ДОДАТОК А

Графічний матеріал атестаційної роботи

Харківський університет радіоелектроники

Кафедра електронних обчислювальних машин

Система виявлення вторгнень у бездротових сенсорних мережах

Студент групи КСМм-19-1 Попазов А.А.

Керівник проф. кафедри ЕОМ, к.т.н. Горбачов В.О

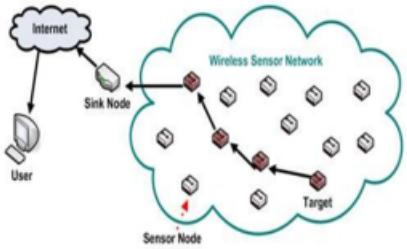
Харьков 2020

Задачі дослідження:

1. Аналіз проблем безпека Wireless Sensor Networks (WSN)
2. Аналіз сучасних систем виявлення вторгнень (IDSs)
3. Використання розподілених систем виявлення вторгнень (DIDSs) .
4. Оцінка ефективності розподілених систем виявлення вторгнень (DIDSs) .

Огляд WSN

- Складається з невеликих недорогих ресурсних обмежених вузлів датчиків (мотивів)
- Моніторинг та повідомлення про певне явище
- Зловмисник може вводити помилкові пакети даних, змінювати оригінальні пакети даних
- Зловмисник також може порушити вузли датчиків

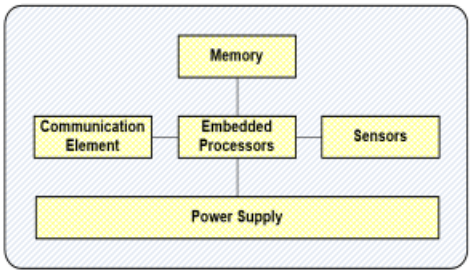


3

Застосування та компоненти WSN

Застосування

Оборонна промисловість
Цивільна Промисловість
Сільське господарство
Моніторинг навколишнього середовища
Розумний дім
Охорона здоров'я / Медицина
Транспорт

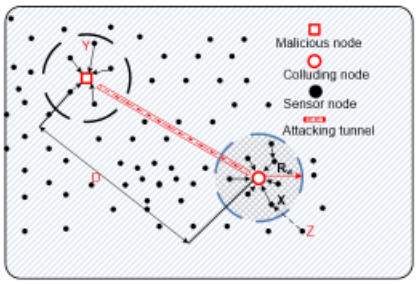


Компоненти Wireless Sensor Networks

Датчики
Блок зондування
Обробний блок
Блок пам'яті
Процесорний блок
Блок живлення
Бездротовий передавач / приймач

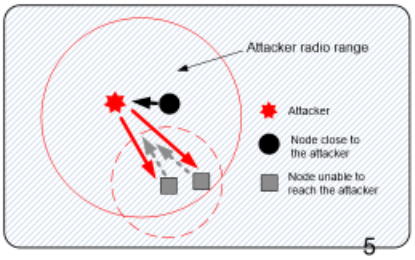
4

Типи атак на Wireless Sensor Networks(1/4)



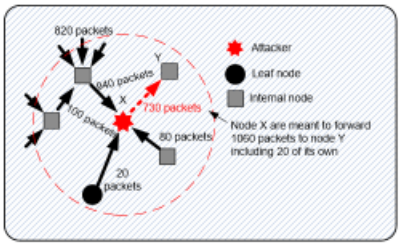
Атака типу черв'як

Атака типу Hello flood



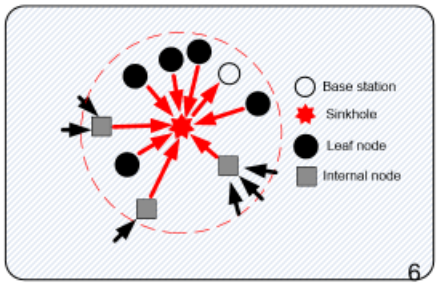
5

Типи атак на Wireless Sensor Networks (2/4)



