується в пункті призначення як недійсний пакет і відкидається.

5.2.3 Серверний блок IDS

Можливості виявлення вторгнень на запропонованій нами моделі зосереджені на цьому блоці, в якому всі агенти всередині СН встановлюють двосторонній зв’язок шляхом моніторингу та виявлення аномалій всередині мережі. Для того, щоб реалізувати IDS, який здатний відрізняти випадкові збої в мережі від випадків нападу, що виконуються зловмисниками, ми представляємо нашу модель, яка відстежує ефект подібності у випадку загальних та підозрюваних збоїв. Це проілюстровано на рисунках 5.6 та 5.5. Ця методика вводить аномалію картини, якій передують сліди вторгнення, згідно з якими всі рішення та відповіді піддаються порівнянню та виявленню вторгнення.

Ідентифікатор IDS також може бути сформульований як проблема класифікації моделей [29], в якій класифікатори призначені для ідентифікації дій як нормальних або нав'язливих на основі набору ознак. Автори застосовують два добре відомих класифікатора; RIPPER та підтримка вектора (SVM). RIPPER [30] є еквівалентними класифікаторами дерева рішень для виявлення правил на основі зменшення обрізки помилок (IREP). Під час поділу наданих даних на відповідні класи RIPPER може обчислювати правила та виявляти аномалії. Що ж, для нашого підходу така схема не підходить.

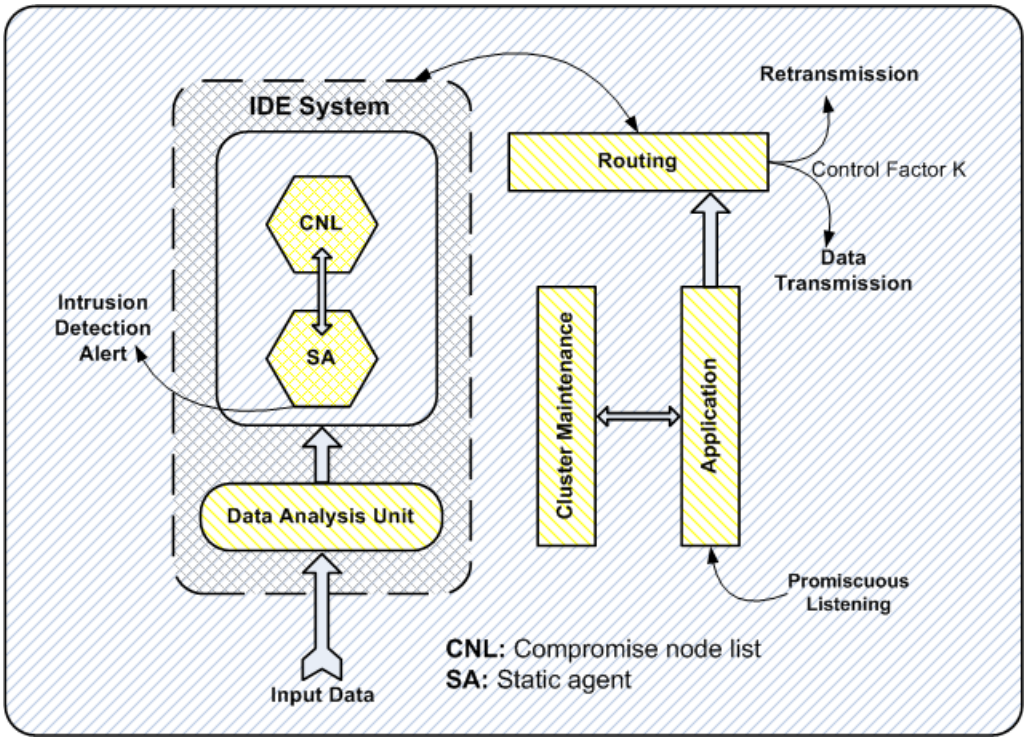


Рисунок 5.2 – Запропонована модель вузла головного кластера DIDS

5.3 Застосування системи

Наша робота забезпечує гнучку структуру управління топологією голови кластера, яка використовує вузли кластера та мережеві агрегації даних із зменшеними витратами енергії, необхідними для підвищення рівня безпеки мережі. Основна ідея полягає у впровадженні системи виявлення вторгнень, необхідної для виявлення наявності атаки jammer всередині мережі. Запропонована схема (DIDS) відповідає трифазній структурі процесу впровадження. По-перше, ми використовуємо алгоритм кластеризації з формуванням головки кластера, потім - фаза виявлення сусідів після спільного поширення інформації, по-третє, алгоритм виявлення на основі пов'язаних атак та класифікацій нормальних та аномальних профілів з урахуванням процесу атаки.

5.3.1 Фаза створення кластеру

З метою забезпечення масштабованості та підтримки зв’язку між вузлами датчиків мережа розподіляється на ряд груп, що не перекриваються, які називаються кластерами, як показано на попередньому рисунку 5.1. Ці кластери створюються за допомогою алгоритмів кластера, і кожен член кластера підтримує QoS-параметричну таблицю інформації [31] про свій розділ. Маршрутизація зазвичай поділяється на два типи: маршрутизація всередині кластера (внутрішньокластерна маршрутизація) та маршрутизація між різними кластерами (міжкластерна маршрутизація).

На кожному вузлі процес кластеризації вимагає певної кількості ітерацій, які ми називаємо N_{iter}. Кожен крок вимагає часу t_c, який повинен бути досить довгим, щоб отримувати повідомлення від будь-якого сусіда в межах кластеру. Ми встановлюємо початковий відсоток головок кластера серед усіх n вузлів, C_{prob} (скажімо, 5%), припускаючи, що оптимальний відсоток не можна обчислити апріорі. C_{prob} використовується лише для обмеження початкових оголошень головки кластера і не має прямого впливу на кінцеві кластери. Перш ніж вузол починає виконувати HEED, він встановлює свою ймовірність стати головою кластера, C_{prob}, таким чином:

$$CH_{prob} = C_p \times \frac{E_{residual}}{E_{max}} \tag{5.1}$$

де $E_{residual}$ - це орієнтовна поточна залишкова енергія у вузлі, а E_{max} - це максимальна енергія (відповідає повністю зарядженій батареї), яка, як правило, однакова для всіх вузлів. Однак значення CH_{prob} вузла не може опускатися нижче певного порогу p_{min} (наприклад, 10^{-4}), який обраний таким, що обернено пропорційний E_{max}. Це обмеження є важливим для припинення алгоритму в ітераціях N_{iter} = O (1), як ми покажемо далі. Зауважте, що наш

підхід до кластеризації здатний обробляти неоднорідні акумуляторні вузли. У цьому випадку кожен вузол матиме власне значення E_{max}.

Під час будь-якої ітерації i, , $i \leq N_{iter}$, кожен «непокритий» вузол (як визначено нижче) вирішує стати головою кластера з імовірністю CH_{prob}. Після набоу орієнтовних голів кластерів, S_{CH}, встановлюється на {голови кластерів після кроку $i-1 \cup$ нових голів, обраних на етапі i }. Вузол v_i обирає свою головку кластера (*my cluster head*) як вузол з найнижчою вартістю в S_{CH} (S_{CH} може включати сам v_i, якщо він обраний як попередня головка кластера). Потім кожен вузол подвоює CH_{prob} і переходить до наступного кроку. Псевдо-код для кожного вузла наведено в нижче. Зауважте, що якщо для внутрішньо кластерного зв'язку можуть використовуватися різні рівні потужності, то лінію 1 на фазі I слід змінити так: Відкриття для себе сусідів у межах кожного рівня потужності $Pwrc \leq pwrc$, де *Pwrc* - рівень потужності кластера. Лише в цьому випадку ми припускаємо, що якщо головка кластера u може досягати вузла *v* з рівнем потужності *l*, то *v* може також доходити до рівня *l*. Виявлення сусідів не потрібно щоразу, коли активізується кластеризація. Це відбувається тому, що в стаціонарній мережі, де вузли не зникають несподівано, сусідський набір кожного вузла змінюється не дуже часто. Крім того, розподіл енергії споживання HEED подовжує термін експлуатації всіх вузлів у мережі, що додає стабільності сусідам. Вузли також автоматично оновлюють набори сусідів у кількох мережах, періодично надсилаючи та отримуючи повідомлення роботи.

