МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 11.00.00.000 ПЗ

Група ІПм-23-1

Грицюк Іван

2024

Івано-Франківський національний технічний університет нафти і газу

Інститут інформаційних технологій

Кафедра інженерії програмного забезпечення

Грицюк Іван Іванович

(прізвище, ім'я, по батькові)

УДК 004.94

(індекс)

МАГІСТЕРСЬКА РОБОТА

Моделі побудови багатовекторної програмної системи виявлення вторгнень

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Грицюк І.І.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Пасєка Надія Мирославівна, к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

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

Івано-Франківськ – 2024

Івано-Франківський національний технічний університет нафти і газу

Інститут інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доц. В.В. Бандура
“ 04 ” вересня 2024 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Грицюку Івану Івановичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ Моделі побудови багатовекторної програмної системи виявлення вторгнень”

керівник проекту (роботи) Пасєка Надія Мирославівна, к.т.н., доцент

затверджені наказом закладу вищої освіти від “ 22 ” листопада 2024 р. № 781/7

2. Строк подання студентом проекту (роботи) 15 грудня 2024 р.

3. Вихідні дані до проекту (роботи) Теоретичні концепції та формальні моделі побудови та інформаційних та програмних технологій виявлення вторгнень

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1. Дослідження предметної області виявлення вторгнень та атак на програмні системи
2. Моделі та алгоритми забезпечення криптографіного захисту
3. Імплементація моделей для побудови багатовекторної системи виявлення вторгнень
4. Представлення схеми гібридної системи виявлення вторгнень

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Базова архітектура системи виявлення вторгнень (IDS) (рис. 1.1)
2. Огляд багатовекторної портативної системи виявлення вторгнень (MVP-IDS) (рис. 1.2)
3. Алгоритм криптографії із закритим ключем (рис. 2.1)
4. Алгоритм криптографії з відкритим ключем (рис. 2.2)
5. Процес генерації MAC для автентифікації повідомлень (рис. 2.3)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2024 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	15.09.2024	виконано
2	Аналіз концепцій та алгоритмів предметної області	29.09.2024	виконано
3	Дослідження предметної області виявлення вторгнень та атак на програмні системи	15.10.2024	виконано
4	Моделі та алгоритми забезпечення криптографіного захисту	08.11.2024	виконано
5	Імплементація моделей для побудови багатовекторної системи виявлення вторгнень	20.11.2024	виконано
6	Представлення схеми гібридної системи виявлення вторгнень	01.12.2024	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	15.12.2024	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 81 с., 24 рис., 3 табл., 54 джерел.

Тема: Моделі побудови багатовекторної програмної системи виявлення вторгнень

Об'єкт дослідження: процеси виявлення загроз та атак у програмних системах, зокрема в мобільних пристроях та бездротових мережах.

Мета роботи: дослідити методи побудови багатовекторної програмної систему виявлення вторгнень, яка поєднує сигнатурні та аномалійно-орієнтовані методи для підвищення ефективності виявлення загроз, особливо у мобільних пристроях та бездротових мережах.

Предмет дослідження: методологія, моделі та алгоритми побудови багатовекторної програмної системи виявлення вторгнень, що використовує сигнатурні методи в поєднанні з алгоритмами машинного навчання.

Результати дослідження

Розроблено багатовекторну методологію виявлення загроз, яка поєднує сигнатурні підходи, що забезпечує високу точність виявлення нових загроз та запропоновано концепцію та модуль виявлення атак на основі Bluetooth, що дозволяє ідентифікувати широкий спектр загроз у бездротових мережах.

Висновок

Результати дослідження можуть бути використані для розробки систем захисту інформаційних систем у різних сферах, зокрема в бізнесі та медичних установах, де важливим є забезпечення конфіденційності та захисту даних.

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, БАГАТОВЕКТОРНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИГНАТУРНЕ ВИЯВЛЕННЯ, АНОМАЛІЙНЕ ВИЯВЛЕННЯ, БЕЗПЕКА BLUETOOTH, МОБІЛЬНІ ПРИСТРОЇ, ВИЯВЛЕННЯ ЗАГРОЗ.

ABSTRACT

Master Thesis: 81 pp., 24 fig., 3 tab., 54 sources.

Thesis Subject: Models for building a multi-vector intrusion detection software system

The object of research: the processes of detecting threats and attacks in software systems, in particular in mobile devices and wireless networks.

The purpose of the work: to investigate the methods of building a multi-vector software intrusion detection system that combines signature and anomaly-oriented methods to improve the effectiveness of threat detection, especially in mobile devices and wireless networks.

Research subject: methodology, models and algorithms for building a multi-vector intrusion detection software system that uses signature methods in combination with machine learning algorithms.

Research results

A multi-vector threat detection methodology has been developed, which combines signature approaches, which ensures high accuracy of new threat detection, and a concept and a Bluetooth-based attack detection module have been proposed, which allows the identification of a wide range of threats in wireless networks.

Conclusion

The results of the research can be used for the development of information systems protection systems in various areas, in particular in business and medical institutions, where it is important to ensure confidentiality and data protection.

INTRUSION DETECTION SYSTEM, MULTI-VECTOR INTRUSION DETECTION SYSTEM, SIGNATURE DETECTION, ANOMALITY DETECTION, BLUETOOTH SECURITY, MOBILE DEVICES, THREATS DETECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

PDAs - Personal Digital Assistants

PIDs - Portable Information Devices

IDS - Intrusion Detection System

B-SIPS - Battery-Sensing Intrusion Protection System

MVP-IDS - Multi-Vector Portable - Intrusion Detection System

IC - instantaneous current

BADSS - Bluetooth Attack Detection and Signature System

DTC Dynamic Threshold Calculation

SAs - security administrators

WAP - Wireless Access Point

ВСТУП

Актуальність теми.

Сучасні інформаційні системи є вразливими до численних загроз у вигляді кібератак та вторгнень, особливо в умовах постійного розвитку технологій та збільшення кількості підключених пристроїв. Зокрема, мобільні пристрої, системи з підтримкою Bluetooth та інші бездротові мережі стають ціллю для атак, що зумовлює необхідність вдосконалення систем виявлення вторгнень. Традиційні методи виявлення загроз мають обмеження, особливо щодо виявлення нових та складних типів атак. Тому розробка багатовекторної портативної системи виявлення вторгнень (MVP-IDS), яка поєднує сигнатурні та аномалійно-орієнтовані методи з використанням алгоритмів машинного навчання, є актуальною для забезпечення надійного захисту інформаційних систем.

У сучасному цифровому світі кількість підключених до мережі пристроїв стрімко зростає, що створює нові виклики для забезпечення безпеки інформаційних систем. Різноманітні загрози, такі як кіберзлочинність, хакерські атаки та несанкціоноване проникнення, ставлять під загрозу конфіденційність, цілісність та доступність даних. Особливу небезпеку становлять атаки на мобільні пристрої та бездротові мережі, які все більше використовуються в різних сферах, включаючи бізнес, медицину та приватне життя. Зокрема, технології на основі Bluetooth та Wi-Fi є важливою складовою таких мереж, але вони також вразливі до атак, спрямованих на перехоплення та маніпуляцію даними.

Традиційні системи виявлення вторгнень (IDS) мають обмежені можливості виявлення нових та складних типів загроз, що еволюціонують разом із розвитком технологій. Це особливо актуально в умовах широкого використання мобільних пристроїв, які через свої обмежені ресурси (потужність процесора, пам'ять) потребують ефективних рішень для захисту. Тому вдосконалення методів виявлення вторгнень із використанням

гібридних підходів, що поєднують сигнатурне та аномалійне виявлення, а також інтеграцію методів машинного навчання, є важливим напрямом у забезпеченні надійного захисту інформаційних систем.

Значення даної теми зростає на фоні швидкого поширення Інтернету речей (IoT) та розширення можливостей мобільних технологій, де кожен новий пристрій є потенційною вразливою точкою для кіберзлочинців. В умовах зростання обсягу цифрових даних та підвищення вимог до їхньої безпеки, дослідження та розробка нових моделей багатовекторної системи виявлення вторгнень (MVP-IDS) є актуальним завданням. Такі рішення дозволяють виявляти та нейтралізувати нові типи загроз завдяки комплексному аналізу поведінки мережевих та програмних компонентів.

Таким чином, актуальність дослідження зумовлена необхідністю створення нових підходів до виявлення загроз та забезпечення безпеки мобільних пристроїв і бездротових мереж, що дозволить знизити ризики несанкціонованого доступу та підвищити рівень захисту конфіденційної інформації.

Мета дослідження – дослідити методи побудови багатовекторної програмної систему виявлення вторгнень, яка поєднує сигнатурні та аномалійно-орієнтовані методи для підвищення ефективності виявлення загроз, особливо у мобільних пристроях та бездротових мережах.

Об’єкт дослідження - процеси виявлення загроз та атак у програмних системах, зокрема в мобільних пристроях та бездротових мережах.

Предмет дослідження - методологія, моделі та алгоритми побудови багатовекторної програмної системи виявлення вторгнень, що використовує сигнатурні методи в поєднанні з алгоритмами машинного навчання.

Відповідно до мети роботи було сформовано наступні **задачі:**

- Проаналізувати існуючі методи та системи виявлення вторгнень, їх переваги та недоліки.
- Дослідити особливості побудови багатовекторної системи виявлення вторгнень.
- Розробити та вдосконалити методологію MVP-IDS для виявлення загроз у мобільних пристроях.
- Розробити схему гібридної системи виявлення вторгнень з використанням методів машинного навчання.
- Реалізувати концепцію виявлення атак на основі Bluetooth та розробити модуль виявлення загроз у бездротових мережах.
- Провести тестування та оцінити ефективність запропонованих моделей та алгоритмів виявлення загроз.

Методи дослідження.

- Методи аналізу та синтезу для вивчення існуючих підходів до виявлення вторгнень.

- Математичне моделювання для розробки алгоритмів виявлення загроз.

- Методи машинного навчання для побудови гібридних моделей виявлення вторгнень.

- Емпіричне тестування для оцінки ефективності розроблених рішень у різних умовах.

Наукова новизна отриманих результатів

Розроблено багатовекторну методологію виявлення загроз, яка поєднує сигнатурні підходи, що забезпечує високу точність виявлення нових загроз та запропоновано концепцію та модуль виявлення атак на основі Bluetooth, що дозволяє ідентифікувати широкий спектр загроз у бездротових мережах.

Практичне значення магістерської роботи

Результати дослідження можуть бути використані для розробки систем захисту інформаційних систем у різних сферах, зокрема в бізнесі та медичних установах, де важливим є забезпечення конфіденційності та захисту даних. Запропонована система виявлення вторгнень може бути інтегрована в існуючі програмні рішення для підвищення їх безпеки та ефективності.

Структура магістерської роботи. Робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 81 сторінку, і містить 24 рисунки, 3 таблиці, список використаних джерел із 54 найменувань.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА АТАК НА ПРОГРАМНІ СИСТЕМИ

1.1. Опис середовища дослідження та систем виявлення вторгнень

Персональні цифрові помічники (PDA - Personal Digital Assistants) і смартфони, також відомі як портативні інформаційні пристрої (PID - Portable Information Device), є менш потужними в обчислювальному відношенні, ніж настільні та портативні персональні комп'ютери (ПК), але мають багато тих самих функцій і мають багато тих самих функцій. Двома визначальними функціями, включеними до PID, є можливості IEEE 802.11 (Wi-Fi) і IEEE 802.15.1 (Bluetooth). Незважаючи на те, що вони подібні, багато базових заходів безпеки, поширених у ПК, відсутні в PID, насамперед через обмежені ресурси живлення та циклу обчислень. Це дослідження показує, що додавання системи виявлення вторгнень (IDS - Intrusion Detection System) до PID може значно підвищити їх безпеку.

Це дослідження спрямоване на безпеку мобільних пристроїв і розширює оригінальну концепцію Battery-Sensing Intrusion.

Battery Sensing Intrusion (втручання в систему вимірювання батареї) – це термін, який використовується для опису будь-якого несанкціонованого доступу або маніпуляції з системою, яка відповідає за моніторинг стану батареї пристрою. Це може включати як фізичний доступ до самої батареї, так і хакерські атаки на програмне забезпечення, яке керує її роботою.

Ось декілька причин чому це небезпечно:

- Неправильна інформація про стан батареї: Зловмисник може підробити дані про рівень заряду батареї, що призведе до несподіваних відключень пристрою або, навпаки, до помилкового повідомлення про низький заряд.

- Швидке розряджання батареї: Шкідливе програмне забезпечення може збільшити споживання енергії пристроєм, що призведе до його швидкого розряджання.

- Пошкодження батареї: Втручання в систему може призвести до перегріву або короткого замикання батареї, що може спричинити її пошкодження або навіть пожежу.

- Викрадення даних: У деяких випадках, система вимірювання батареї може бути пов'язана з іншими системами пристрою, що дозволяє зловмисникам отримати доступ до конфіденційної інформації.

Важливо розуміти, що абсолютна захищеність від всіх можливих загроз неможлива. Однак, дотримуючись певних рекомендацій, користувач зможе значно знизити ризик втручання в систему вимірювання батареї портативного пристрою.

Від часу розробки першої моделі для виявлення вторгнень було запропоновано численні системи виявлення вторгнень (IDS) як у науковому, так і в комерційному середовищі.

Незважаючи на значну різноманітність технічних підходів, які застосовуються цими системами для збору та аналізу даних, більшість з них базуються на відносно загальній архітектурній структурі (рис. 1.1), що складається з наступних компонентів:

- Пристрій збору даних (сенсор) відповідає за збір інформації з моніторингової системи.

- Детектор (двигун аналізу виявлення вторгнень (ID)) обробляє дані, зібрані від сенсорів, для ідентифікації втручальних дій.

- База знань (база даних) містить інформацію, зібрану сенсорами, але у попередньо обробленому форматі (наприклад, база знань про атаки та їхні сигнатури, відфільтровані дані, профілі даних тощо). Ця інформація зазвичай надається мережевими та безпековими експертами.

- Пристрій конфігурації надає інформацію про поточний стан системи виявлення вторгнень (IDS).