Атака типу вибіркова переадресація

Атака типу Sinkhole



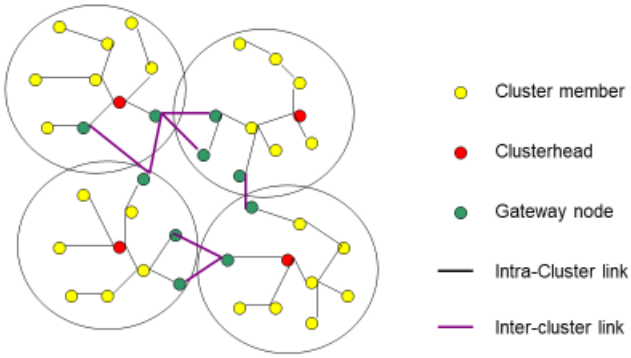
6

Методи виявлення вторгнень та їх класифікацію

Методи виявлення вторгнень
Виявлення зловживання
Виявлення аномалії
Виявлення на основі специфікації

Класифікація виявлення вторгнень
Автономний IDS
Розподілена та кооперативна IDS
Ієрархічна IDS
IDS мобільного агента

Архітектура на основі кластерів



Кластерна мережа поділяється на підмножини вузлів.

Кожна група вузлів містить одного лідера (cluster head) і кілька звичайних вузлів (cluster member)

Кластеризація в WSN

Кластеризація полягає в наступному:

- Групуванні вузлів у кластери та виборі головкою кластера (CH) Члени кластеру можуть безпосередньо спілкуватися зі своїм CH
- Головний кластер може пересилати зведені дані до центральної базової станції через інші Головні кластери

Мета кластеризації:

- Дозволяє агрегування
- Обмежує передачу даних
- Сприяє повторному використанню ресурсів
- Головні кластери і вузли шлюзу можуть утворювати віртуальну магістраль для міжкластерної маршрутизації
- Структура кластера 1)зменшує меншої розміри мережі та підвищує стабільність мережі 2) Підвищує термін служби мережі

9

Алгоритм створення кластера

Запропонована схема Distributed Intrusion Detection System (DIDS) відповідає трифазній структурі процесу впровадження.

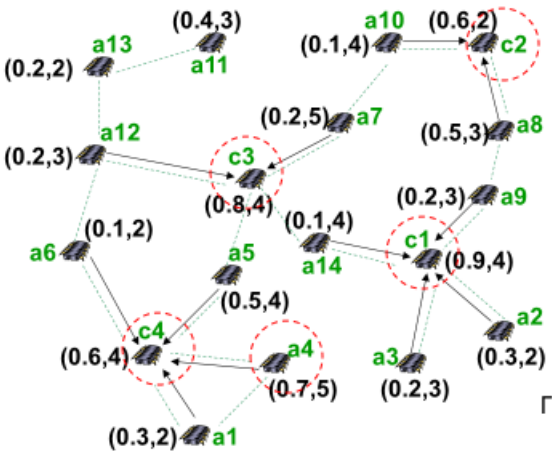
1. По-перше, ми використовуємо алгоритм кластеризації з формуванням голови кластера,

2. потім - фаза виявлення сусідів після спільного поширення інформації,

3. по-третє, алгоритм виявлення атаки на основі пов'язаних атак та класифікацій нормальних та аномальних профілів з урахуванням процесу атаки.