Зауважте також, що якщо вузол вирішує стати головою кластера, він надсилає повідомлення cluster_head_msg (Node_ID, статус вибору, значення), де статус вибору встановлюється *CH*, якщо його CH_{prob} менше 1, або кінцевий *CH*, якщо його CH_{prob} досягнув 1. Вузол вважає себе "охопленим", якщо він почув або попередній *CH*, або кінцевий *CH*. Якщо вузол завершує виконання HEED, не вибираючи голову кластера, що є остаточним *CH*, він вважає себе непокритим і оголошує себе головою кластера з кінцевим *CH*.

Орієнтовний вузол *CH* може стати звичайним вузлом при більш пізній ітерації, якщо він знайде голову кластера з меншою вартістю. Зауважте, що вузол може вибрати голову кластера через послідовні інтервали кластеризації, якщо він має високу залишкову енергію та низьку вартість.

Псевдокод алгоритму HEED, що виконується кожним вузлом, наведено нижче:

I. Initialize

1. $S_{nbr} \leftarrow$ {v: v lies within my cluster range}
2. Compute and broadcast cost to $\in S_{nbr}$
3. $CH_{prob} \leftarrow max\left(C_{pro} \times \frac{E_{residual}}{E_{max}} p_{min}\right)$
4. is_final_CH $\leftarrow$ FALSE

III. Finalize

1. If (is_final_CH = FALSE)
2. If ((S_{CH} {v: v is a final cluster head})
3. my cluster head least cost(S_{CH})
4. join cluster(cluster_head_ID, NodeID)
5. Else Cluster head msg(NodeID, final CH, cost)
6. Else Cluster_head_msg(NodeID, final_CH, cost)

II. Repeat

1. If (($S_{CH} \leftarrow$ {v: v is a cluster head}) $\neq \emptyset$)
2. my_cluster_head $\leftarrow$ least cost(S_{CH})
3. If (my_cluster_head = NodeID)
4. If (CH_{prob} = 1)

14. $CH_{previous}$ CH_{prob}
15. CH_{prob} min(CH_{prob} × 2, 1)

Until $CH_{previous}$ = 1

Приклад 5.1 – Псевдокод алгоритму HEED

Для здійснення успішного механізму виявлення вторгнень з метою збільшення часу життя сенсорної мережі при збереженні підключення до неї, ми розглядаємо створення / вибір головки кластера на основі середньої вартості енергії (залишкової енергії) кожного сусіднього вузла та середньої довжини шляху, яка становить функція вартості зв'язку з точки зору близькості сусідів або щільності кластеру, отже, міру коефіцієнта контролю перевантаженості.

5.3.2 Фаза відкриття сусідів

Відкриття сусідів як частина нашої схеми DIDS у додатках датчиків вузлів забезпечує проактивну форму переадресації повідомлень, використовуючи взаємодію вузлів, необхідну для запобігання зловмисникам зриву роботи мережі. Як і в [31], життєво важливим процесом залишається взаємодія у вузлах, що спирається на виявлення відхилень від очікуваної поведінки сусіда. Дозорний підхід [32] - це ще одна методика, яка використовується при сусідовому моніторингу та вибірковому пересиланні. У цьому контексті, як зображено на рисунку 5.3, ми використовуємо відкриття сусіда на основі розподіленого та спільного рішення.

Ми вивчаємо концепцію послідовності пересилання повідомлень у суцільному кластері як форму стримування вторгнень. Як показано на рисунку 5.3, для виявлення сусідів використовується дифузійний процес та кількість переходів для ініціалізації маршрутів повідомлень серед вузлів, зберігаючи локальні оновлення з кожним сусідом. Виявивши головний вузол кластера, ініціюється маршрут топології, спочатку розсилаючи своє повідомлення Beacon Topology Control (BTC) з максимальною потужністю передачі. Крім усього іншого, BTC виконує функцію пробудження для всіх членів кластеру у разі будь-якої неминучої небезпеки. Після отримання повідомлення всі вузли в межах найближчого кроку (k-відстань) встановлюються для попередження про можливе оновлення та переадресацію. При виявленні будь-якого вторгнення ініціалізується реактивна форма сповіщення, відома як стримування. Це стосується підтвердження атаки, стримування та колективної дії всіх сусідніх вузлів у кластері, включаючи голови кластерів проти підозри на вторгнення. Рисунок 5.4 ілюструє виявлення та стримування зловмисника за допомогою взаємодії з вузлами після процесу виявлення сусіда.

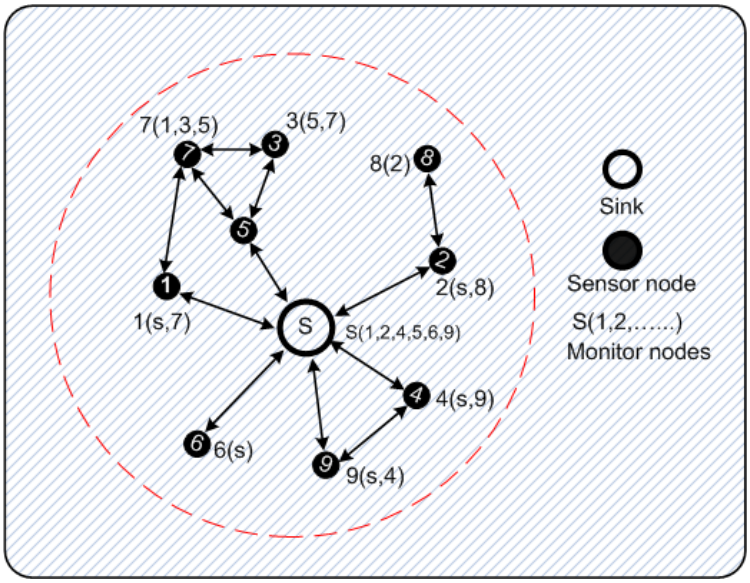


Рисунок 5.3 – Послідовність переадресації повідомлень BTC через кількість переходів.