- Компонент відповіді ініціює дії, коли виявлено вторгнення. Ці відповіді можуть бути або автоматизованими (активними), або включати взаємодію людини (неактивними).

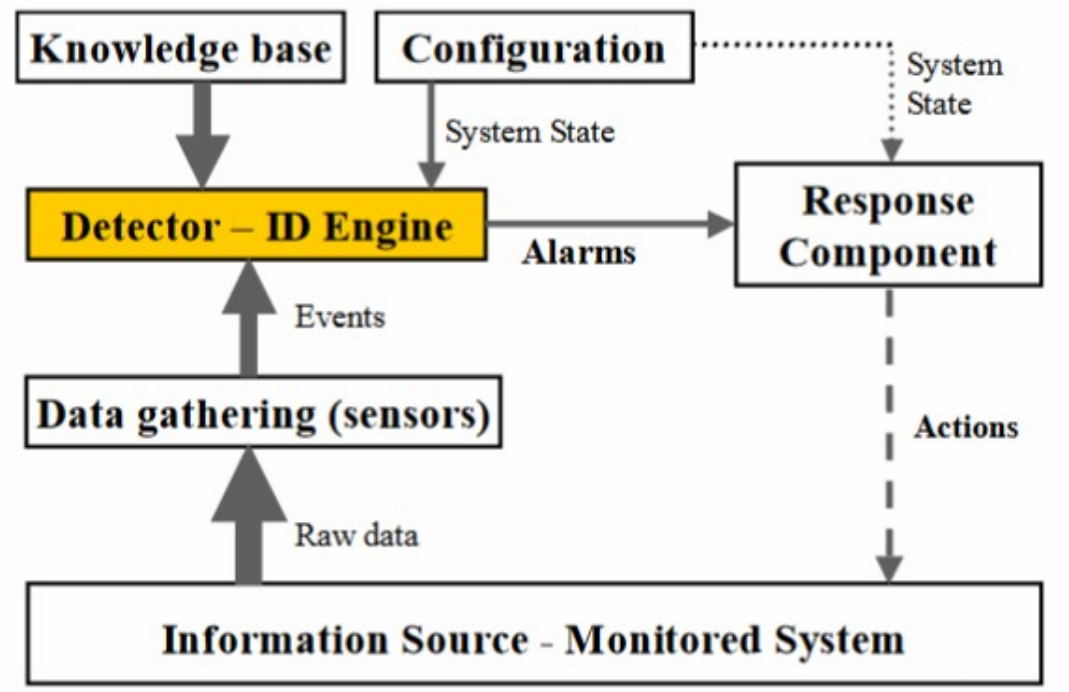

Рис. 1.1. Базова архітектура системи виявлення вторгнень (IDS)

Стратегія аналізу визначає характеристики детектора (двигун виявлення вторгнень з рис. 1.1). Коли IDS виявляє події або набори подій, що відповідають попередньо визначеному шаблону відомої атаки, ця стратегія аналізу називається виявленням зловживань. Якщо ж IDS ідентифікує вторгнення як незвичайну поведінку, відмінну від нормальної поведінки моніторингової системи, така стратегія аналізу називається виявленням аномалій.

Часові аспекти використовуються для класифікації IDS на онлайн-IDS, які виявляють вторгнення в режимі реального часу, та офлайн-IDS, що зазвичай спочатку зберігають моніторингові дані, а потім аналізують їх у пакетному режимі для виявлення ознак вторгнення.

Архітектура IDS дозволяє розрізняти централізовані IDS, які аналізують дані, зібрані лише з однієї моніторингової системи, та розподілені

IDS, що збирають інформацію з кількох моніторингових систем для дослідження глобальних, розподілених та скоординованих атак.

Система захисту (B-SIPS) [1] розроблена шляхом представлення багатовекторної портативної системи виявлення вторгнень (MVP-IDS). MVP-IDS перевіряє повідомлення про аномальне розрядження батареї від клієнтів B-SIPS із Wi-Fi у режимі реального часу та трафік Bluetooth з використанням модулів виявлення сигнатур атаки. Щоб співвіднести аномалії миттєвого струму (IC) із трафіком атак Wi-Fi та Bluetooth, MVP-IDS інтегрує виявлення аномалій B-SIPS із системами відповідності на основі сигнатур Snort [2] і системою Bluetooth Attack Detection and Signature.

У медичній промисловості нові пристрої дають пацієнтам змогу покращити стан здоров’я завдяки використанню імплантованих пристроїв. Ці пристрої можуть контролювати фізіологічні умови в організмі та передавати інформацію на віддалені точки моніторингу для аналізу даних і повторного калібрування пристрою [3]. Деякі з цих імплантованих пристроїв включають кардіостимулятори, дефібрилятори, системи доставки ліків, слухові апарати, епілептичні монітори мозку та нейростимулятори [3, 4]. Іншим застосуванням бездротового зв’язку в галузі медицини є використання комп’ютерних чіпів із підтримкою Bluetooth, вбудованих у протези кінцівок для контролю рухів суглобів [5]. Незважаючи на те, що розробка медичних пристроїв для покращення здоров’я пацієнтів є чудовим застосуванням технологій, безпека технології також має бути головною проблемою. Дослідження показали, що прослуховування сигналів і вилучення інформації з цих пристроїв можливо. Що ще гірше, вони показали, що вони здатні отримати бездротовий доступ до комбінації серцевого дефібрилятора/ кардіостимулятора та перепрограмувати пристрій, щоб посилати фатальні поштовхи електрики пацієнту [6, 7].

Малі та великі підприємства однаково використовують PID для підвищення продуктивності, надаючи працівникам доступ до інформації про компанію або клієнтів, навіть коли вони не в офісі. Багато підприємств

звертаються до PID, які працюють під управлінням бізнес-рішень BlackBerry, OSX, Symbian OS і Windows Mobile, щоб задовольнити свої мобільні потреби. ПК в офісі зазвичай дотримуються суворого протоколу щодо безпеки; більшість навіть не надають користувачам адміністративних привілеїв на їхніх власних ПК з міркувань безпеки. Проте PID у цих середовищах мають підвищений ризик використання через відсутність безпеки, але більшість компаній не захищають їх, ніби вони становлять підвищений ризик безпеки. PID, як і ПК, можуть бути заражені шпигунським програмним забезпеченням або вірусами, текстові повідомлення та електронна пошта можуть бути перехоплені, а мікрофони можна віддалено вмикати для запису та/або моніторингу розмов [8]. Атака на бізнес-PID може призвести до витоку конфіденційної інформації компанії, інформації про клієнта та навіть, можливо, порушити зв'язок пристрою, якщо використовується атака «Відмова в обслуговуванні» (DoS).

1.2. Особливості методології багатовекторної портативної системи виявлення вторгнень

Основна мета цього дослідження полягає в тому, щоб перешкодити зовнішнім джерелам негативно впливати на зручність використання та термін служби PID на одному заряді акумулятора. Оскільки PID залежать від джерел мобільних акумуляторів з обмеженим терміном служби, атаки, зосереджені на розрядженні акумулятора, можуть, по суті, спричинити DoS на цих пристроях [1, 11, 12].

Методологія MVP-IDS проста: розпізнати значну зміну IC на PID і співвіднести цю зміну зі зловмисним трафіком Wi-Fi або Bluetooth. Для цього MVP-IDS розділено на чотири окремі модулі:

- Клієнт B-SIPS для запуску аномалії IC, модуль Wi-Fi на основі Snort для виявлення атак Wi-Fi, модуль BADSS для виявлення атак Bluetooth і сервер CIDE [1] для кореляції атак і відповіді, як показано на рисунку 1.2.

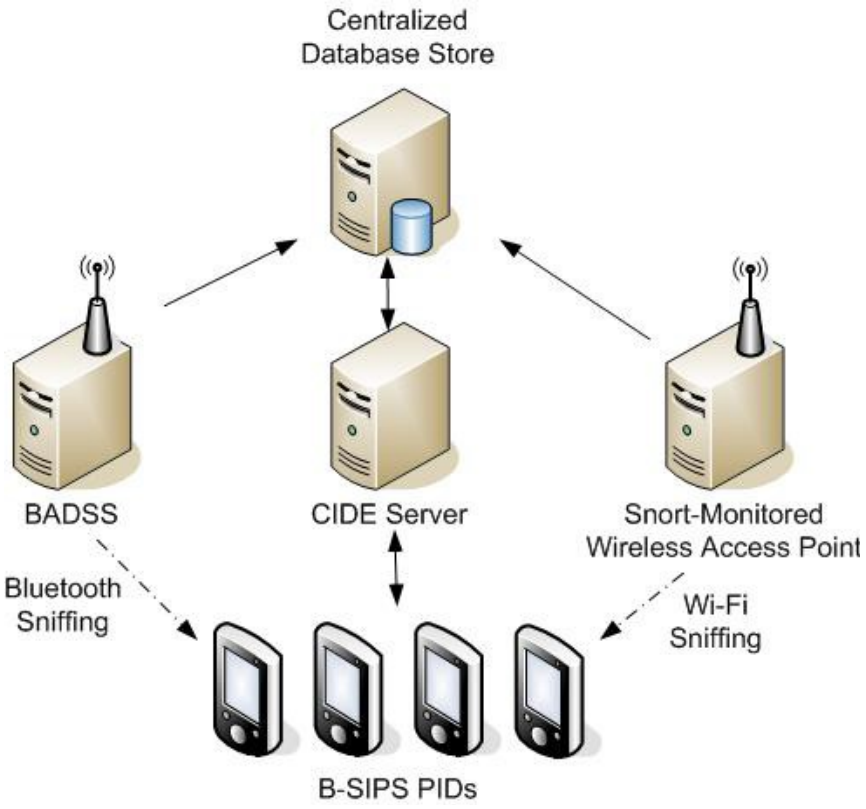

Рис. 1.2. Огляд багатовекторної портативної системи виявлення вторгнень (MVP-IDS)

Виявлення атак клієнта B-SIPS базується на порушеннях у змінах IC пристрою. Клієнти B-SIPS опитують інтелектуальну батарею щодо напруги, струму, температури, відсотка роботи батареї, прапора батареї та стану мережі змінного струму, щоб визначити стан споживання батареї. Алгоритм DTC був розроблений, щоб запобігти системі помилково ідентифікувати зміни IC як справжні атаки, враховуючи відомі причини розрядження батареї, зокрема запуск відомих процесів і зміну підсвічування пристрою. На основі цієї інформації регулюються порогові значення тривоги, щоб зменшити помилкові спрацьовування [1].

Теоретичний підхід до виявлення атак Wi-Fi та Bluetooth полягає у відстеженні всього надісланого та отриманого трафіку від PID через ці середовища та запускати тривоги на основі відомих шкідливих пакетів. Це завдання може бути виконано шляхом використання необроблених сокетів в

операційній системі (ОС), що дозволяє отримати доступ до заголовка та корисного навантаження всіх переданих пакетів [13]. Наше дослідження запропонувало таким чином відстежувати весь бездротовий трафік для PID і надсилати отриманий трафік назад на сервер CIDE для аналізу за допомогою Snort і BADSS. Однак, оскільки надсилання кожного пакета повністю назад на сервер CIDE подвоїло б обсяг типового мережевого трафіку і не було повністю необхідним для виявлення атак, було вирішено надсилати лише частини кожного пакета Wi-Fi разом із пакетом високого рівня для сигналізації через Bluetooth.

1.2.1. Опис основних елементів методології

На жаль, готову доступність необроблених сокетів для Wi-Fi було видалено з Windows Mobile середовище Microsoft з міркувань безпеки, залишаючи пошук гіпотетичних результатів за допомогою моделювання для перевірки перехоплення пакетів для виявлення атак. У нашому моделюванні пакети захоплюються, коли вони проходять через контрольовану Snort точку бездротового доступу (WAP), з якою пов’язані PID. Незважаючи на те, що цей підхід не є ідеальним мобільним рішенням для захоплення трафіку, він забезпечує більш точні результати та не буде обмежений обсягом отриманих даних, які можна передати без споживання великої кількості ресурсів PID.

BADSS спочатку був розроблений для виявлення атак Bluetooth таким же способом, як спочатку запропоновано в теоретичному підход до захоплення пакетів. Захоплення всього трафіку Bluetooth для PID дозволяє контролювати зв’язок у режимі реального часу з кореляцією, яку виконує сервер CIDE. Через відсутність необроблених сокетів Bluetooth, аналізатор протоколу Bluetooth Merlin II [14] використовувався для пасивного захоплення трафіку між взаємодіючими пристроями Bluetooth. BADSS аналізує текстові файли захоплення з аналізатора та намагається співвіднести записаний трафік із відомими сигнатурами атак у базі даних сигнатур

BADSS. Після виявлення атаки реєструються в базі даних атак BADSS для аналізу та перегляду на сервері CIDE.

Сервер CIDE функціонує як супервізор системи, виконуючи кореляцію атак і розробляючи підстави для відповідних дій. Кореляційний та адміністративний аналіз виконується за межами PID через обмежену пам'ять, заряд акумулятора та обмеження обробки PID. Сервер CIDE взаємодіє з модулями Snort і BADSS, щоб визначити, який вектор(и) атаки викликав порушення DTC клієнтом B-SIPS.

Щойно сервер CIDE отримує інформацію про зв'язок аномалії IC із пов'язаною сигнатурою атаки, він надсилає адміністративні відповіді назад до атакованого PID. Адміністративні відповіді не тільки повідомляють користувачеві PID, що його атакують, але й надають подробиці про атаку та адміністративні заходи, які вживаються.

1.2.2. Вдосконалення системи виявлення вторгнень MVP-IDS

Для подальшого розвитку проекту та створення MVP-IDS було реалізовано наступні вісім значних покращень, що суттєво підвищили його надійність та ефективність захисту PIDs у шкідливих середовищах.

- Додана система виявлення вторгнень Bluetooth на основі відповідності шаблонів для розпізнавання атак Bluetooth.

- Впроваджено сканування трафіку Wi-Fi за допомогою Snort та реєстрацію виявлених атак у базі даних, доступній для перегляду в CIDE.

- Завдяки використанню Snort для трафіку Wi-Fi та BADSS для трафіку Bluetooth стало можливим диференціювати атаки та засоби їх здійснення.