10

Приклад кластера



Виявлення сусідів

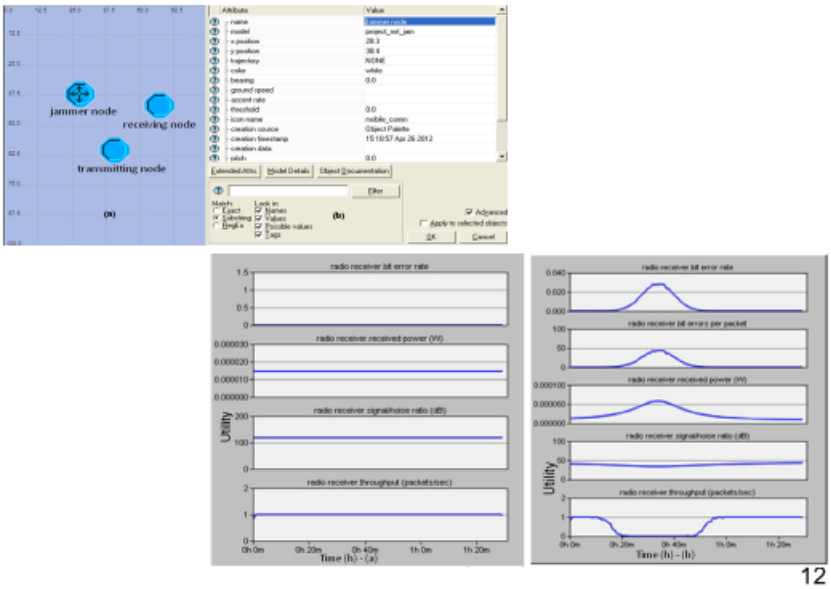
Обрати голову кластера

Розв'язання зв'язків

Голову кластера обрано

11

МОДЕЛЮВАННЯ ТА РЕЗУЛЬТАТИ



12

ВИСНОВКИ

- Безпека в WSN значно відрізняється від традиційної (дротової) мережі
- Обмеження та відкриті середовища бездротових сенсорних мереж роблять безпеку цих систем складною.