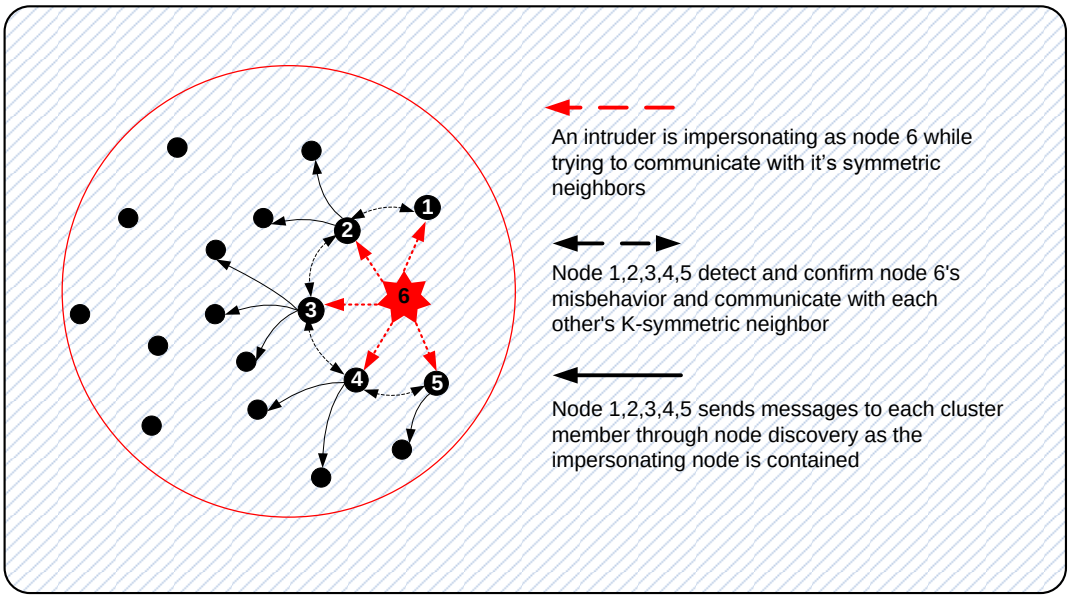


Рисунок 5.4 – Адаптація виявлення зловмисників у фазі виявлення вузла

Спочатку кожен датковий вузол N_i, *(для i=1)* намагається виявити своїх сусідів за допомогою рівня MAC, що працює на максимальній енергії передачі (залишкова енергія), зберігаючи при цьому оновлення сусіда (N^*_i) в межах значної кількості рівнів. Вузол головки кластера (CH) під час

моніторингу ініціює процес виявлення шляхом зондування всіх членів кластера та вимагає оновлень, він видає повідомлення контролю топології маяка (ВТС), що містить список k найменш віддалених сусідів (N^k_i), серед інших полів, які оновлюються а потім транслювання на всі інші вузли, як показано на рисунок 5.3.

Після підозри в неправильній поведінці на вузлі 6 (наприклад, ненормальне падіння пакетів) вузол (шлюз) монітора (наприклад, вузли, 1, 2, 3, 4, 5) взаємодіють один з одним та інформують про інші сусідні вузли, зображені на рисунку 5.4. Кожен член кластера *i* перевіряє свою ступінь симетрії з СН та або вузлом(ами) шлюзу та вузлом зловмисника 6, позначеними *j*, якщо *i* та *j* є k-симетричними, тобто $\left(\{j/j \in N_i^k\} \wedge \{i/i\} \in N_j^k\right)$ СН відправляє профілі на базову станцію для перевірки, тоді як приймальні вузли самоорганізовуються. Якщо існують k-асиметричні, тобто .$\left(\{j/j \ni N_i^k\} \wedge \{i/i\} \in N_j^k\right)$, вузли шлюзу вибирають СН і підтримують новий кластер, щоб містити зловмисника в межах його виділеного кластер. Базова станція порівнює профіль вузла зловмисника з попередніми прийомами пакетів через проміжки часу, якщо отриманий пакет відповідає статистиці сусідів, він приймається як нормальний, інакше відхилення сигналізує про вторгнення.

5.3.3 Фаза виявлення

Дотримуючись гібридної схеми виявлення, такої як методика виявлення на основі специфікації в 4.1.3; ми коротко ознайомимося з попередньо передбачуваними моделями атак та відповідними правилами, що є основою для встановлення нашого алгоритму IDS. Наступні кроки передбачають початкову лінію дій, спрямовану на створення відповідного алгоритму, як зазначено нижче.

Попередній вибір із наявного набору правил, шаблону та інформації тих, які можуть бути потрібні / використані для встановлення або контролю

аномальних особливостей у процесі виявлення.

Визначення відповідних параметрів обраних правил або набору даних зі значеннями визначень вторгнення.

Порівняння інформації за звичайними схемами, що вимагаються попередньо вибраним правилом, з інформацією, доступною в цільовій мережі, для будь-якої ненормальної діяльності, щоб отримати певну відповідь.

5.3.4 Запропоновані правила та визначення вторгнення

Розглянувши етапи попереднього вибору, як описано вище, ми визначимо набір метрик на основі правил, які є частиною процесів виявлення, необхідних для встановлення виявлення вторгнення в мережі. Наш механізм боротьби DIDS дотримується принципу виявлення, встановленого цими правилами, в якому певні збої розглядаються або як поширені, або внаслідок нападів зловмисників.

Правило інтервалу: враховуючи заздалегідь визначений часовий проміжок, помилка спостерігається, якщо час, пройдений між прийомами двох послідовних повідомлень, більший або менший, ніж дозволені межі. який вузол каналу приймача не посилає повідомлення даних, згенеровані вузлом передавача через перешкоди шуму та атаки виснаженням, при яких швидкість споживання енергії збільшується за рахунок більш високого рівня потужності передачі джемпера.

Правило цілісності: будь-яка атака на модифікацію переданого пакету в каналі передачі є аномалією і буде виявлена на основі цього правила. Невдача розповсюдження через втручання джемперів у мережу є прикладом такого правила і буде використовуватися як частина нашого процесу виявлення.

Правило передачі / повторної передачі: моніторинг через вузол, що стосується кількості повідомлень, призначених для будь-якого з сусідів,

падає нижче очікуваної тривалості, оскільки вузли не пересилають повідомлення на наступний рівень. Три типи атак, які можна виявити за цим правилом, - це атака jamming, атака black hole та селективна атака переадресації. Під час цих атак зловмисник пригнічує деякі або всі повідомлення, які повинні були бути передані для переадресації, не даючи їм досягти призначеного місця в мережі.

Правило затримки: передача повідомлення сусідом монітора повинна відбуватися до визначеного тайм-ауту, інакше буде виявлена атака. Для запропонованого алгоритму ми розкриємо ці правила як частину нашого процесу реалізації. Ми визначаємо розповсюдження послідовності затримок через неправильну діяльність вузла під атакою jamming.

5.4 Алгоритм виявлення атаки

Складність алгоритму виявлення залежить від особливостей характеристики системи, яка є функцією багатьох комунікаційних особливостей. Для простоти ми представляємо наш розподілений метод, який відповідає чутливим, комунікаційним та обчислювальним можливостям бездротових сенсорних мереж. Наш алгоритм має послідовність прийому пакетів на основі вікна буфера.

Як було сказано раніше, завдяки етапам попереднього вибору статистику кожного вузла сусіда записують відповідно до швидкості передачі та прийому пакетів, тут для обчислення відповідної статистики використовується лише останній отриманий з N пакетів, а потім порівнюється з кожним прибуваючим пакетом, це зберігається в буфері пакетів довжиною L. Якщо отриманий пакет відповідає статистиці існуючих сусідів без будь-яких слідів порушень заздалегідь визначених правил, він приймається як звичайний і передається для використання для нових обчислень. Значення найстаріших пакетів видаляються зі списку за порядком

«перший війшов, перший вийшов» (FIFO) і записуються наступні метричні значення; час прибуття, відсутність пакету та потужність приймача.

Для того, щоб визначити швидкість аномалій в потужності приймача, ми встановлюємо межі, при яких мінімальні та максимальні значення одержуваних повноважень кожного пакету оновлюються для кожного прийому пакету. Відхилення від цих достовірностей (мінімальних і максимальних) меж означає аномалію. Аномальний пакет - це той, у якому отримані повноваження є нижче або вище меж довіри, що зараз знаходяться в буфері довжини *L*. Враховуючи попередньо визначені правила, зазначені вище, і для конкретного застосування, використовуючи розгортання вузла, тривогу про вторгнення можна підвищувати з кожною підозрою на аномальний пакет або виникнення послідовного числа аномалій, що демонструється отриманими пакетами. Дивитися рисунок 5.5, такі пакети є ізольованими, що складають список скомпрометованих вузлів (CNL) і зберігаються в новому буфері (буфер вторгнення) довжиною *L2* до прийняття рішення. На додаток до варіацій потужності передачі, швидкість, з якою були отримані пакети на основі нової послідовної довжини буфера *L2*, була представлена з використанням двох послідовних співвідношень швидкості надходження пакетів. Порівняння між співвідношенням швидкості *R2* та попередньою швидкістю *R1* визначається порогове значення *K* (рисунок 5.6). Порогове значення *K* відображає зміну шаблону вікна буфера з правилами вторгнення, що застосовуються для виявлення аномалії.