- MVP-IDS тепер здатний розпізнавати гібридні або багатовекторні атаки, що поєднують елементи як Wi-Fi, так і Bluetooth атак.

- Оскільки Snort і BADSS реєструють атаки в централізованій базі даних, сервер CIDE може проводити кореляцію в реальному часі від клієнтів B-SIPS, як тільки вони повідомляють про атаку.

- На відміну від попередньої реалізації B-SIPS, MVP-IDS тепер має можливість активно реагувати на атаки за допомогою двостороннього зв'язку.

- У разі виявлення атаки, MVP-IDS вимикає лише бездротові інтерфейси, які вважаються атакованими, на відміну від попередньої реалізації B-SIPS, яка відключала як Wi-Fi, так і Bluetooth інтерфейси.

- Для забезпечення конфіденційності, автентифікації, цілісності повідомлень та незаперечності усі передачі повідомлень між клієнтами B-SIPS та сервером CIDE були захищені відповідними механізмами.

- Щоб пом’якшити втручання в транзакції даних між клієнтами B-SIPS і сервером CIDE, конфіденційність, автентифікація, цілісність повідомлень і невідмовність були інтегровані в усі передачі повідомлень.

1.3. Опис основних характеристик пристроїв з точки зору їх вразливостей до різних видів атак та вторгнень

Розглянемо визначальні характеристики КПК і смартфонів на основі яких можуть вчинятися зловмисні дії та вторгнення.

КПК були вперше представлені в середині 1990-х років, першими популярними моделями були Apple Newton і Palm Pilot. Спрощене визначення КПК: «комп’ютер, який поміщається у вашій долоні [15, 16]».

Багато функцій, які є стандартними для більшості КПК, включають:

• РК-дисплеї: більша частина поверхні пристрою використовується як графічний інтерфейс, за допомогою якого користувачі взаємодіють за допомогою стилуса або натискань пальців. Це дозволяє користувачам легко та без зусиль переміщатися між меню для виконання бажаних завдань.

• Операційні системи: зазвичай більш базові та зменшені версії, ніж інстальовані на ПК, ці версії ОС працюють приблизно так само, як і повнофункціональні ОС. Деякі з популярних ОС включали Symbian, Palm OS і Windows Mobile.

• Синхронізація: більшості користувачів, як правило, потрібні КПК для мобільного керування зустрічами, контактною інформацією, електронною поштою та щоденним плануванням. Оскільки ці дані зазвичай потрібні як на КПК, так і на ПК, синхронізація між ними є важливою. КПК можна підключати або синхронізувати з ПК, дозволяючи користувачеві зберігати дані, електронну пошту тощо актуальними на обох пристроях. Це робиться для того, щоб кожен пристрій відображав точну та актуальну інформацію.

• Програмні додатки: КПК дозволяють обробляти дані та підвищувати продуктивність у дорозі за допомогою програмних додатків, таких як Microsoft Word, Excel, Outlook та багато інших. Більшість кишенькових комп'ютерів навіть дозволяють користувачам переносити програми сторонніх розробників, такі як ігри чи спеціальні утиліти, на свої пристрої.

• Мультимедійні програвачі: багато користувачів бажають мати пристрій не лише для функціональності, але й із задоволенням можуть використовувати його для розваг. Можливість відтворювати музику чи фільми з КПК позбавляє користувачів від необхідності носити з собою другий пристрій, призначений виключно для відтворення мультимедіа.

• Підключення до Інтернету: доступ до Інтернету та підключення Wi-Fi дозволяють користувачам виконувати завдання так, ніби вони перебувають перед ПК. Завдяки вбудованим програмам, таким як Microsoft Outlook і Internet Explorer, користувачі лише одним дотиком отримують доступ до електронної пошти та веб-перегляду.

• Bluetooth: користувачі можуть бездротово синхронізуватися з ПК, передавати файли за допомогою програм протоколу передачі файлів (FTP) і спілкуватися з іншими пристроями, такими як принтери та клавіатури, за допомогою технології Bluetooth. Bluetooth забезпечує бездротове з'єднання на короткій відстані між КПК і периферійними пристроями, для яких колись були потрібні кабельні з'єднання.

Як і у випадку з більшістю технологічних пристроїв, з часом їхня популярність зростала. Однак з КПК ні маючи можливості телефонії,

користувачі виявили, що мають два пристрої: один для організації свого життя та інший просто для послуг телефонії. Користувачі кишенькових комп'ютерів хотіли мати можливості стільникового телефону зі своїми кишеньковими комп'ютерами, а користувачі стільникових телефонів хотіли функціональність стільникових телефонів із стільниковими телефонами. Обидва ці пристрої тепер об'єдналися, щоб створити один пристрій – смартфон. Хоча більшість специфікацій не дають стандартного чи чіткого визначення смартфону [17 - 19], усі описують його як КПК із повною функціональністю мобільного телефону. Деякі з розширених функцій смартфонів, які зазвичай не є стандартними для КПК, включають:

• Телефонія та обмін текстовими повідомленнями. Зважаючи на те, що в сучасному суспільстві переважає технологія мобільних телефонів, має сенс лише додавати цю функцію до КПК. Додавання текстових повідомлень і можливості голосових дзвінків дозволило користувачам носити один пристрій, смартфон, замість того, щоб відставати від КПК і мобільного телефону окремо.

• Клавіатури QWERTY: клавіатури QWERTY мають розкладку комп'ютерних клавіатур, але більш компактні. Вони містять усі буквено-цифрові символи та дозволяють користувачам вводити букви замість використання цифрової клавіатури для створення тексту. Хоча клавіатури QWERTY не популярні на більшості КПК, вони вважаються галузевим стандартом для смартфонів.

• Системи глобального позиціонування (GPS): Новіші смартфони дозволяють користувачам використовувати GPS для отримання точних географічних координат і відображення карт.

Продажі смартфонів постачальниками кінцевим користувачам останніми роками досить зросли [20]. Незважаючи на те, що останнім часом економічні умови не надто сприяли зростанню продажів, IDC, провідна дослідницька фірма в галузі технологій, усе ще прогнозує зростання на 4-5 щороку [21]. У решті даної роботи кишенькові комп'ютери та смартфони

тепер називатимуться разом PID. Класифікація PID дозволяє обговорювати без розрізнення між двома пристроями або згадування обох.

Пристрої, такі як КПК, ПК та мобільні телефони, мають ряд характеристик, які роблять їх вразливими до різних видів атак та вторгнень. Розглянемо деякі з них:

- Вразливості операційних систем та програмного забезпечення:

- Застарілі версії: Неоновлені операційні системи та програмне забезпечення часто містять відомі вразливості, які можуть бути використані зловмисниками для проникнення в систему.

- Незахищені налаштування: Неправильна конфігурація системи, наприклад, відкриті порти, слабкі паролі або відсутність брандмауера, значно збільшують ризик атак.

- Вразливості в додатках: Поширені програми та додатки можуть містити вразливості, які можуть бути використані для отримання доступу до системи або даних користувача.

- Мережеві загрози:

- Незахищені бездротові мережі: Підключення до незахищених Wi-Fi мереж робить пристрій вразливим для перехоплення даних та інших атак.

- Фішинг: Зловмисники можуть використовувати фішингові електронні листи або веб-сайти для отримання конфіденційної інформації, такої як паролі або номери кредитних карток.

- Шкідливе програмне забезпечення: Віруси, троянські коні та інше шкідливе програмне забезпечення можуть проникнути в систему через Інтернет або заражені файли.

- Додаткові фактори:

- Слабкі паролі: Використання простих або легко вгаданих паролів є однією з найпоширеніших причин порушення безпеки.

- Відсутність резервного копіювання: Відсутність регулярного резервного копіювання даних може призвести до їхньої втрати в разі атаки або поломки пристрою.

- Необережне використання мобільних пристроїв: Використання мобільних пристроїв у громадських місцях, таких як кафе або аеропорти, збільшує ризик перехоплення даних.

Висновки до розділу

У результаті дослідження предметної області виявлення вторгнень та атак на програмні системи було проведено аналіз сучасних підходів до розробки систем виявлення вторгнень (IDS) з акцентом на багатовекторні та портативні рішення. Дослідження дозволило виявити ключові особливості, переваги та недоліки сучасних підходів, а також визначити можливості для їхнього вдосконалення.

Аналіз середовища та систем виявлення вторгнень продемонстрував важливість створення адаптивних і гнучких систем, здатних працювати у різних середовищах з підвищеним рівнем загроз. Зокрема, досліджено вплив складності мережевої інфраструктури та різноманітності можливих атак на ефективність традиційних IDS. Це підтвердило необхідність розробки багатовекторних рішень, що забезпечують широкий спектр моніторингу та аналізу.

Розгляд методології багатовекторної портативної системи виявлення вторгнень (MVP-IDS) дозволив розкрити ключові елементи, що роблять такі системи ефективними в сучасних умовах кіберзагроз. Методологія MVP-IDS включає у собі використання декількох джерел даних, що дозволяє здійснювати комплексний аналіз трафіку, виявлення аномалій та аналіз сигнатур вторгнень. Це підвищує точність та ефективність системи, зменшуючи ймовірність помилкових спрацьовувань та пропущених атак.

Вдосконалення системи MVP-IDS продемонструвало її переваги над традиційними підходами, особливо у розширенні функціональності та можливостях адаптації до нових загроз. MVP-IDS покращує виявлення вторгнень завдяки інтеграції з методологією B-SIPS (Battery-Sensing Intrusion

Protection System), що забезпечує додатковий рівень захисту, використовуючи аналіз енергоспоживання пристроїв для виявлення аномалій у їх роботі.

Оцінка вразливостей пристроїв показала, що сучасні пристрої, особливо в таких критично важливих сферах, як медицина та бізнес, мають значну кількість потенційних точок доступу для зловмисників. Це включає слабкості в бездротових з'єднаннях, недостатню захищеність програмного забезпечення, а також обмеженість ресурсів для впровадження комплексних захисних рішень. Висвітлено важливість впровадження портативних та ресурсоефективних систем захисту, таких як MVP-IDS, для забезпечення високого рівня безпеки.

Таким чином, дослідження підтвердило, що застосування багатовекторного підходу до проєктування портативних систем виявлення вторгнень є перспективним напрямком для підвищення рівня безпеки програмних систем у різноманітних середовищах. Використання MVP-IDS разом із методологією B-SIPS сприяє розширенню можливостей виявлення аномалій та вторгнень, забезпечуючи більш комплексний підхід до захисту сучасних інформаційних систем.

РОЗДІЛ 2. МОДЕЛІ ТА АЛГОРИТМИ ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІНОГО ЗАХИСТУ

2.1. Форми криптографії: конфіденційність, автентифікація, цілісність повідомлень і невідмовність

Конфіденційність, автентифікація, цілісність повідомлень і невідмовність — це всі форми криптографії, які використовуються для забезпечення успішного обміну таємними повідомленнями між двома сторонами. Ці криптографічні властивості використовуються в багатьох транзакціях, пов’язаних з Інтернетом, дуже сприйнятливими до атак, зокрема: онлайн-банкінг, онлайн-магазини та багато інших місць, де потрібен обмін особистою інформацією.

Існує дві форми шифрування, які зазвичай використовуються для забезпечення конфіденційності: криптографія із закритим ключем і криптографію з відкритим ключем. В даному розділі йде мова про криптографію із закритим ключем, розглядається сфера криптографії з відкритим ключем та досліджується автентифікація, цілісність повідомлень і невідмовність, показуючи, як кожне з них може бути застосоване до повідомлень або ідентифікаторів для захисту транзакцій даних.

2.1.1. Криптографія приватного ключа

Криптографія із закритим (приватним) ключем є найдавнішою формою шифрування, яка сягає століть у стародавні цивілізації [22]. Інший термін для цього для криптографії із закритим ключем — симетрична криптографія, оскільки вона використовує лише один секретний ключ як для процесу шифрування, так і для процесу дешифрування, як показано на рисунку 2.1. Щоб повністю зрозуміти цей процес, існує шість основних термінів, які необхідно знати [22]:

• Відкритий текст: це зрозуміле для людини повідомлення або інформація, яку хочеться зробити секретною.

• Зашифрований текст: це нечитабельне повідомлення, яке виводиться в процесі шифрування.

• Алгоритм шифрування: це процес, за допомогою якого відкритий текст перетворюється на зашифрований за допомогою різноманітних замін і перетворень. Вхідні дані для алгоритму шифрування включають відкритий текст і секретний ключ; на виході буде зашифрований текст.

• Секретний ключ: це частина інформації, яка повинна зберігатися в секреті. Секретний ключ використовується як вхідні дані для алгоритму шифрування, тому кожна комбінація відкритого тексту та секретного ключа створює різні нечитабельні результати. Перетворення та заміни, які виконує алгоритм шифрування, базуються на ключі.

• Алгоритм дешифрування: це алгоритм шифрування, який виконується у зворотному порядку. Алгоритм дешифрування приймає секретний ключ і зашифрований текст як вхідні дані та повертає відкритий текст як вихідні дані.

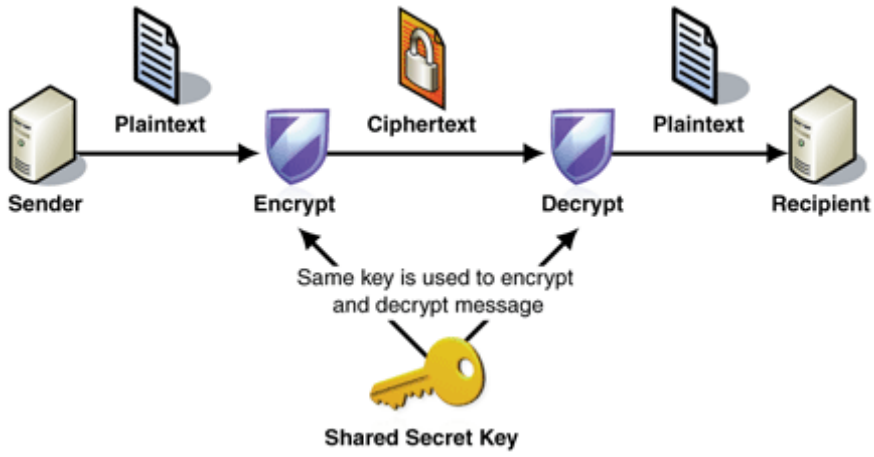

Рис. 2.1. Алгоритм криптографії із закритим ключем [23]

2.1.2. Криптографія публічного ключа

Криптографія з відкритим ключем дотримується багатьох тих самих принципів і процедур криптографії з закритим ключем, але використовує

різні ключі в процесі шифрування та дешифрування, як показано на рисунку 2.2.