ДОДАТОК Б

Система моделювання Opnet

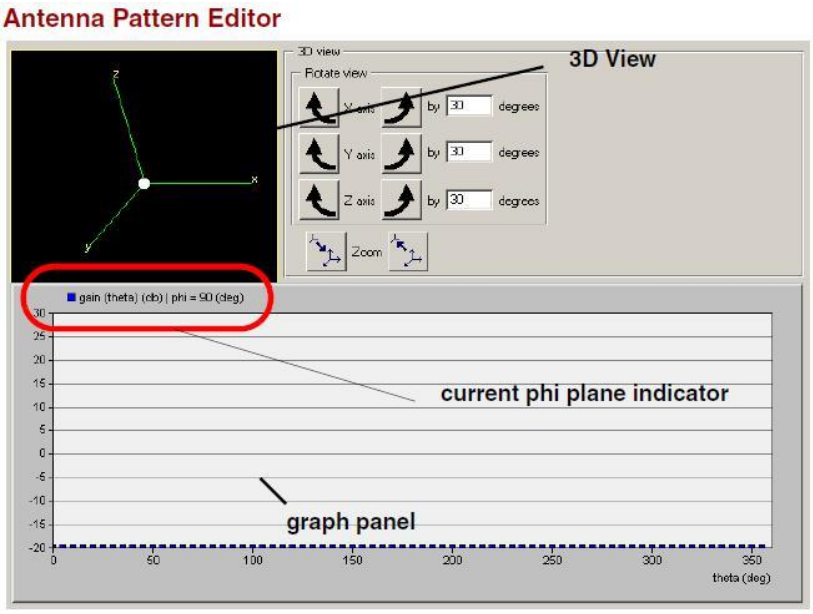


Рисунок Б.1 – Інтерфейс системи

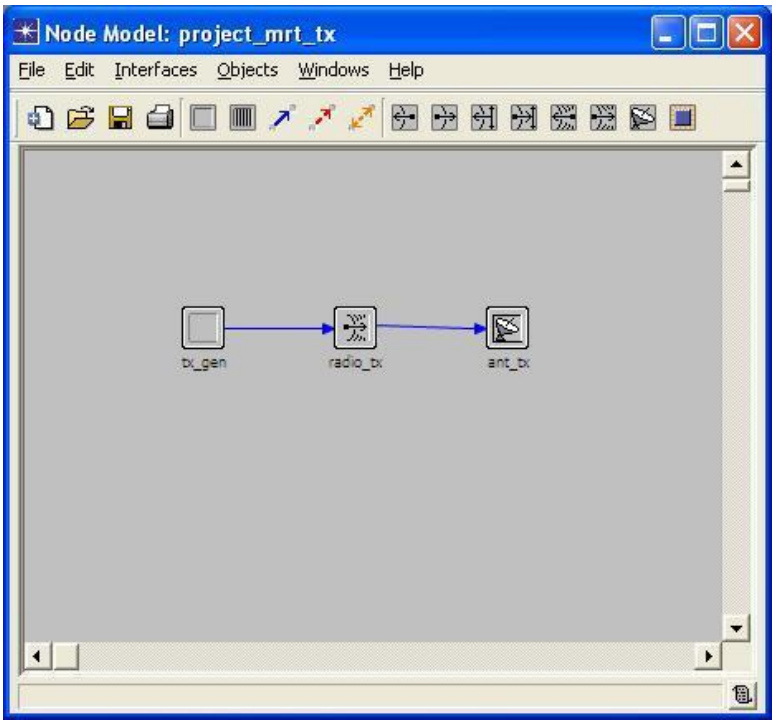


Рисунок Б.2 – Інтерфейс системи