5.5 Виявлення аномалії

Наші запропоновані фази схеми виявлення розподілу вторгнень можуть бути узагальнені на основі таких припущень:

- Сенсорний вузол надсилає до сусідніх вузлів запит про стан вторгнення (або аномалії) після оповіщення про вторгнення.
- Кожен вузол, включаючи вузли ініціації, потім поширює інформацію

про стан, вказуючи на ймовірність вторгнення або неправильної поведінки сусіднього вузла.

- Кожен вузол, включаючи CH, може незалежно визначати, чи сукупний (розподільний) отриманий звіт вказує на вторгнення або аномалію та надсилає відповідь на базову станцію.

- Аномальна картина спостерігається з точки зору відхилень у потужностях передачі та надходженні пакетів.

- Будь-який вузол мережі, який виявляє вторгнення, зв'язується зі своїм k-сусідом і, нарешті, з CH для подальшого утримання атаки, а потім ініціює відповідь.

- Дії атаки та реагування на реалізацію можна спостерігати за допомогою моделювання.

- Нормальні дії та вторгнення мають чітку поведінку, яку видно на графіках мереж.

Таким чином, виявлення вторгнення включає захоплення даних та обґрунтування доказів, щоб визначити наявність нападу.

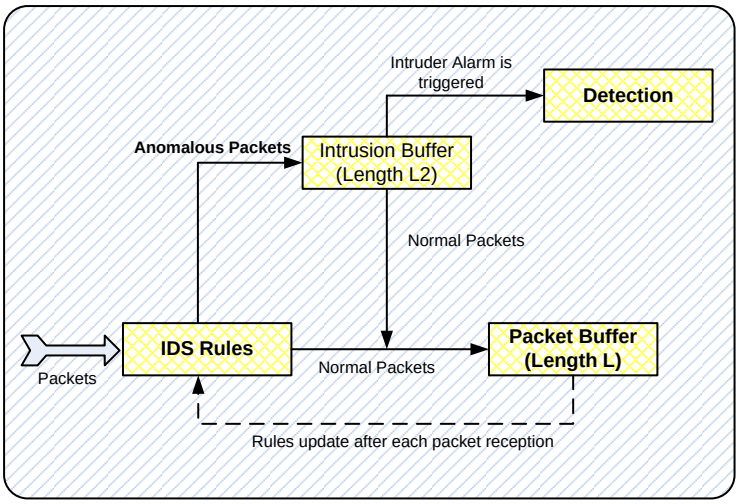


Рисунок 5.5 – Виявлення аномалії отриманої потужності

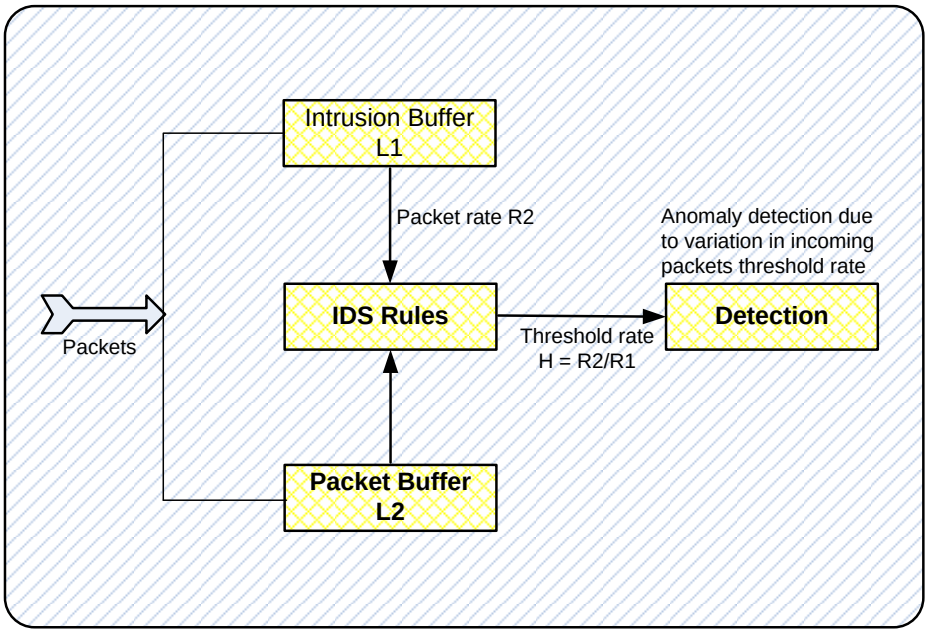


Рисунок 5.6 – Виявлення аномалії швидкості прибуття пакетів

6 ОЦІНКА ПРОДУКТИВНОСТІ СИСТЕМИ

6.1 Імітаційні моделі

Для оцінки працездатності механізму DIDS ми реалізуємо виявлення аномалії в мережевому симуляторі та проводимо ряд запусків моделювання за допомогою симулятора OPNET v14.5 [33]. Важливість цього моделювання полягає в оцінці ступеня ефективності нашого виявлення вторгнень шляхом спостереження за наявністю атаки заглушенням проти моделей передачі та прийому пакетів всередині мережі. Слідуючи нашому вибору функцій, заснованому на виявленні атаки вторгнення, ми розглядаємо різні атаки заглушення, про які ми говорили раніше, та вивчаємо вплив нашої схеми IDS на них відносно пропускної здатності мережі.

OPNET широко використовувався на основі прийнятного рівня впевненості у валідації результатів. Ми прийняли використання засобу моделювання OPNET для реалістичного аналізу та оцінки продуктивності нашої методики виявлення вторгнень. У нашій роботі наша мета полягає в моделюванні атаки заглушення (DoS), використовуючи повноваження передачі та прийому, а також зміни швидкості прильоту пакетів вузлів як частини наших слідів даних, щоб зробити висновки про аномальні структури при наявності таких атак.

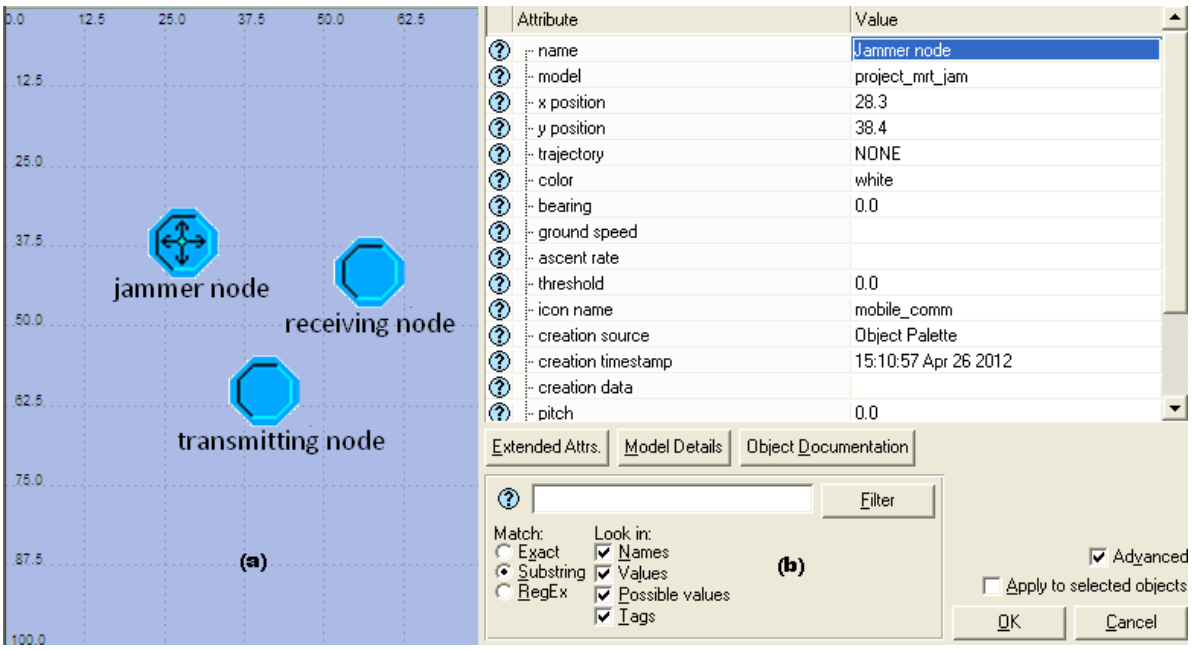
Відповідно до запропонованої нами схеми, OPNET забезпечує графічний інтерфейс користувача (GUI) для сценарію бездротової сенсорної мережі, який дозволяє реалістичне моделювання мереж за допомогою модуля збору даних про продуктивність, надаючи нам широке різноманіття середовищ моделювання.