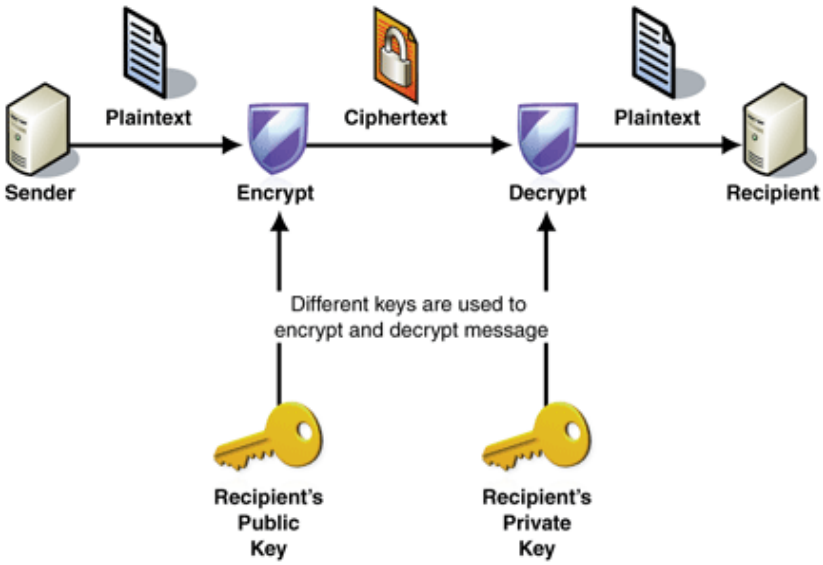

Рис. 2.2. Алгоритм криптографії з відкритим ключем [23]

Для використання різних ключів також відома криптографія з відкритим ключем як асиметрична криптографія. Ключі, які використовуються в криптографії з відкритим ключем, визначені нижче [22]:

• Відкритий ключ: цей ключ є загальнодоступною інформацією, і відправник може використовувати його під час шифрування повідомлення.

• Приватний ключ: цей ключ є приватною інформацією для одержувача та використовується в процесі дешифрування.

2.1.3 Автентифікація, цілісність повідомлення та невідмовність

Автентифікація — це процес підтвердження того, що хтось є тим, за кого себе видає. Можливість довести, що отримані дані є саме тими, що були надіслані, називається цілісністю повідомлення. Цілісність повідомлення підтверджує, що вихідне повідомлення отримано без будь-яких вставок, видалень або змін. Невідмовність означає здатність одержувача беззаперечно знати, що отримане повідомлення надійшло від заявленого відправника [22].

Хоча шифрування забезпечує конфіденційність даних, можна також стверджувати, що воно забезпечує певний ступінь автентифікації, цілісності повідомлення та неспростовності через використання спільних секретних ключів. Хоча це можна прийняти, якщо є впевненість, що лише дві сторони, що спілкуються, справді знають відповідні ключі, воно стає повністю недійсним, якщо секретний ключ стає скомпрометованим для третьої, ненавмисної сторони. З цієї причини криптографи створили дві загальноприйняті криптографічні процедури, які можна застосувати до повідомлень для успішного досягнення криптографічних властивостей, розглянутих у цьому розділі.

Двома найпоширенішими алгоритмами, які використовуються для забезпечення автентифікації, цілісності повідомлень або неспростування, є коди автентифікації повідомлень (MAC) і безпечні хеш-функції. На відміну від алгоритмів шифрування, процес використання MAC і безпечної хеш-функції є одностороннім, тобто незворотним [22]. Вхідні дані, які використовуються для обчислення MAC або хеш-значення, не можуть бути витягнуті з результату.

• Коди автентифікації повідомлень (MAC): цей алгоритм намагається забезпечити криптографічну безпеку повідомлення за допомогою згенерованого значення фіксованої довжини, відомого як MAC. Щоб створити це значення, відправник використовує алгоритм MAC і два вхідні дані: спільний секретний ключ і вихідне повідомлення. Після того, як значення згенеровано, воно зазвичай об’єднується в кінець вихідного повідомлення, а потім надіслано. Після отримання одержувач може згенерувати MAC, як і відправник, щоб порівняти ці два значення. Якщо значення збігаються, це означає, що повідомлення криптографічно еквівалентне надісланому. Якщо ні, то можна сказати, що під час передачі повідомлення сталася помилка або повідомлення було змінено [22]. Процес використання MAC можна побачити на рисунку 2.3.

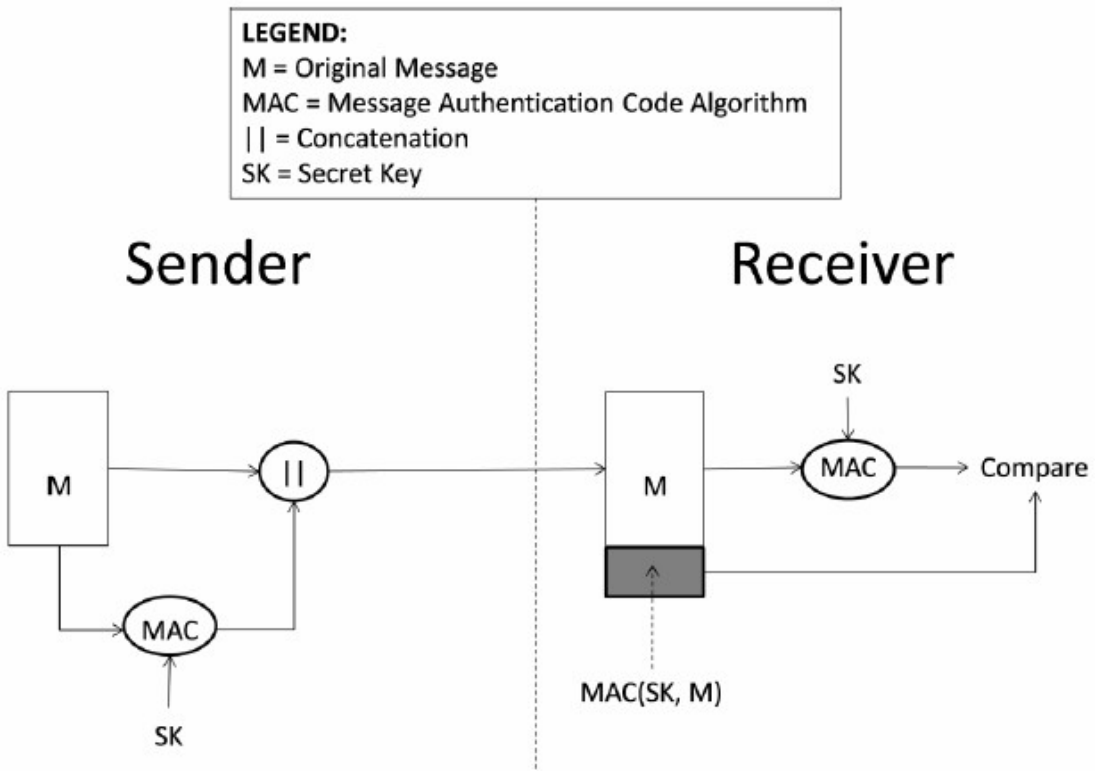

Рис. 2.3. Процес генерації MAC для автентифікації повідомлень

• Захищені хеш-функції: це алгоритм, який намагається зіставити повідомлення змінної довжини з хеш-значенням фіксованої довжини, також відоме як дайджест повідомлення.

Захищені хеш-функції – це математичні алгоритми, які перетворюють дані довільної довжини у фіксовану послідовність символів, звану хешем або дайджестом. Головна особливість таких функцій полягає в їхній однобічності: знаючи хеш, практично неможливо відновити вихідні дані.

Приклади захищених хеш-функцій:

- SHA-256: Широко використовується в криптографії, включаючи біткоїн.

- MD5: Хоча колись був популярним, зараз вважається недостатньо безпечним через виявлені вразливості.

- SHA-3: Новіший стандарт, розроблений для заміни SHA-2.

Основна відмінність між безпечними хеш-функціями та MAC полягає в тому, що алгоритми хешування залежать лише від повідомлення, яке використовується як вхід. Єдиний спосіб перевірити автентичність хеш-

значення для обох залучених сторін обчислити хеш-значення повідомлення та порівняти результати [22]. Процес використання безпечної хеш-функції можна побачити на рисунку 2.4.

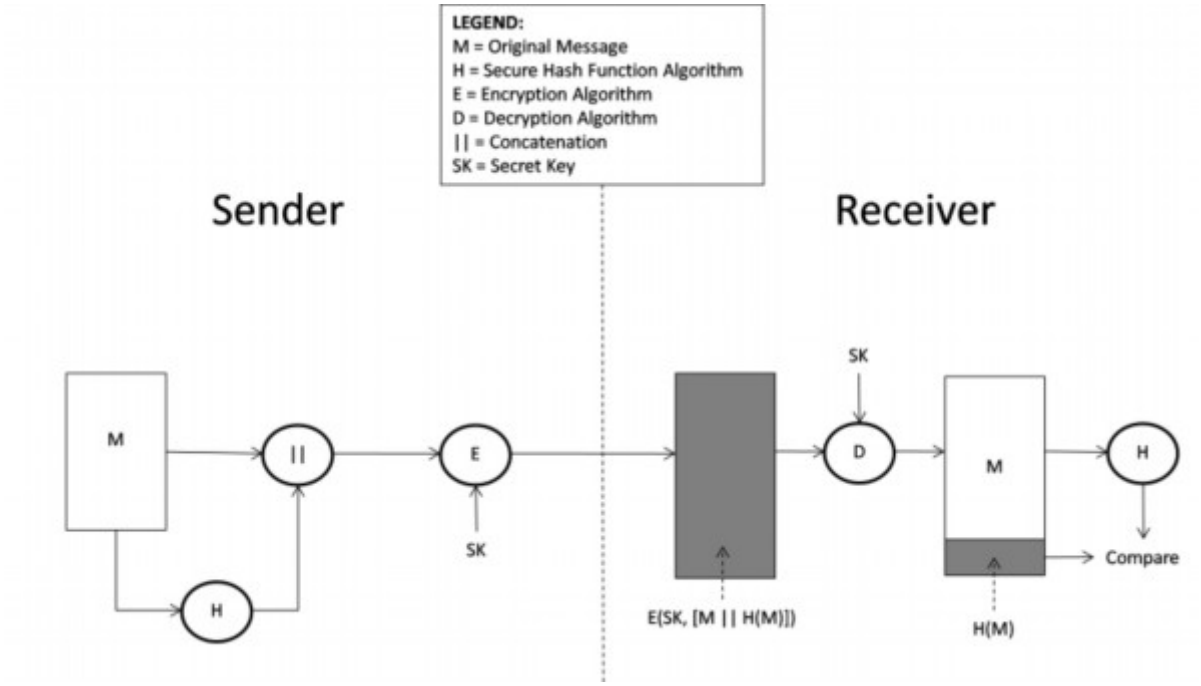

Рис. 2.4. Процес генерації хеш-значення для автентифікації повідомлення

2.2. Дослідження протоколів TCP/IP і WiFi з точки зору їх вразливостей і захисту

2.2.1. Моделі протоколу TCP/IP

Стек протоколів TCP/IP – це сукупність протоколів, які визначають, як комп'ютери спілкуються один з одним в Інтернеті та інших мережах. Цей стек забезпечує надійну передачу даних між різноманітними пристроями, від персональних комп'ютерів до серверів.

Набір протоколів керування передачею Інтернет-протоколу (TCP/IP) — це 5-рівнева модель, заснована на моделі OSI, яка використовується для представлення мережевих протоколів і організована в ієрархічний стек протоколів. Кожен рівень використовується для інкапсуляції власних даних і надає послуги рівню над ним 5 шарів стека: прикладний рівень,

транспортний рівень, мережевий рівень, канальний рівень і фізичний рівень [24 - 27]. Стек TCP/IP і характеристики представлено в таблиці 2.1.

Таблиця 2.1.

Модель TCP/IP

	Layer	Data Unit	Function	Examples
Host Layers	5. Application	Data	Networked applications	HTTP, FTP, POP3, SMTP, SSH
	4. Transport	Segment	End-to-end connections and reliability	TCP, UDP
Media Layers	3. Network	Packet	Path Determination and logical addressing	IP, ICMP
	2. Data Link	Frame	Single hop connections	ARP, NDP
	1. Physical	Bit	Binary transmission	-

• Прикладний рівень: у верхній частині моделі стеку протоколів TCP/IP знаходиться прикладний рівень. Цей рівень надає послуги, з якими користувач може взаємодіяти, такі як веб-браузери, FTP-клієнт/сервери, SSH-клієнти/сервери та багато інших програм, які використовуються для мережевого зв’язку.

• Транспортний рівень: цей рівень складається з TCP і протоколу дейтаграм користувача (UDP). Метою цього рівня під час використання протоколу TCP, орієнтованого на з’єднання, є надання кінцевим користувачам надійної передачі даних, забезпечуючи доставку даних у визначені місця на комп’ютері-одержувачі. Забезпечуючи надійну передачу даних між кінцевими користувачами, цей рівень також має можливість повторно передавати сегменти, втрачені під час передачі, для додатків, які потребують цієї послуги. Навпаки, UDP пропонує протокол без з’єднання, корисний для передач, які мають бути дуже швидкими, наприклад

потокового мультимедіа, але не забезпечує надійності, перевірки помилок і повторного надсилання пакетів, які реалізує TCP.