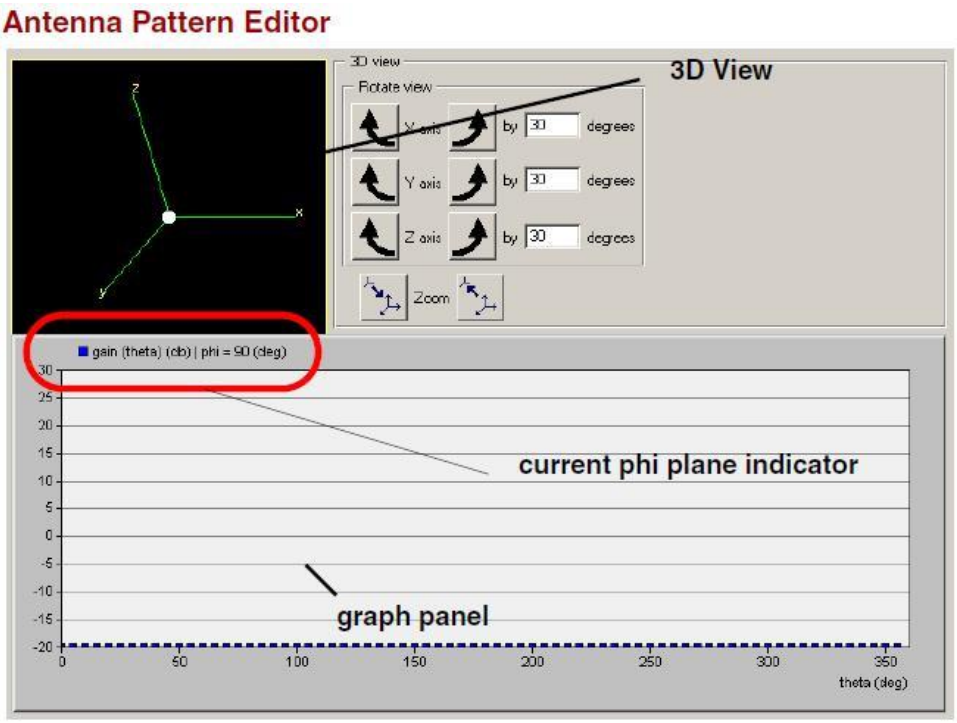


Рисунок Б3 – Інтерфейс системи

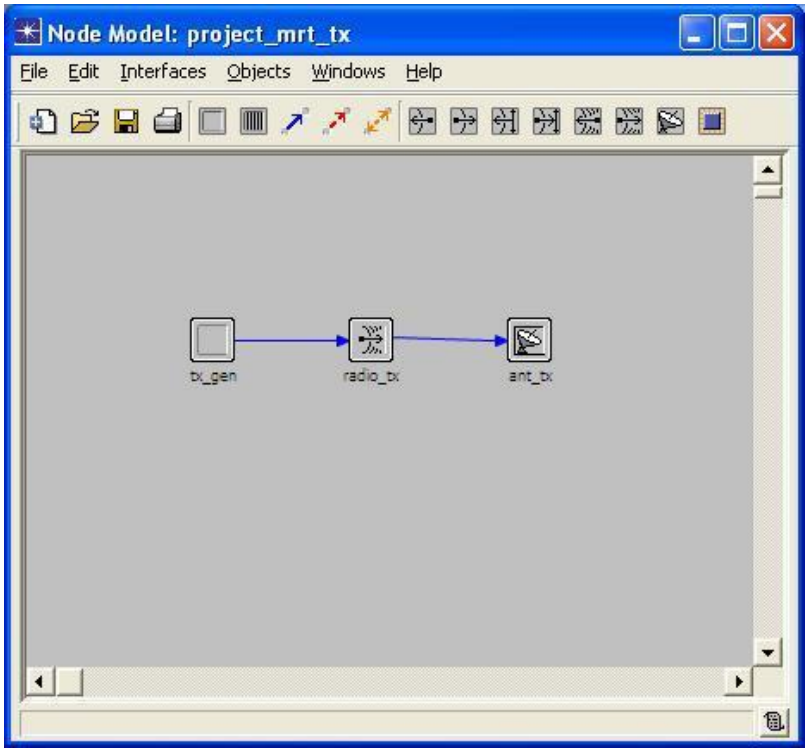


Рисунок Б.4 – Інтерфейс системи

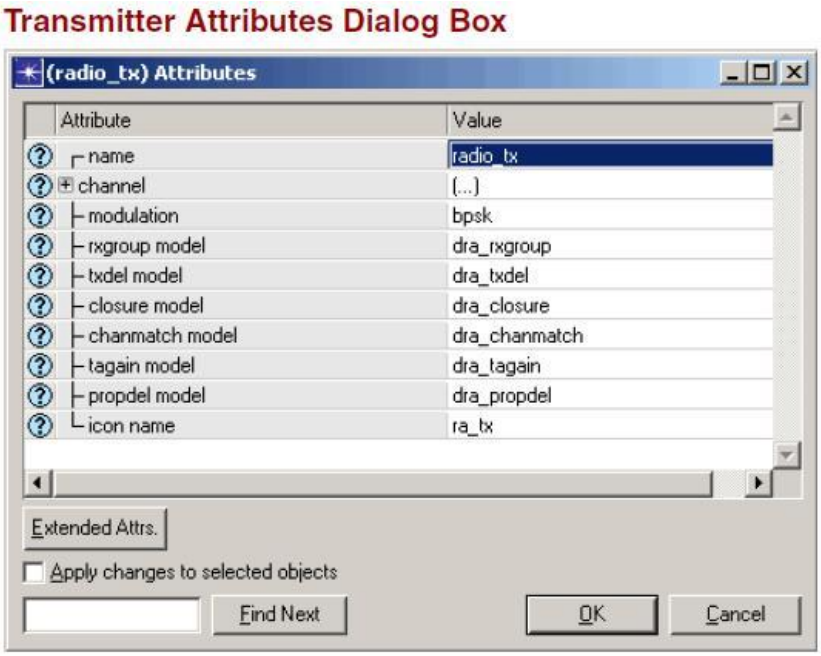