6.2 Імітаційна модель OPNET

У цьому розділі ми представляємо наше середовище моделювання за допомогою інструментів моделювання OPNET, моделей бездротових вузлів, моделей мережі та моделей трафіку та їх атрибутів, що використовуються для нашого моделювання.

6.2.1 Мережева модель

Моделювання нашої схеми виявлення вторгнень за допомогою моделювання OPNET реалізовано на основі стандарту IEEE Wireless 802.15.4, що використовує рівні MAC та PHY. У цій моделі є два окремих сценарії; сценарій 1 складається з 3-х вузлів (вузол заглушки, один вузол передавача та один вузол приймача) в межах 100 м на 100 м, розміщених у фіксованому положенні для нашої навчальної послідовності, тоді як сценарій 2 складається з 12 вузлів (вузол заглушки, вузол передавача і приймач вузлів). Згодом усі вузли розподіляються випадковим чином у статичних положеннях у межах мережі 100 м на 100 м, як показано на рисунку 6.2. Розглянуто два типи топології мережі кластерів з використанням вузлів станції MANET; рівномірна топологія кластера та (запропонована DIDS) кластера. В обох налаштуваннях, як заслінкові вузли, так і законні приймальні (моніторингові та датчикові) вузли розгорнуті способом сенсорної мережі, і передбачається, що кожен вузол може спілкуватися зі своїм безпосереднім сусідом (к-симетричним) максимум на відстані не більше 300 м, як визначено стандартом IEEE802.15.4.



Рисунокк 6.1 – (а) сценарій мережі з 3 атрибутами вузла (б) бездротові вузли

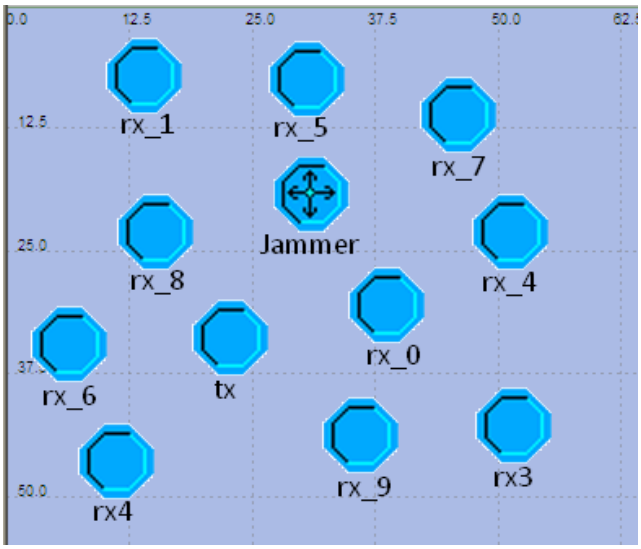


Рисунок 6.2 – Мережевий сценарій з 12 бездротовими вузлами

6.2.2 Модель вузла

Модель вузла, що використовується в нашому моделюванні, складається в основному з трьох моделей бездротових вузлів, що включають вузол заглушки, передавач і приймач, ці вузли підтримують загальні

атрибути з невеликими відмінностями на основі нашої модифікації. У цьому розділі ми представляємо лише вузли заглушки, як обговорювалося раніше в 3.1.1.1, є три різні типи вузлових замикань, отримані в бездротовому OPNET для нашого моделювання та оцінки, які включають; імпульсне заглушення, односмугове і .частотне.

Конфігурація моделі мережевого вузла аналогічна моделі вузла передавача і складається з модуля генератора пакетів, модуля радіопередавача та антенного модуля. Він налаштований так, як поводитися з нерухомим вузлом передавача, але з модифікаціями потужності каналу, модуляції сигналу та пропускної здатності. Вузол глушника створюється за допомогою процесора, радіопередавача та антенних об'єктів, пов'язаних по радіозв'язку під назвою пакетний потік, які динамічно встановлюються під час моделювання, але їх не видно в редакторі, як показано на рисунку 6.3 (а). Генератор пакетів генерує помилкові пошкоджені пакети і вводить радіо шум у мережу з простого джерела заглушення і використовує тип техніки модуляції, відомий як jammod, завдяки якому пакети приймаються модулем приймача як шум. Модель процесу була модифікована таким чином, щоб відображати нашу схему виявлення заглушення на основі типу глушника, використовуваного на рисунку 6.3 (б).

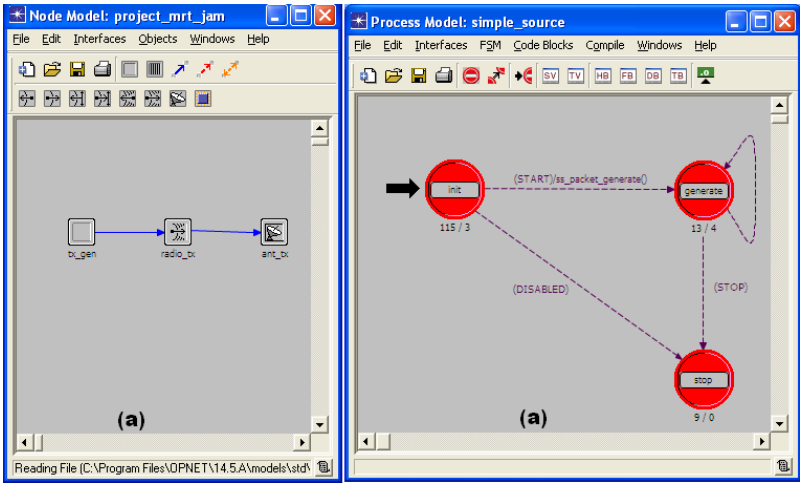


Рисунок 6.3 – (а) модель вузла глушника (б) модель технологічного процесу

6.2.3 Модель трафіка

У цьому моделюванні ми налаштовуємо нашу модель трафіку, необхідну для генерації атаки заглушенням з простого трафіку джерела глушника до вузлів призначення приймача. Трафік налаштований відносно типу заглушення, що використовується в різних сценаріях для генерації як експоненціальних, так і постійних розподілів пакетів. Зауважте, що для стаціонарного вузла ми не враховували траєкторію (рухливість), отже, траєкторія встановлена приблизно. Таким чином, ми встановлюємо атрибути бездротового вузла відповідно до наших специфікацій рівня MAC щодо наших правил вторгнення; вони відображаються на вузлах налаштувань бездротового каналу з початковою потужністю передачі, встановленою на 0,100 Вт, поріг потужності прийому пакетів-90 Вт, поріг RTS становить від 128 до 1024 байт.