• Мережевий рівень: цей рівень виконує функції маршрутизації, які зосереджені на наскрізній доставці пакетів у мережі та включають протокол IP. Фрагментація та повторна збірка пакетів, логічна адресація та визначення мережевого шляху є ключовими операціями, які виконуються пристроями на цьому рівні. Протокол IP широко використовується маршрутизаторами, які намагаються доставити дані до наступного передбачуваного стрибка.

• Канальний рівень: під час надсилання даних цей рівень додає заголовок і трейлер до даних мережевого рівня, щоб апаратне забезпечення могло правильно розпізнавати початкову та кінцеву точки кадрів, що передаються на фізичному рівні. Під час отримання даних основною метою цього рівня є прийом необроблених передач отриманих бітів та інтерпретація їх у кадри Ethernet. Після того, як початок і кінець кадру розпізнано, канальний рівень видаляє його заголовок кадру та кінцеву частину, а потім передає решту даних кадру на мережевий рівень, щоб він міг виконувати заплановані операції.

• Фізичний рівень: цей рівень є фактичним фізичним середовищем, через яке передаються необроблені біти даних. На цьому рівні дані перетворюються між цифровими даними та електричними сигналами, щоб апаратні пристрої могли належним чином спілкуватися один з одним.

Коли один комп’ютер намагається надіслати дані іншому комп’ютеру через пакет TCP/IP, корисні дані починаються у верхній частині стека протоколів комп’ютера-відправника та просувається донизу. На кожному прогресивному нижчому рівні додаються метадані, щоб забезпечити успішну доставку фактичних даних корисного навантаження. Коли переданий кадр досягає комп’ютера-одержувача, він рухається у зворотному напрямку або вгору по стеку протоколів. Кожен рівень видаляє свої метадані перед передачею фактичних даних вищого рівня на наступний вищий рівень. Цей процес можна побачити на рисунку 2.5.

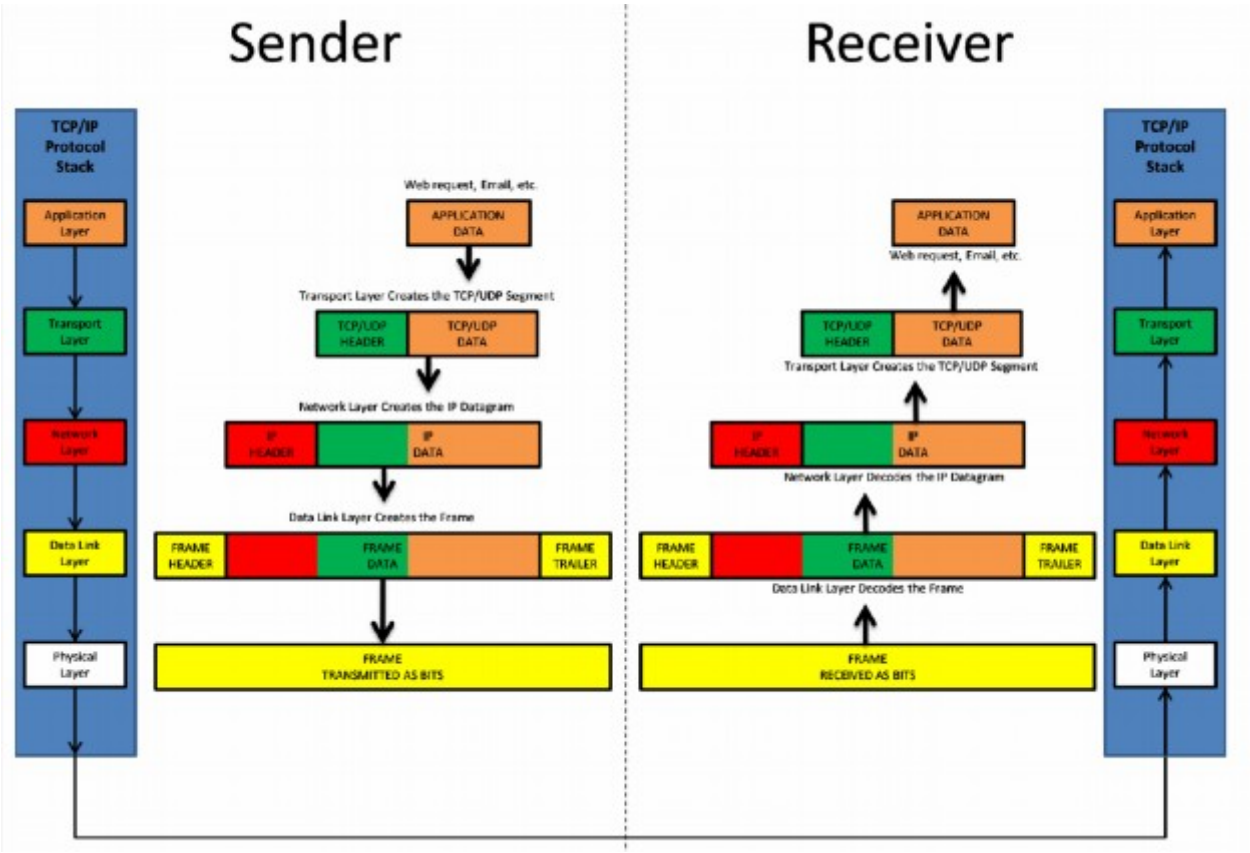

Рис. 2.5. Передача даних у моделі TCP/IP

2.2.2. Модель бездротової мережі Wi-Fi

IEEE 802.11 – це сімейство стандартів, які визначають, як пристрої можуть бездротово підключатися до локальної мережі (WLAN). Ці стандарти забезпечують основу для технології Wi-Fi, яку ми використовуємо щодня для підключення наших смартфонів, ноутбуків та інших пристроїв до Інтернету.

IEEE 802.11 Wi-Fi — це стандартна технологія для високошвидкісної бездротової локальної мережі (WLAN) [29]. Wi-Fi використовує радіочастоти 2,4–2,5 або 5 ГГц у промисловому, науковому та медичному (ISM) діапазоні. Wi-Fi функціонує шляхом створення WLAN, що складається з одного або кількох бездротових клієнтських вузлів, кожен з яких пов’язаний з WAP, що з’єднує їх із загальною мережею. У цій WLAN кожен клієнтський вузол ідентифікується своєю адресою керування доступом до середовища (MAC) та/або IP-адресою. Бездротово передані кадри 802.11, показані на рисунку 2.6., використовуються для зв’язку між бездротовими клієнтськими вузлами

та WAP [30]. Топологію WLAN/Wi-Fi показано на рисунку 2.7, а деякі ключові характеристики WLAN/Wi-Fi наведено в таблиці 2.2.

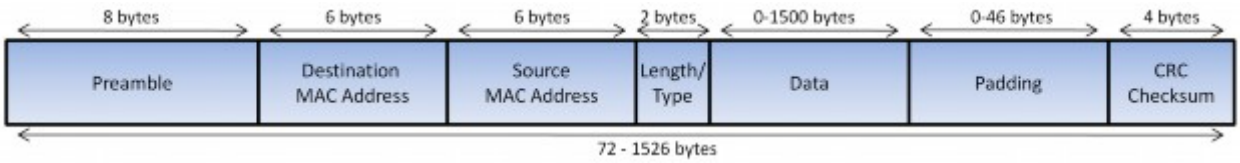

Рис. 2.6. Макет кадру 802.11

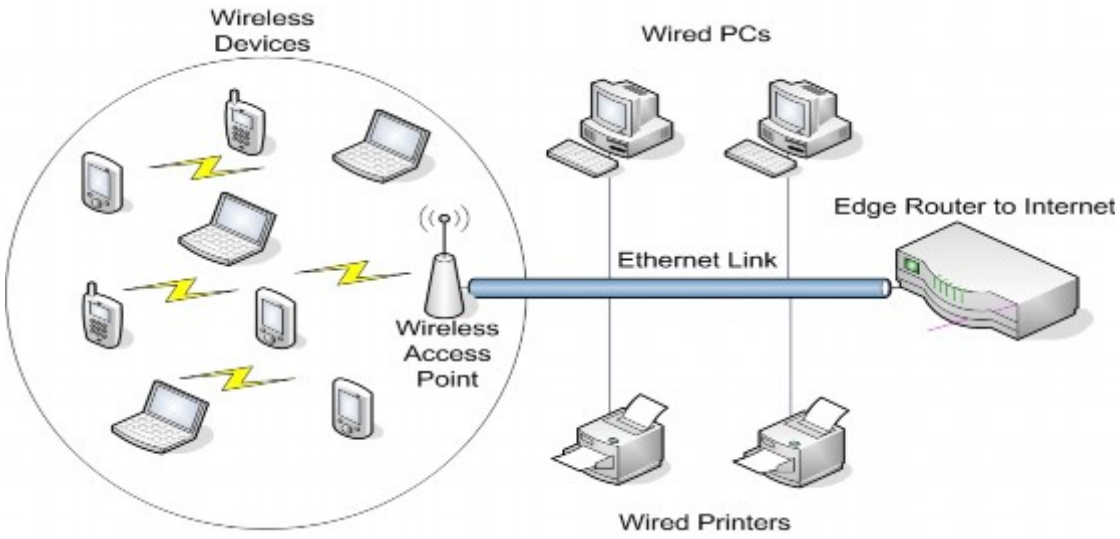

Рис. 2.7. Основна топологія 802.11 WLAN/Wi-Fi

Таблиця 2.2.

Характеристики технології 802.11 WLAN/Wi-Fi

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a), 54 Mbps (11g), 74 Mbps (11n)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors, depending on operating environment.
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

2.3. Огляд архітектури та особливостей стеку протоколів Bluetooth

У 1998 році було засновано Спеціальну групу інтересів Bluetooth (SIG) для нагляду за стандартизацією та увічненням протоколу Bluetooth IEEE 802.15.1. Bluetooth — це бездротова технологія, яка реалізує ідею персональної мережі (PAN). Це недороге, малопотужне бездротове рішення малої дальності для передачі голосу та даних до/від периферійних пристроїв, для яких колись були потрібні кабельні з'єднання. Багато пристроїв, які використовують Bluetooth, включають: стільникові телефони, смартфони, гарнітури «вільні руки», GPS, клавіатури, принтери тощо.

З тією простотою використання, яку Bluetooth надає своїм користувачам, він стає все більш популярним.

2.3.1. Огляд архітектури Bluetooth

Bluetooth також працює в бездротовому режимі в діапазоні 2,4 ГГц – 2,485 ГГц, ISM. Щоб уникнути перешкод для інших бездротових пристроїв, що передають у діапазоні ISM, і пом'якшити прослуховування, Bluetooth використовує дві схеми стрибків частоти. Адаптивне стрибкоподібне перемикання частоти дозволяє уникнути перешкод для інших бездротових пристроїв, виявляючи та уникаючи частот, які використовуються цими пристроями. Це виявляється корисним, якщо пристрої Bluetooth спілкуються в тому ж повітряному просторі, що й технологія Wi-Fi, яка передає на фіксованих частотах у діапазоні 2,4 ГГц, ISM. Щоб пом'якшити прослуховування, стрибкоподібна зміна частоти в розширеному спектрі дозволяє пристроям передавати пакети по 79 різних радіочастотних каналах, кожен з яких відстань становить 1 МГц, зі швидкістю до 1600 стрибків/секунду. Кожен радіочастотний канал розділений на часові слоти, кожен довжиною 625 мкс, причому провідні пристрої передають у парні часові слоти, а підлеглі пристрої — у непарні. Головні пристрої класифікуються як ті, що ініціюють з'єднання, а підлеглі — це пристрої-

партнери пов’язаного з’єднання. Пристрої надсилають пакети в ці часові інтервали, і один пакет може використовувати до п’яти послідовних часових інтервалів, якщо це дозволяють обставини [31 - 35]. Базовий формат пакету Bluetooth показано на рисунку 2.8.

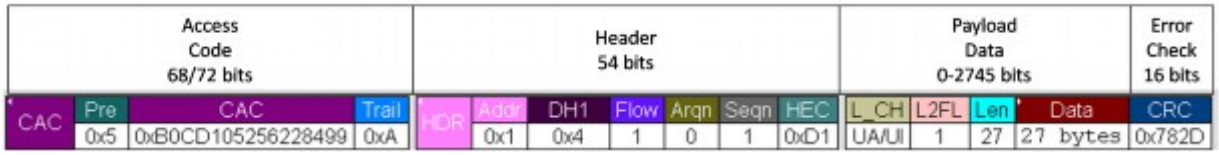

Рис. 2.8. Базовий формат пакету Bluetooth

Пристрої, що підтримують технологію Bluetooth, формують піконет – невеликі групи сполучених пристроїв. Кожен піконет складається з одного основного пристрою та максимум семи активно спілкувальних підлеглих пристроїв. Кількість активних підлеглих обмежена 7 через 3-бітову адресу активного члена, призначену кожному підлеглому пристрою. Пристрої, що не активно спілкуються, але залишаються сполученими з основним пристроєм, вважаються в паркованому стані. Піконет може підтримувати до 256 паркованих підлеглих, використовуючи 7-бітову адресу паркованого члена.

Один пристрій може бути частиною кількох піконетів, або бути підлеглим у кількох піконетах, або основним пристроєм в одній і підлеглим пристроєм в іншій. Ця взаємозв'язок піконетів утворює розсіяну мережу. В одній розсіяній мережі може бути з'єднано до 10 піконетів, перш ніж помітне зниження продуктивності [31- 35]. Така топологія сполученої комунікації представлена на рисунку 2.9.