Рисунок Б.5 – Інтерфейс системи

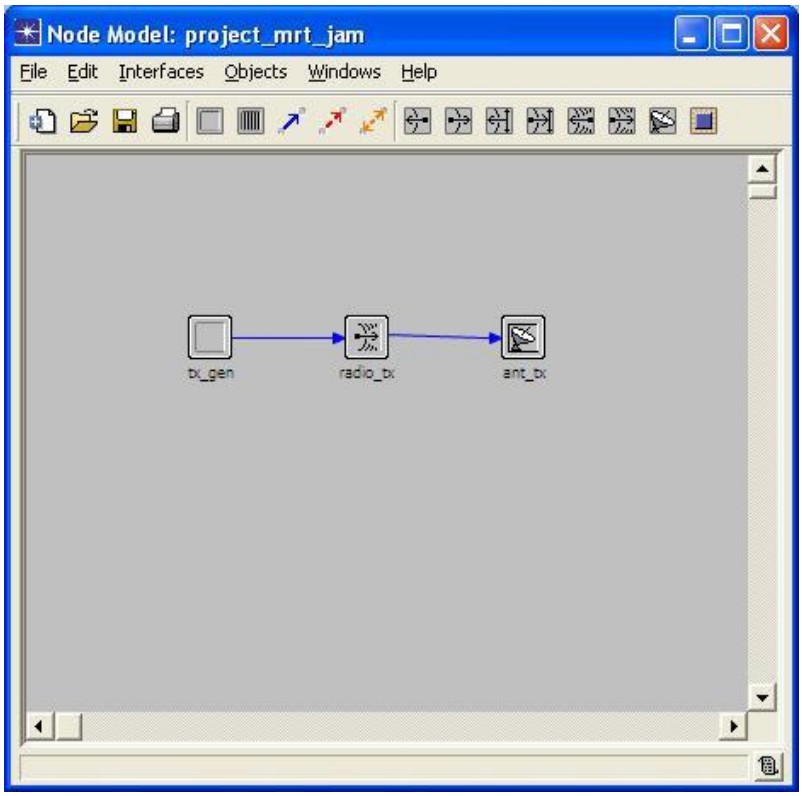


Рисунок Б.6 – Інтерфейс системи

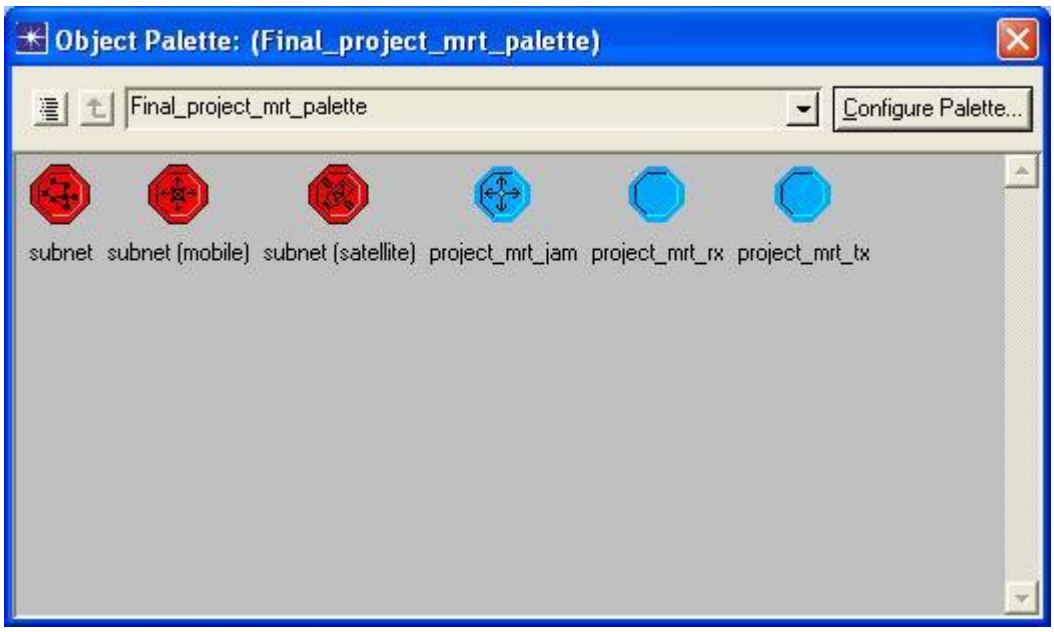


Рисунок Б.7 – Інтерфейс системи