Ці параметри представляють нашу навчальну послідовність із початковими значеннями. Модуль радіопередавача передає пакети до антени із рівнем потужності за замовчуванням 0,001 Вт з максимальною швидкістю передачі даних 1024 біт / с, використовуючи приблизно 100 відсотків його пропускної здатності каналу. Слідуючи нашому алгоритму виявлення та реалізованому в моделері Opnet, ми помічаємо, що для кожного пакета-кандидата, що надходить, модуль радіоприймача перекликається з декількома властивостями, щоб визначити, чи є середній показник похибки біту пакета (BER), потужність приймача, ніж визначений поріг, напраклад, якщо BER досить низький, пакет називається недійсним, класифікується як шум, надсилається в раковину і знищується.

Наші початкові порогові значення симуляції означають, що якщо пакет даних з розміром разом із MAC, напр. 28 байт перевищує цей поріг, він вимагає класифікації за рівнем MAC для доступу як дійсна передача, інакше пакет буде відкинутий. У наступних сценаріях ми змінюємо ці атрибути та

встановлюємо їх відповідно до вимог наших правил вторгнення та навантаження трафіку щодо розміру мережі.

Щоразу, коли пакет надходить з джерела трафіку заглушення, його поля встановлюються відповідно до генерації пакетів на основі змінених аргументів етапу RTP. Наприклад швидкість передачі даних (bps), час між прибутком (секунди), розмір пакету (байти), розмір буфера (біт) тощо, як показано на рисунку 6.4, потім пакет передається в модуль призначення радіоприймача, для якого вміст пакета буде узгоджено з вихідним джерелом трафіку від законного вузла передавача у разі виявлення та контролю помилок.

Якщо пакети, отримані у вузлі, напр. з потужністю менше 0,005 Вт (виникає під час нашого моделювання), це вважається шумом і не змінить статус модуля приймача на зайнятий, інакше більш високе значення потужності приймача, ніж цей поріг, вважатиметься дійсним. Якщо не буде змінено потужність передачі за замовчуванням, всі пакети WPAN повинні досягти пунктів призначення з достатньою потужністю, щоб бути дійсними пакетами з урахуванням відстані поширення.

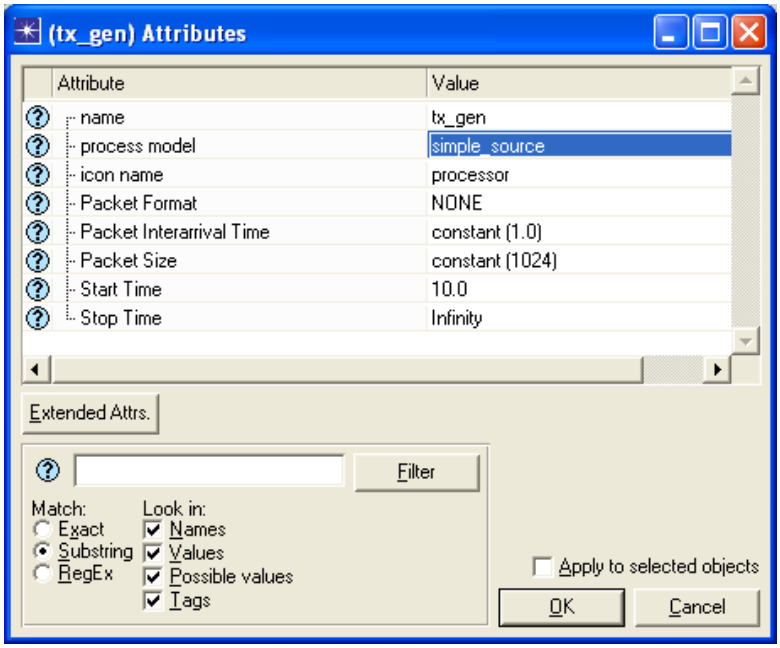


Рисунок 6.4 – Атрибути моделі вузла трафіку Jammer

6.3 Оцінка результатів моделювання

Щоб оцінити придатність нашого імітованого алгоритму виявлення вторгнень та виділити фактори, що впливають на процес виявлення, спочатку ми розглядаємо показники ефективності та основні статистичні дані при виявленні атак глушника для наших цілей оцінки. По-друге, ми провели ряд моделювання у двох різних сценаріях за різний проміжок часу, і, нарешті, представляємо відповідні результати нашого моделювання.

Пропускна здатність: це частка трафіку, правильно отримана приймачем радіоканалу, нормалізована до загальної потужності мережі. Таким чином, ми посилаємось на аномалії, зумовлені швидкістю надходження пакетів та варіаціями порогу потужності приймача як функції пропускної здатності мережі.

Метричний показник пропускної здатності обчислюється чисельно шляхом ділення загальної кількості пакетів, відправлених на час отримання першого пакету, мінус часу отримання останнього пакету. Ми використовуємо цей показник для оцінки можливостей виявлення нашої схеми виявлення за нормальних сценаріїв мережі та атаки.

Коефіцієнт доставки пакетів (PDR): коефіцієнт доставки пакетів представляє співвідношення між кількістю відправлених пакетів із рівня додатка та кількістю отриманих пакетів у вузлах призначення. PDR може вимірюватися двома способами [34]; або відправника, або одержувача, тоді як у відправника PDR можна обчислити, відслідковуючи, скільки підтверджень отримує від одержувача, з іншого боку, PDR одержувача може бути обчислений як відношення числа пакетів, які проходять перевірку циклічної надмірності (CRC) щодо кількості отриманих пакетів. Наше моделювання враховує PDR для оцінки виявлень та реакцій на заглушення в мережі.

Потужність прийнятого сигналу (RSP): обчислюється як функція відстані кластера між вузлом передавача та вузлом приймача проти коефіцієнта ослаблення або втрати шляху, маємо:

$$P_r = P_t / max(d, d0)\, fa \qquad (6.2)$$

Де P_t - потужність передавача

d - відстань між вузлами

fa - коефіцієнт загасання відносно відстані d0

У нашому моделюванні ми реалізуємо RSP як частину нашого алгоритму виявлення на основі аномалії живлення приймача, яка відображає класифікацію шаблону, наші результати оцінювали на підставі наступної статистики; співвідношення сигнал / шум, ймовірність помилки бітів і затримки в каналі передачі. Ми оцінюємо реакцію цих факторів за допомогою та без нападу глушником.

Утиліта: ми визначаємо корисність мережі як поєднання двох або більше показників. Ріст цього показника випливає з того, що для оптимізації мережі слід проводити спільний метричний аналіз для визначення відповіді щодо загальної суми накладних витрат. Для запропонованої нами схеми виявлення вторгнень ми визначаємо нашу утиліту за допомогою таких статистичних функцій: коефіцієнт сигналу / шуму, швидкість помилок бітів, затримка в кінці черги, час приходу, вірогідність виявлення, ймовірність успіху, позитивна ставка і хибнопозитивна ставка.

6.3.1 Сценарій 1: Нормальна реакція на рух

Перший сценарій, як зображено на рисунку 6.1 (a), був змодельований для контролю та виявлення ефекту нормального трафіку та заважання трафіку в рівномірному середовищі бездротової мережі. У цьому сценарії ми розглядаємо бездротову мережу (100x100) квадратних метрів з 3

бездротовими вузлами (Jammer, TX та RX), зазначеними раніше в моделі трафіку. Ми симулюэмо моделювання джерела атаки глушником частково із значеннями за замовчуванням за допомогою мережі моделі. Однодіапазонний трафік глушника з простого джерела заглушення генерується в мережі, що містить вузли одного передавача та приймача. У двох окремих режимах моделювання в середньому 2000-х ми моделюємо реакцію на вторгнення як у звичайному, так і в глушительному трафіку з відповіддю на пропускну здатність, середні пакети, що приймаються каналом радіоприймача, та швидкість потужності приймача. По-перше, ми моделюємо схему трафіку без жодного заглушення в мережі, використовуючи низькі рівні енергії за замовчуванням. Ми спостерігаємо за ефектом трафіку, що надсилається та отримується на окремому приймачі. По-друге, ми встановлюємо потужність передачі заслінки, використовуючи ті ж атрибути, що й інші вузли, і відстежуємо реакцію як у всій мережі, так і на окремому каналі приймача вузла, як показано на графіках нижче.