Коли два пристрої з підтримкою Bluetooth об’єднуються в пару, з’єднання між головним і підлеглим може бути трьох різних типів [31 - 35]:

Орієнтований на синхронне підключення (SCO):

• Використовується для голосового зв'язку

• Реалізовано за допомогою комутації каналів (комутація телефону)

• Надає синхронні та симетричні послуги

• Резервування слотів через фіксовані проміжки часу

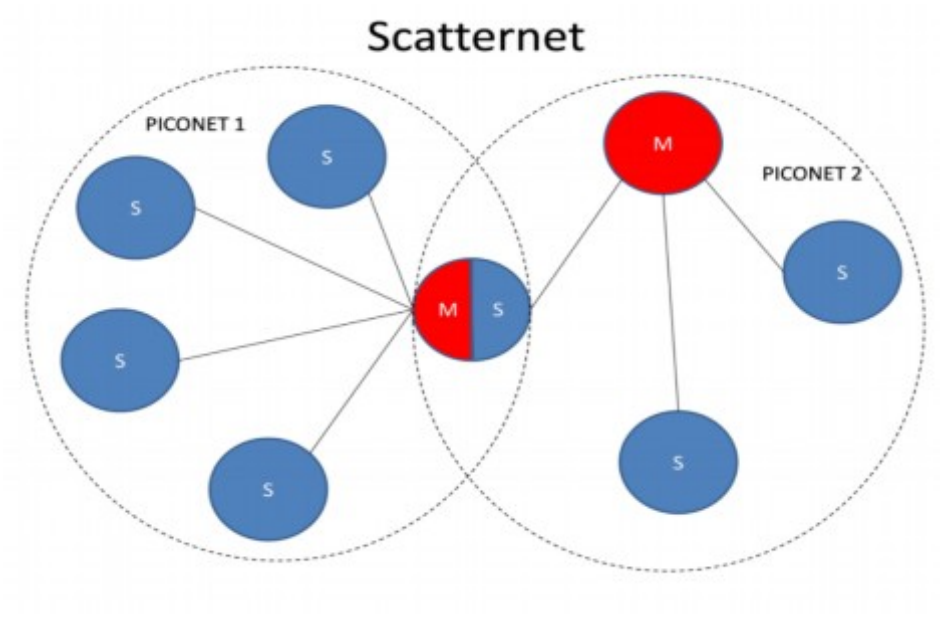

Рис. 2.9. Топологія пікомережі / розсіяної мережі Bluetooth

Без асинхронного підключення:

• Використовується для передачі даних і сигналізації

• Реалізовано за допомогою комутації пакетів

• Підтримує симетричні та асиметричні асинхронні служби

• Використовується для виявлення пристроїв і пейджінгу

Стек протоколів Bluetooth, показаний на рисунку 2.10, упорядкований у багаторівневу ієрархію, подібну до моделі TCP/IP. Кожен нижній рівень у стеку надає дані та послуги рівню, що знаходиться безпосередньо над ним.

Радіорівень забезпечує фактичну модуляцію та демодуляцію цифрових даних у радіочастотні хвилі Гауссова частотна маніпуляція (GFSK). Baseband Layer керує фізичними з'єднаннями між пристроями, що використовують радіорівень, збирає пакети та контролює стрибкоподібні зміни частоти. Рівень базової смуги також контролює роботу радіорівня, дозволяючи йому працювати в одному з трьох різних класів, кожен з різними діапазонами передачі та номінальною потужністю. Більшість пристроїв працюють у

середовищах PAN (клас 2), які вимагають лише обмеженого радіусу дії та мінімального енергоспоживання.

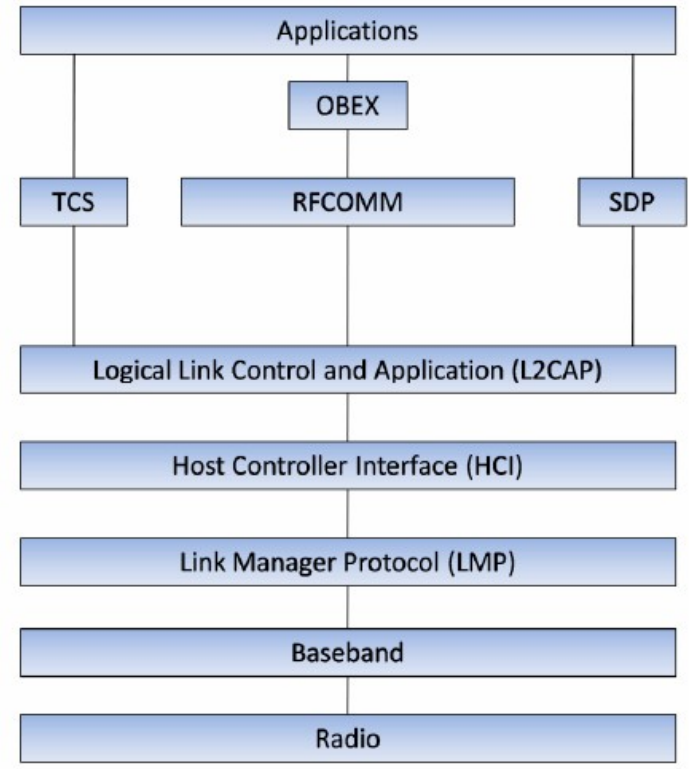

Рис. 2.10. Стек протоколів Bluetooth

Протокол керування зв'язками (LMP) налаштовує та контролює всі зв'язки з іншими пристроями. Інтерфейс хост-контролера (HCI) діє як сполучна ланка між верхніми рівнями додатків і нижніми рівнями апаратного забезпечення. Він має можливість змінювати параметри конфігурації базової смуги та рівня LMP за допомогою стандартизованих команд. Рівень керування та адаптації логічного зв'язку (L2CAP) дозволяє сегментувати та повторно збирати пакети, контролювати потоки, якість обслуговування шляхом повторної передачі непідтверджених пакетів і мультиплексування протоколів вищого рівня до каналів нижчого рівня. Baseband Layer обмежує розмір окремих пакетів для цілей передачі, але L2CAP.

Рівень дозволяє передавати більші пакети за допомогою сегментації та повторного складання, як показано на рисунку 2.11.

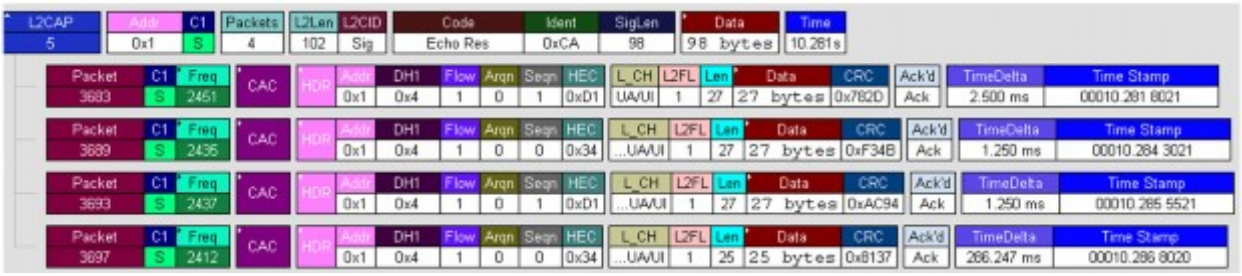

Рис. 2.11. Збірка пакета рівня L2CAP

2.3.2. Методика виявлення пристроїв

Для виявлення пристрою адреса пристрою Bluetooth є важливою частиною інформації. Без нього неможливе підключення до інших пристроїв. Адреса пристрою Bluetooth ділиться на три компоненти: нижня частина адреси (LAP), верхня частина адреси (UAP) і незначима частина (NAP) [36]. LAP має 24-бітну довжину та залежить від моделі/пристрою. LAP можна знайти в заголовках пакетів і перевірити за допомогою контрольної суми, обчисленої в полі циклічної перевірки надмірності (CRC) пакета. UAP має 8-бітну довжину і передається лише в полі коду помилки заголовка (HEC) пакетів, які узгоджують пару пристроїв. HEC містить результат лінійного алгоритму зворотного зв'язку, який ініціалізується за допомогою UAP. Змінивши алгоритм на приймальному кінці, можна визначити UAP. NAP має довжину 16 біт, причому старші 8 біт майже завжди дорівнюють нулю. Хоча NAP використовується для ідентифікації пристрою, він не впливає на генерацію пакетів і не міститься в них. NAP і UAP разом залежать від постачальника та відомі як організаційно-унікальний ідентифікатор (OUI).

Усі адреси пристроїв Bluetooth є унікальними, і IEEE призначає окремим постачальникам ексклюзивні діапазони адрес [37]. Це робиться для того, щоб розділити адресний простір Bluetooth і уникнути повторюваної адресації. На рисунку 2.12 показана адреса пристрою Bluetooth і розбивка його компонентів.

Є два способи отримати адресу пристрою Bluetooth. Якщо адреса пристрою відома, спроба підключення до адреси може призвести до

успішного з’єднання. Якщо адреса пристрою невідома, процес дещо складніший. Коли пристрій хоче ідентифікувати всі пристрої поблизу, він надсилає широкомовний запит, на який можуть відповісти інші пристрої Bluetooth. Однак пристрої відповідають, лише якщо вони перебувають у відповідному режимі роботи.

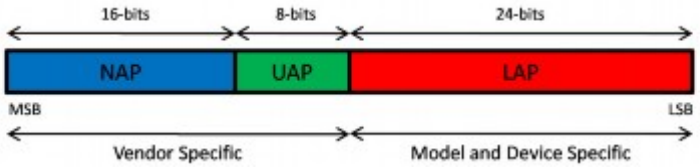

Рис. 2.12. Компоненти адреси пристрою Bluetooth

2.4. Забезпечення безпечного з'єднання між пристроями шляхом сполучення, аутентифікації та шифрування

2.4.1 Генерація ключа Bluetooth

Генерація ключів Bluetooth – це фундаментальний процес, який забезпечує безпеку бездротового з'єднання між пристроями. Цей процес передбачає створення унікальних криптографічних ключів, які використовуються для шифрування даних та аутентифікації під час встановлення з'єднання.

Коли двом пристроям потрібно безпечно обмінюватися даними, вони повинні пройти процес автентифікації та встановити ключ шифрування. Для цього необхідно згенерувати два ключі: ключ посилання (також відомий як ключ блоку) і ключ шифрування. Для генерації цих ключів обидві сторони мають використовувати спільний секретний персональний ідентифікаційний номер (PIN). PIN-коди Bluetooth містять 0–16 буквено-цифрових символів, але багато користувачів використовують лише 4 десяткові цифри, щоб PIN-код легко запам’ятати [33]. Процес генерації ключа посилання та ключа шифрування за допомогою алгоритму шифрування SAFER+ показано на рисунку 2.13.

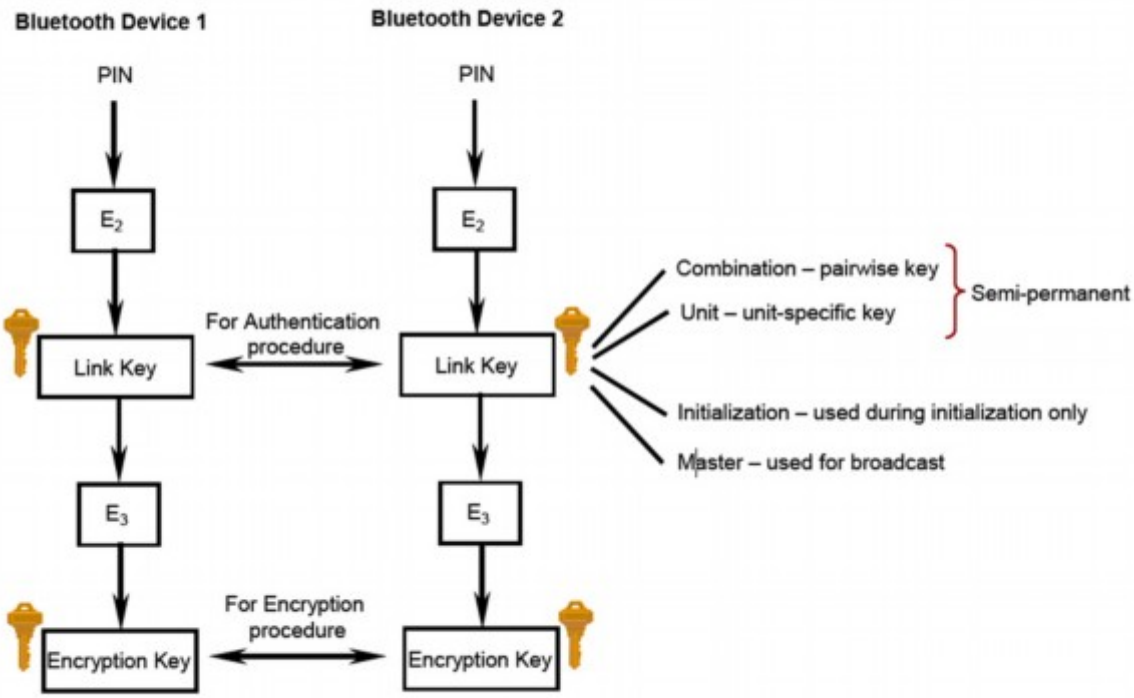

Рис. 2.13. Генерація ключа Bluetooth з PIN-коду

2.4.2. Bluetooth автентифікація до базової специфікації

Процес автентифікації може відрізнятися залежно від версії Bluetooth і рівня безпеки. Однак, загалом, він включає такі етапи:

- Ініціалізація: Один з пристроїв ініціює з'єднання.

- Обмін ключами: Пристрої обмінюються ключами шифрування, які використовуються для захисту даних під час передачі.

- Аутентифікація: Пристрої перевіряють один одного, використовуючи ці ключі. Це може включати введення PIN-коду або використання інших методів аутентифікації.

- Установлення з'єднання: Якщо автентифікація успішна, встановлюється захищене з'єднання.

До випуску специфікації Bluetooth Core Specification v2.1 + Enhanced Data Rate (EDR) взаємна аутентифікація двох підключаються пристроїв відбувалась за процесом, зображеним на рисунку 2.14. Хоча цей процес є

застарілим у контексті сучасних специфікацій, він залишається актуальним, оскільки значна кількість пристроїв Bluetooth, що використовуються сьогодні, були розгорнуті до оновлення найновішої специфікації [31].

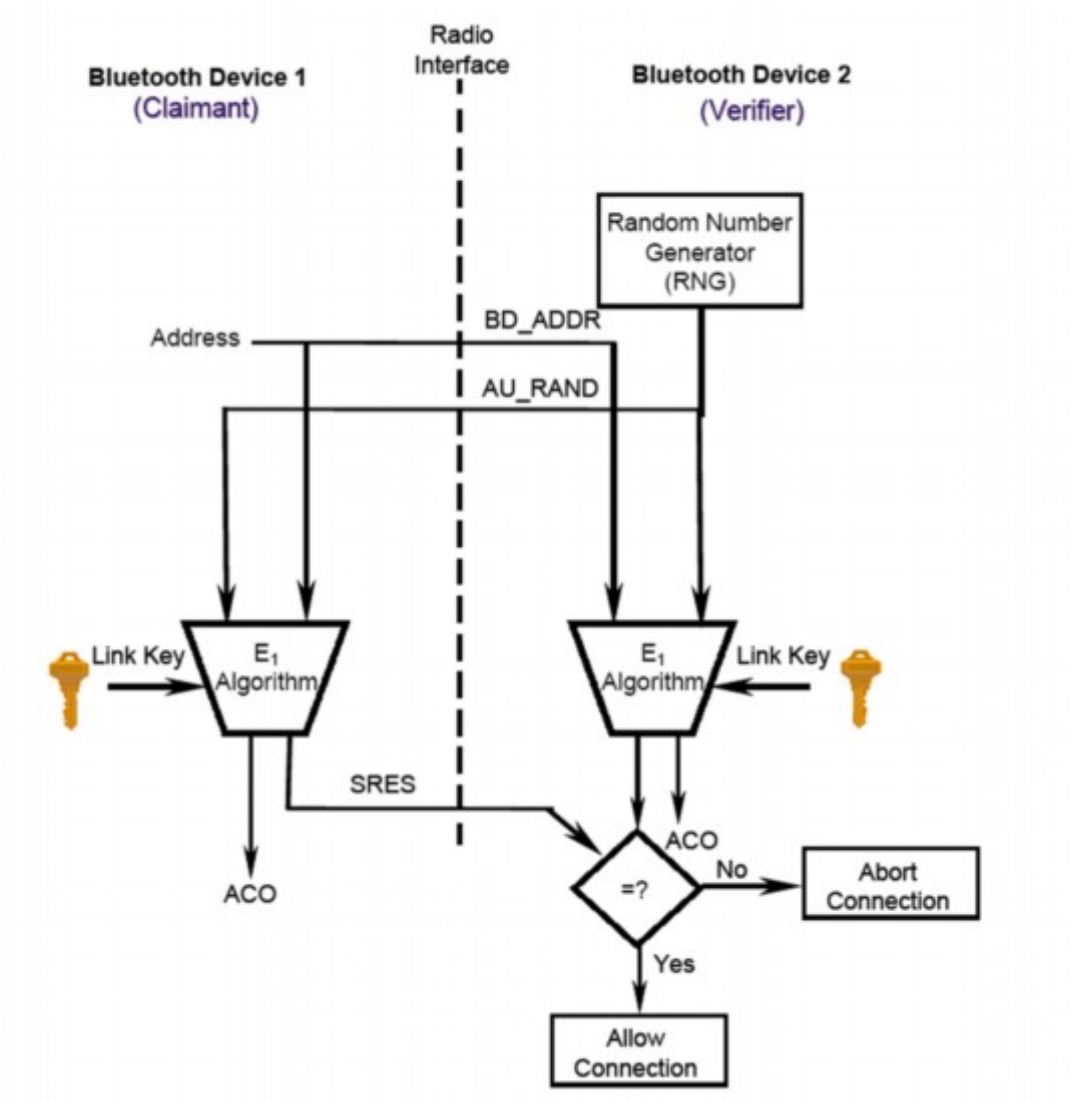

Рис. 2.14. Процес автентифікації Bluetooth

З метою підвищення рівня безпеки процесу автентифікації, Bluetooth SIG запровадив новий протокол, відомий як "безпечне просте сполучення". Цей протокол, детально описаний на рис. 2.15, базується на криптографічному алгоритмі обміну ключами Діффі-Хелмана на еліптичних кривих (ECDH) [31, 35], який значно ускладнює перехоплення та підробку ключів під час встановлення з'єднання.

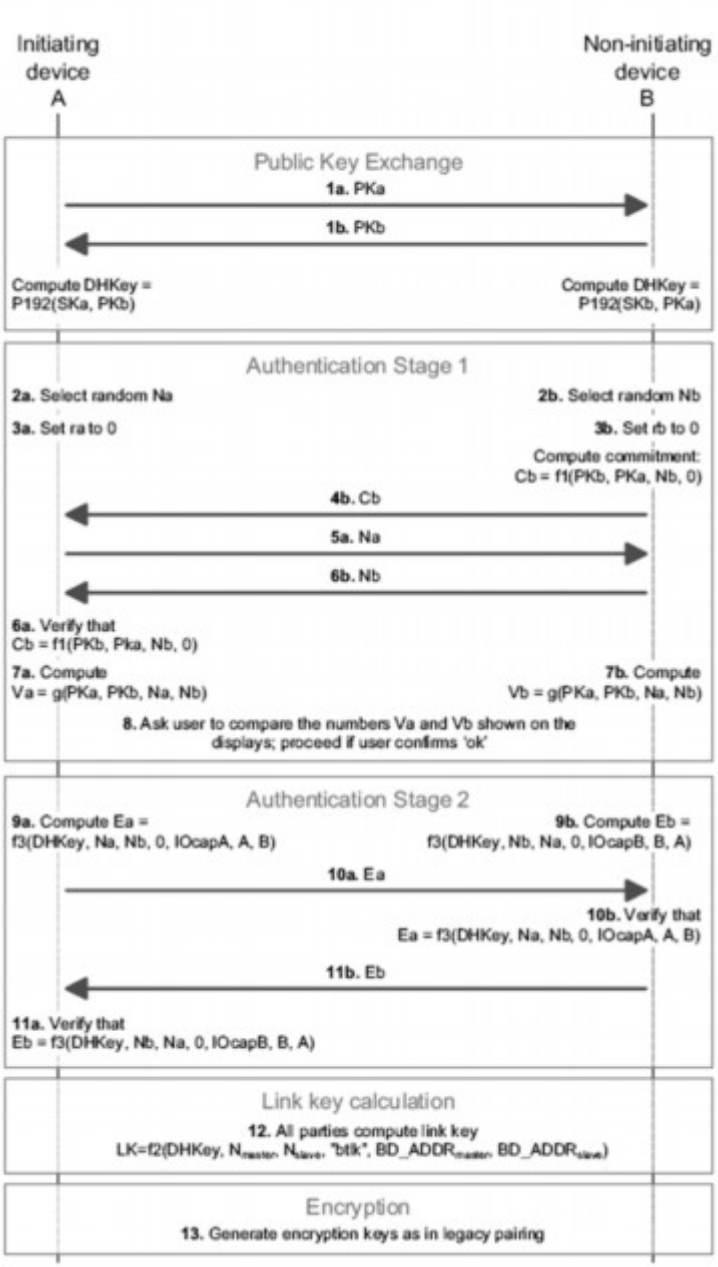

Рис. 2.15. Аутентифікація Bluetooth за допомогою Secure Simple Pairing

2.4.3. Процес шифрування

Після успішної автентифікації пари пристроїв з підтримкою Bluetooth, між ними встановлюється захищене криптографічне з'єднання. Цей процес передбачає генерацію спільного секретного ключа, який використовується для шифрування та дешифрування всіх даних, що передаються між пристроями.

Механізм генерації спільного ключа зазвичай базується на алгоритмах обміну ключами, таких як Diffie-Hellman або його еліптичної кривої аналог

ECDH. Ці алгоритми дозволяють двом сторонам встановити спільний секрет через незахищений канал, при цьому сам секрет залишається невідомим третім сторонам. Процес шифрування даних Bluetooth для передачі показаний на рисунку 2.16.

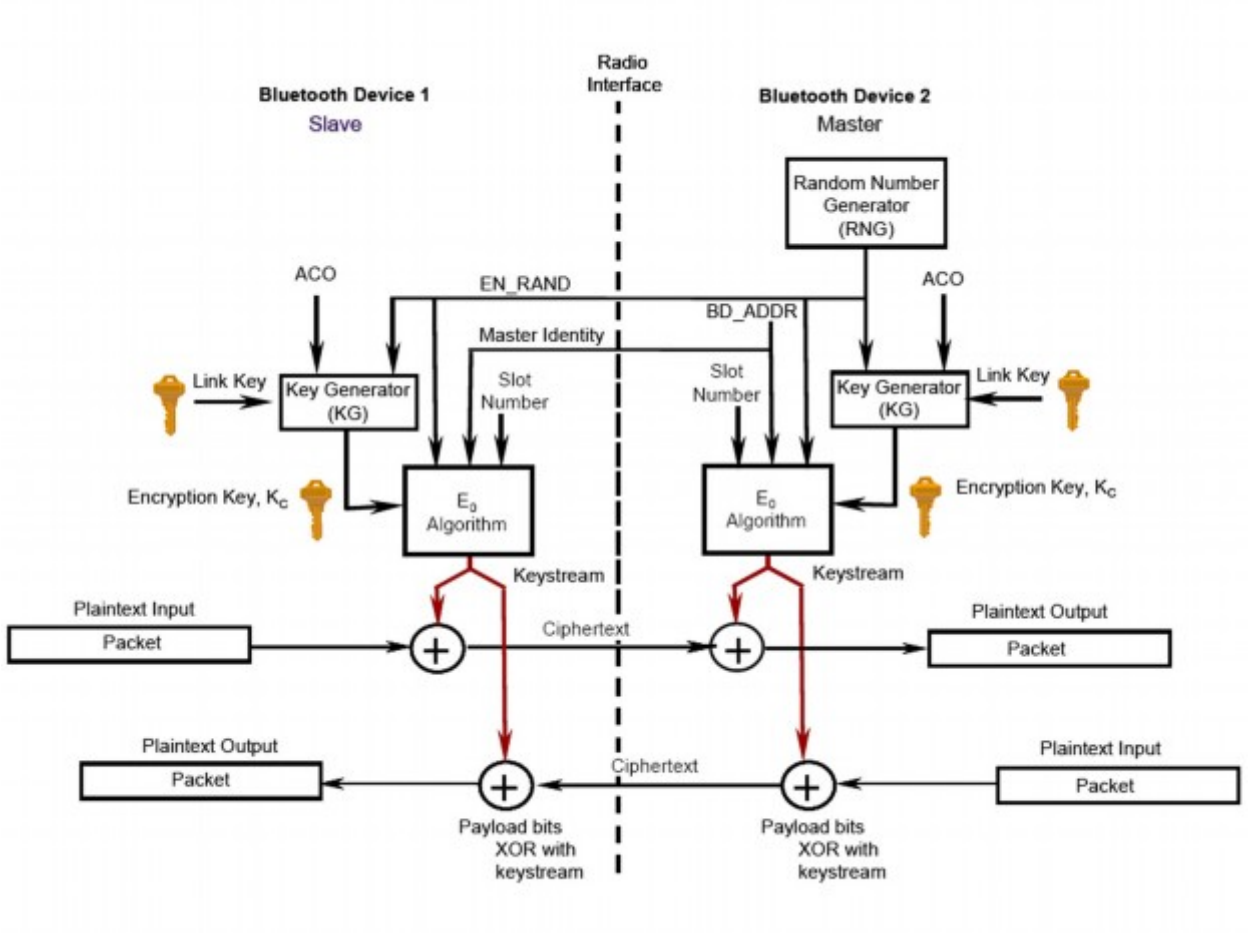

Рис. 2.16. Процес шифрування Bluetooth

2.4.4. Функції безпеки Bluetooth

Коли Bluetooth SIG розробляв специфікацію протоколу, вони робили це з урахуванням необхідності безпеки. Послуги безпеки, реалізовані специфікацією:

• Автентифікація: Ця функція безпеки намагається перевірити ідентичність двох пристроїв, які намагаються встановити зв’язок. Без нього пристрої не можуть бути впевнені, з ким вони спілкуються.

• Конфіденційність: ця функція безпеки намагається забезпечити конфіденційність пристроїв, які спілкуються, за допомогою засобів шифрування. Таким чином він намагається запобігти атакам підслуховування, під час яких зловмисники пасивно контролюють трафік.

• Авторизація: ця функція безпеки дозволяє контролювати доступ до ресурсів і їх використання.

Специфікація Bluetooth дозволяє пристроям Bluetooth працювати в одному з чотирьох різних режимів безпеки [31]:

• Режим безпеки 1: цей режим також відомий як незахищений режим. Він не забезпечує автентифікацію чи шифрування під час передачі Bluetooth.

• Режим безпеки 2: цей режим також відомий як режим безпеки рівня обслуговування. Він забезпечує автентифікацію та шифрування на рівні L2CAP, що означає, що безпека забезпечується між пристроями після встановлення з'єднання. У цьому режимі запроваджується служба безпеки авторизації, яка дозволяє контрольований доступ до служб на пристрої.

• Режим безпеки 3: цей режим також відомий як режим безпеки на рівні зв'язку. Він забезпечує автентифікацію та шифрування на рівні базової смуги, тобто процедури безпеки виконуються до підключення будь-якого пристрою.

• Режим безпеки 4: цей режим було введено, коли було випущено Bluetooth v2.1 + EDR. Він був просто створений для використання Secure Simple Pairing, що значно покращує процес взаємної автентифікації зв'язку Bluetooth.

Окрім режимів безпеки та режимів шифрування, специфікація Bluetooth також передбачає два різні рівні довіри. Довірені пристрої – це ті, які підтримують постійний зв'язок з іншим пристроєм, таким чином надаючи їм повний доступ або авторизацію до всіх служб. Ненадійні пристрої – це ті, які не підтримують постійний зв'язок з іншим пристроєм, тобто вони мають обмежений доступ до служб на іншому пристрої.

Для послуг також існують різні рівні безпеки. Безпека служби також є ще одним режимом безпеки Bluetooth, який пропонує три рівні підтримки:

• Рівень обслуговування 1: цей рівень вимагає авторизації та автентифікації. Довіреним пристроям автоматично надається доступ, а ненадійним потрібно авторизувати вручну.

• Рівень обслуговування 2: цей рівень вимагає лише автентифікації, авторизація не потрібна. Доступ до послуг надається після завершення процесу автентифікації.

• Рівень обслуговування 3: на цьому рівні обслуговування не потрібні автентифікація та авторизація. Доступ автоматично надається пристрою, що підключається.