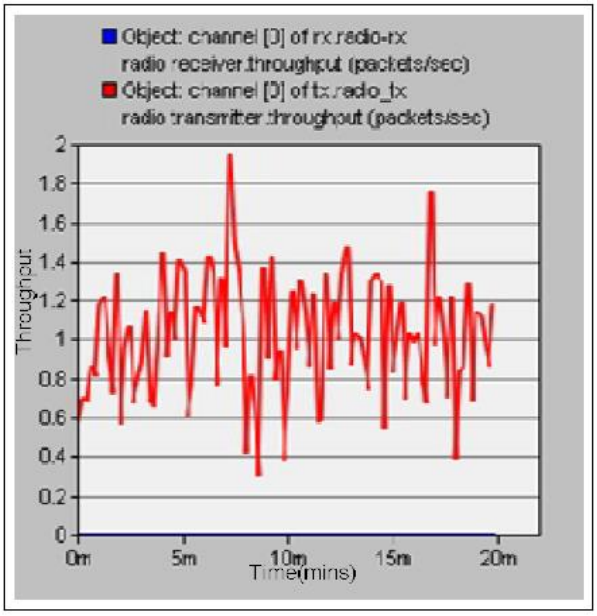


Рисунок 6.5 – Відповідь TX радіоканалу з надсиланням нормального трафіку

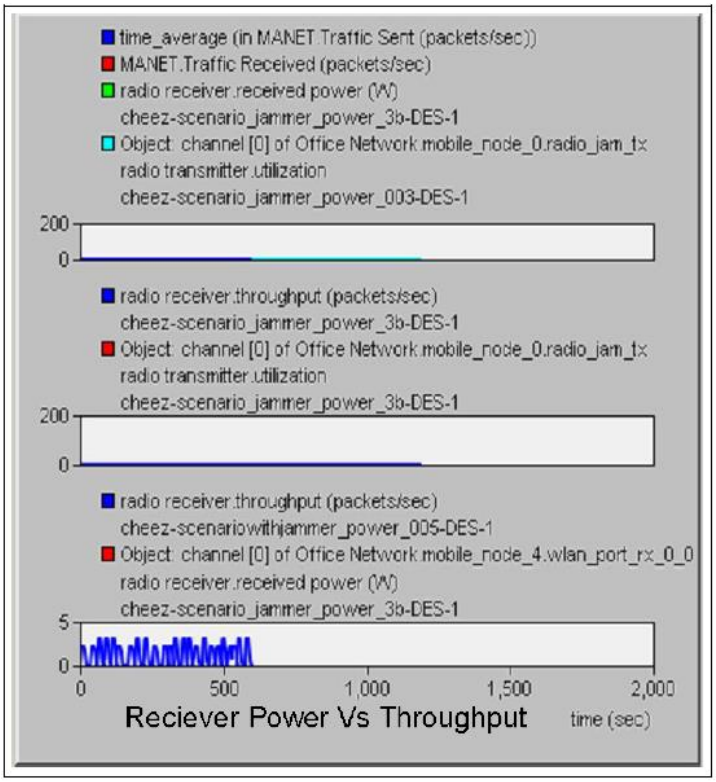


Рисунок 6.6 – Середня пропускна здатність каналу вузла приймача (атака заглушенням)

Сценарій 1: Аналіз продуктивності: на рисунку 6.5 показано нормальні схеми руху трафіку, що надсилається та приймається на радіоканалі без будь-якої форми атаки, тоді як на рисунку 6.6 показано наявність глушника на різних рівнях потужності зі зниженою пропускною здатністю. Це пов’язано зі збільшенням середньої потужності передачі та прийому, використовуючи швидкість експоненціальної передачі пакетів 1сек при 1024bps.

6.3.2 Сценарій 2: Зображення аномалії надходження пакетів

Після виконання моделювання в сценарії 1 ми вводимо сценарій 2 з більшим розміром мережі та пропонованим навантаженням. Цей сценарій складається з 10 спеціальних бездротових вузлів (9 вузлів монітора та 1 вузол глушника), розміщених випадковим чином у мережі площею 100x100 квадратних метрів з реактивним джерелом трафіку.

Потім ми застосували наше правило вторгнення таким чином, що вузли утворюють топологію кластера з кожним вузлом, слідуючи мінімальній відстані рівнів близько 50 м. Кожен вузол має тенденцію до передачі та прийому пакетів, підтримуючи тим самим оновлення маршруту сусіда. Для визначення ефекту схеми вторгнення на атаку заглушенням з використанням наших заздалегідь визначених показників було змодельовано в середньому 5 різних прогонів на 700s / 1hr20m у двох наборах моделювання відповідно.

У першому наборі моделювання ми припускаємо нормальну мережу заглушення, що використовує як імпульсний глушник, так і односмуговий та без правил виявлення вторгнень. За перші 5 запусків ми відключили певні атрибути вузлів монітора, які відіграють важливу роль у розподільній природі мережевих вузлів, такі як їх функції доступу, фізичні характеристики та методи модуляції. За допомогою цих атрибутів вузлам не потрібно підтримувати оновлення сусідів, що розповсюджуються або кооперативні. У другому запуску ми повертаємо конфігурації і потім реалізуємо наші алгоритми виявлення таким чином, що і вузол заглушення, і інші 9 мережевих вузлів приймають відносну потужність передавача і приймача. У той час як вузол використовує модуляцію джемода, вузли приймача були встановлені для використання методики модуляції бінарного фазового зсуву (BPSK) з фізичними характеристиками, встановленими для прямої послідовності та функціонування точки доступу. Ми зібрали нашу статистику на основі визначених вище функцій корисності; швидкість бітових помилок, співвідношення сигнал / шум і пропускної здатності мережі.

У другому наборі запуску моделювання інші параметри WPAN встановлюються на підвищені значення. Ми оцінюємо швидкість міжприбуткових пакетів на основі різних розмірів (128-1024 байт), використовуючи поріг вторгнення в буфер, щоб відповідати нашому алгоритму виявлення аномалій, описаному в главі 5.4, отже ми спостерігаємо ефект запропонованої нами схеми IDS в мережі та результати, показані відповідно.

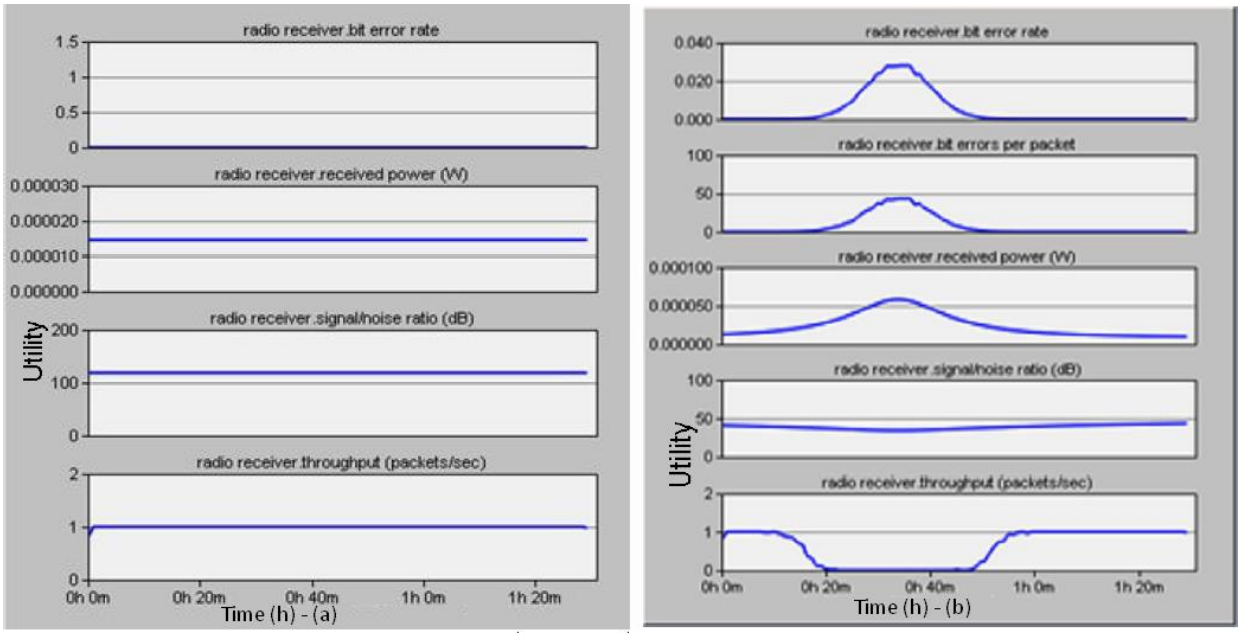


Рисунок 6.7 – Порівняння відповіді утиліти, що показує рівень успішності виявлення (а) без IDS (б) з IDS

Сценарій 2: Аналіз продуктивності: На рисунках 6.7 (а) (б) графіки показують реакцію виявлення атаки заглушення над утилітою мережі, можна помітити, що дуеметричні показники швидкості помилок бітів та потужності приймача значно посилюються майже вище 50% відмічається в деяких випадках при зниженні рівня співвідношення сигнал / шум, тоді як пропускна здатність приймача падає до нульових значень за часовий інтервал між 20-40 хвилин під атакою за схемою IDS. На рисунку 6.7 (б) імпульсний глушник вводиться в мережу, надсилає пакети з високим рівнем енергії так само, як і пакети передавача, на приймачі обидва пакети приймаються та порівнюються за аномальними схемами, виходячи з нашої схеми DIDS, одержувач класифікує пакет як недійсний, який має функції перешкод і шуму завдяки своїй техніці модуляції.

ВИСНОВКИ

Труднощі безпеки в сенсорних мережах головним чином пов'язані з обмеженнями, які накладаються простотою сенсорних пристроїв: обмежена потужність, обмежена пропускна здатність зв'язку та можливості обробки, а також невелика ємність пам'яті. У цій дипломній роботі ми зосередилися на вивченні та розробці розподілених алгоритмів безпеки для сенсорних мереж, які заважають зловмиснику отримати доступ до інформації, що направляється всередину, або ін’єктує шкідливі пакети. Ми також вивчали проблему виявлення зловмисника, коли запобіжні заходи не можуть досягти успіху.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. P. Techateerawat, and A. Jennings. Energy efficiency of intrusion detection systems in wireless sensor networks, 227 - 230 pp.

2. Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks, 275 – 283 pp.

3. C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami. Intrusion detection for routing attacks in sensor networks, 313 – 332 pp, 2006.

4. C. Perkins and E. Royer. Ad-hoc on demand distance vector routing, 90 p, 1999.

5. P. R. Da-Silva, M. H.T Martins, B. Rocha,A. Loureiro, L. Ruiz, and H. C. Wong. Decentralized Intrusion detection in wireless sensor network

6. Aravind Iyer, S. S. Kulkarni, Vive M, and Catherine P. Rosenberg. A taxonomy-based Approach to Design of Large-scale Sensor Networks. Kluwer, 2004.

7. D. E. D. Culler and M. Srivastava. Sensor networks an overview. August, 2004.

8. K. Casey, Security in wireless sensor networks. In department of computer science and Software Engineering, Auburn University.

9. T. Dimitriou and I. Krontiris. Autonomic communication security in sensor networks. Lecture Notes in Computer Science, 141- 152 pp, 2005.

10. A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. Security protocols for sensor networks. In mobile computing and networking, 189 – 199 pp, 2001.

11. J. Zheng and Myung J. Lee (2006). A comprehensive performance study of IEEE 802.15.4. Wiley Inter-science. IEEE press chapter 4. 218 - 237pp.

12. Jose A Gutirez et al. IEEE 802.15.4: A Developing for Low Rate Wireless Personal Area Network.

13. K. Casey. Security in wireless sensor networks. In department of computer science and software engineering, Auburn University.

14. W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks, 46 - 57 pp, 2005.

15. Li G. and He J. and Fu, Y. A group based intrusion detection scheme in WSN, Workshops, Washington, USA, IEEE computer society, 286 – 291 pp, 2008.

16. F. Freiling, I. Krontiris, and T. Dimitriou. Towards intrusion detection in WSNs, URL, http://pi1.informatik.uni- mannheim.de/ filepool/publications/krontiris-ew2007.pdf

17. T. Hai, and E Huh. Detecting selective forwarding attacks in WSN using two-hops neighbor knowledge, 325 – 331 pp, 2008.

18. I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos. Intrusion detection of sinkhole attacks in WSNs, 150–16, 2007.

19. J. Wang, G. Yang, Y. Sun, and S. Chen. Sybil attack detection based on RSSI for WSN, 2684 – 2687 pp, 2007.

20. M. Wen, H. Li, Y. Zheng, and K. Chen. TDOA-based sybil attack detection scheme WSN, Journal, 66 – 70 pp, 2008.

21. S. Axelsson. Intrusion detection systems: A survey and taxonomy Chalmers University of Technology, 2000.

22. U. Lindqvist and P. A. Porras. Detecting computer and network misuse through the production based expert system toolset (p-BEST) 146 - 161 pp, 1999.

23. H. S. Javitz and A. Valdes. The NIDES statistical component: SRI International, Menlo Park, CA, 1994.

24. C. Ko, M. Ruschitzka, and K. Levitt. Execution monitoring of security critical programs in distributed systems: A specification based approach. 175 - 187 pp, 1997.

25. O. Kachirski, R. Guha, D. Schwartz, S. Stoecklin, and E. Yilmaz, Case based agents for packet level intrusion detection in ad hoc networks, 315 – 320 pp, 2002.

26. I. Krontiris, T. Giannetsos, and T. Dimitriou. LIDeA: distributed lightweight intrusion detection architecture for sensor networks 1 – 10 pp, 2008.

27. A. Abbasi, M..I.Buhari ‘’A Multi-Layer Intruder Detection System for Multi-Hop Cluster-Based Sensor Networks, ´´ IEEE Proc.on Int´l.Conf.on Wireless Networks ICWN, June 26-29 2006.

28. A. Shajin Nargunam, M.P Sebastian Distributed Security Scheme for Mobile Ad-Hoc Networks; IEEE Int’l.166 -171 pp, 2006.

29. Y.Zhang et al. Intrusion detection techniques for mobile wireless networks 545 – 556 pp, 2003.

30. S.Salvador, P.Chan and J.Brodie. Learning and rules for rime series anomaly aetection. 300 - 305 pp, 2004.

31. I.Onat, A. Miri. An intrusion detection system for wireless sensor networks. Network and Comm.Vol.3, August, 2005.

32. K.Ioannis, T.Dimitrou, and F.C Freiling. Towards intrusion detection in wireless sensor networks. 3th European Conference on WSN (EWSN’07) Paris, 2007.

33. W.Xu, W.Trappe, Y.Zhang, and T.Wood, The feasibility of launching and detecting jamming attacks in wireless networks, 46-57 pp, 2005.