2.4.5. Поточні недоліки безпеки

Незважаючи на значні досягнення в галузі безпеки Bluetooth, технологія все ще має певні вразливості, які можуть бути використані зловмисниками. Ось деякі з найпоширеніших недоліків:

1. Брутфорс-атаки на PIN-коди

Проблема: Багато пристроїв використовують чотиризначні PIN-коди для автентифікації. Це робить їх вразливими до підбору пароля (брутфорс-атак).

Рішення: Використання більш довгих і складних паролів, а також додаткових методів автентифікації, таких як біометричні дані.

2. Вразливості в старих протоколах

Проблема: Старі версії протоколу Bluetooth можуть містити вразливості, які можуть бути використані для несанкціонованого доступу до пристрою.

Рішення: Оновлення програмного забезпечення пристроїв до останніх версій, що містять виправлення безпеки.

3. Bluejacking та Bluesnarfing

Bluejacking: Несанкціонована відправка повідомлень на Bluetooth-пристрій.

Bluesnarfing: Несанкціонований доступ до даних на Bluetooth-пристрої.

Рішення: Увімкнення виявлення пристроїв і вимкнення Bluetooth, коли він не використовується.

4. Man-in-the-middle атаки

Проблема: Зловмисник може перехопити з'єднання між двома пристроями і підмінити дані.

Рішення: Використання шифрування з сильним ключем і перевірка автентичності пристроїв.

5. Вразливості в реалізації

Проблема: Помилки в програмній реалізації Bluetooth-протоколу на різних пристроях можуть призвести до вразливостей.

Рішення: Регулярне оновлення програмного забезпечення пристроїв.

6. Відсутність належної конфігурації

Проблема: Неправильна конфігурація параметрів безпеки Bluetooth може зробити пристрій більш вразливим.

Рішення: Дотримання рекомендацій виробника щодо налаштування безпеки Bluetooth.

Висновки до розділу

В даному розділі проведено дослідження, що охоплює основні аспекти забезпечення безпеки передачі даних, включаючи конфіденційність, автентифікацію, цілісність повідомлень та невідмовність. Ці елементи є важливими для побудови надійних систем захисту інформації, особливо в контексті бездротових мереж, де існує підвищена загроза несанкціонованого доступу до даних. Необхідність забезпечення цих принципів випливає з важливості захисту інформації під час передачі даних.

Також розділ містить аналіз протоколу TCP/IP та його застосування в середовищі Wi-Fi, що дозволяє краще зрозуміти механізми передачі даних у бездротових мережах. Цей аналіз надає контекст для розгляду безпеки в мережах на базі протоколу Bluetooth, де описуються архітектура та функції Bluetooth, структура його протокольного стека, а також механізми виявлення пристроїв та встановлення зв'язку між ними.

Розглянуто процедури шифрування та автентифікації, які є невід'ємними елементами забезпечення захисту під час створення пари пристроїв. Окремо аналізуються базові функції безпеки, інтегровані у протокол Bluetooth, що дозволяє виявити потенційні недоліки, які можуть стати вразливими місцями під час використання Bluetooth-пристроїв у сучасних мережах.

На додаток, проведено огляд методів виявлення вторгнень та аналіз їх реалізації у різних середовищах. Виявлення вторгнень є важливим аспектом підтримки безпеки мережевих середовищ, що дозволяє своєчасно виявляти загрози та запобігати можливим атакам на системи. Дослідження підкреслює важливість розуміння архітектурних особливостей та специфікацій технологій для розробки ефективних рішень у сфері інформаційної безпеки.

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ МОДЕЛЕЙ ТА АЛГОРИТМІВ ДЛЯ ПОБУДОВИ БАГАТОВЕКТОРНОЇ ПРОГРАМНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1. Особливості систем виявлення вторгнень

Спроба вторгнення — це можливість навмисної несанкціонованої спроби отримати доступ до інформації, маніпулювати інформацією або зробити систему ненадійною або непридатною для використання. Необхідність розпізнавати ці спроби вторгнення та реагувати на них призвела до розвитку IDS. IDS — це система безпеки, яка контролює комп'ютерні системи разом із мережевим трафіком для виявлення можливих атак [40].

Системи виявлення вторгнень (IDS) можна розгортати двома способами: моніторинг окремої системи або всієї мережі. Моніторинг єдиної системи називається хостом. Моніторинг цілих мереж на їхніх кордонах, захист кількох систем, відомий як мережевий IDS. IDS складаються з двох основних компонентів:

1. Датчики: ці пристрої відстежують мережевий трафік і записують зловмисні дії як події безпеки.

2. Консолі керування: ці пристрої дозволяють адміністраторам безпеки (SA) контролювати датчики та переглядати сповіщення. Консоль керування також можна використовувати для реєстрації записаних подій до централізованої бази даних для подальшого криміналістичного аналізу.

Системи виявлення вторгнень можуть контролювати комп'ютерні мережі різними способами, щоб розпізнавати шкідливі потоки пакетів. Їх можна розділити на три основні типи на основі підходу, який використовується для виявлення мережевих атак: системи на основі сигнатур, на основі аномалій та гібридні системи.

Системи виявлення вторгнень є важливим компонентом сучасних систем безпеки. Вони допомагають виявляти і запобігати різноманітним кіберзагрозам. Однак, для забезпечення максимального рівня захисту, IDS слід використовувати в комплексі з іншими засобами безпеки, такими як фаєрволи, системи виявлення вторгнень, системи управління доступом та ін.

3.1.1 Системи виявлення вторгнень на основі сигнатур

IDS на основі сигнатур побудовано на основі ідеї, що атаки можна розпізнати в першу чергу за потоком пакетів, які мають передбачувані шаблони, також відомі як підписи. Система порівнює вхідний трафік з відомими шаблонами атак (підписами). Якщо знаходить збіг, вона генерує сигнал тривоги.

Системи, які використовують IDS на основі сигнатур, широко використовуються в промисловості, оскільки вони часто дають дуже точні та конкретні результати виявлення. Недоліком використання IDS на основі сигнатур є те, що під час аналізу мережевого трафіку використовуватимуться лише відомі атаки в базі даних сигнатур. Якщо буде розроблено нову атаку, вона буде нерозпізнаною для IDS на основі сигнатур. Однак перевага використання системи на основі сигнатур полягає в тому, що як тільки нова атака стає відомою та зрозумілою, сигнатуру атаки можна додати до бази даних сигнатур атак IDS, щоб завжди розпізнавати атаку в майбутньому.

На рисунку 3.1 представлена загальна архітектура IDS на основі сигнатур. Є відомою розробка системи виявлення мережевих вторгнень (NIDS) для захисту мережі за допомогою алгоритму IDS на основі сигнатур. Йому вдалося перехопити пакети, надіслані через всю мережу, використовуючи змішаний режим, і порівняти трафік із сигнатурами атак дизайнера. Це захистило мережу та зменшило простір пам’яті в середовищі.

IDS на основі сигнатур не в змозі виявляти нові та невідомі атаки, оскільки базу даних сигнатур потрібно переглядати вручну для кожного нового типу виявленого вторгнення.

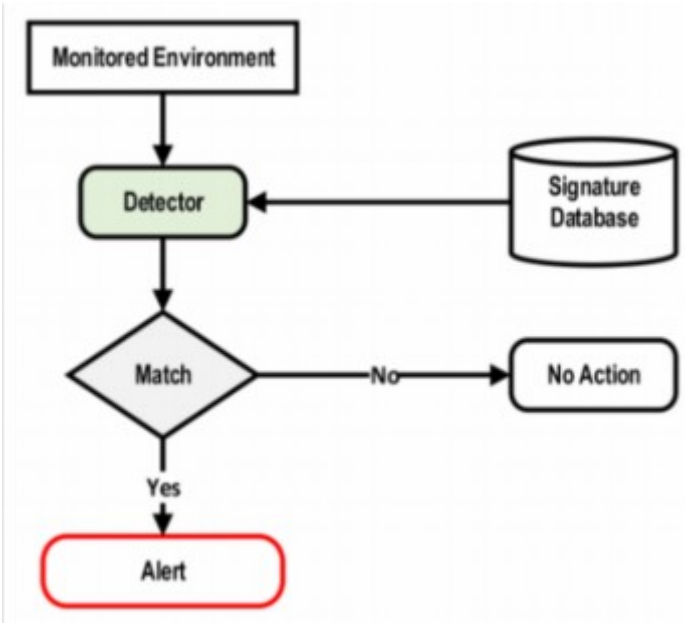

Рис. 3.1. Архітектура IDS на основі сигнатур

3.1.2. IDS на основі аномалій

IDS цього типу побудовані на передумові, що всі атаки є аномальними за своєю природою, тобто вони не слідують передбаченій моделі норм мережевого трафіку. Ці системи можна побудувати за допомогою двох різних підходів.

• Прогнозне розпізнавання образів: цей метод намагається передбачити майбутні події на основі тих, що вже відбулися. Ця система також використовує підписи, або правила, але не так, як традиційні IDS на основі підписів. Правила для цього типу системи базуються на ідеї, що події 1 і 2 відбулися, і, отже, передбачають, що є ймовірність X% події 3, Y% ймовірності події 4 та Z% ймовірності наступної події 5, і т. д. Якщо мережевий потік відповідає правилу шаблону прогнозування, IDS може позначити потік пакетів як втручаючий і створити сповіщення. Недоліком цього методу є те, що подія 6 може слідувати за подіями 1 і 2, але оскільки подія 6 не вказана в правилі, мережевий потік не буде позначено як втручаючий. Переваги цих систем полягають у тому, що вони виявляють послідовні шаблони, які колись було важко розпізнати, а також вони дуже адаптивні до змін, подібно до IDS на основі сигнатур [39].

• Статистичний аналіз: для використання цього методу спочатку генеруються профілі поведінки для точного зображення «нормальної» або базової поведінки системи. Для побудови профілю поведінки використовується кілька факторів, зокрема: час використання ЦП, підключення до мережі за період часу та інші показники активності. Коли система має профіль поведінки, вона може відстежувати мережевий трафік на наявність поведінки, яка відхиляється від базового профілю. Перевага використання статистичного аналізу полягає в тому, що з часом IDS може вивчати поведінку своїх користувачів. Однак це також передбачає серйозний недолік. Поступово, з часом, зловмисники можуть навчити систему вважати нав'язливі події або поведінку нормальною діяльністю [39].

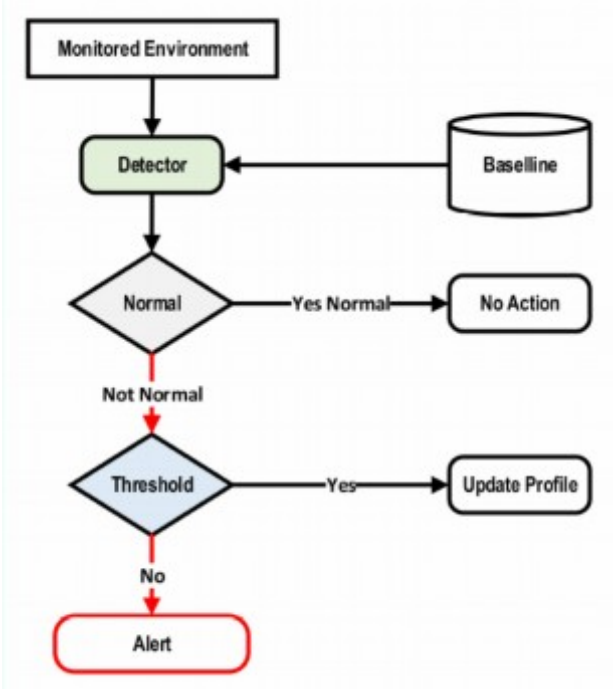

Рис. 3.2. Архітектура IDS на основі аномалій

IDS на основі аномалій виявляє неправильне використання в хмарному середовищі або проникнення та класифікує їх на нормальну та ненормальну поведінку користувачів за допомогою системи, яка збирає всю інформацію про нормальну поведінку або дії користувача протягом певного періоду часу. Потім виконується статистичний тест, щоб перевірити, чи підозрювана

поведінка пов’язана зі звичайною поведінкою користувача чи ні. На рисунку 3.2 представлена загальна архітектура IDS на основі аномалій. Складність підтримки цього типу IDS полягає в тому, що його неможливо оновити без втрати даних, на яких навчалася попередня система. Крім того, точність ідентифікації низька, що дає високу кількість помилкових спрацьовувань для цього типу системи.

Незважаючи на розглянуті переваги використання IDS на основі аномалій, є дві основні проблеми, які роблять IDS на основі аномалій менш бажаними для промислового використання. По-перше, вони ефективні лише тоді, коли правильні порогові значення встановлено як базову нормальну систему, що в більшості випадків важко зробити. Другий недолік полягає в тому, що через накладні витрати на відстеження мережевих потоків і зберігання інформації про стан ці системи дуже дорогі з точки зору обчислень і ресурсів.

3.2. Представлення схеми гібридної системи виявлення вторгнень на основі методів машинного навчання

Гібридна IDS просто використовує модуль на основі сигнатур і модуль на основі аномалій, щоб розпізнавати напади. Поєднуючи два підходи, гібридна IDS може використовувати переваги обох методів, одночасно пом’якшуючи недоліки кожної з систем.

Розглянемо архітектуру гібридної IDS на основі методів машинного навчання.

SVM застосовується для виконання фактичної класифікації мережевих даних на нормальну та ненормальну поведінку. Однак перед застосуванням алгоритму до набору даних його потрібно попередньо обробити, щоб алгоритм безперебійно працював на чистих і послідовних даних.

Процес починається із застосування генетичного алгоритму для вибору необхідної кількості ознак. На цьому етапі попередньо оброблені дані

подаються на вхід запропонованого генетичного алгоритму для вилучення оптимального набору ознак, оскільки вихідні дані складаються з високорозмірного набору ознак із 77 ознак, з яких вилучаються найкращі ознаки.

На наступному етапі набір даних цих ознак ділиться на тренувальний та тестовий набори. Потім до тренувального набору застосовується машина векторів опор, а потім обчислюється придатність.

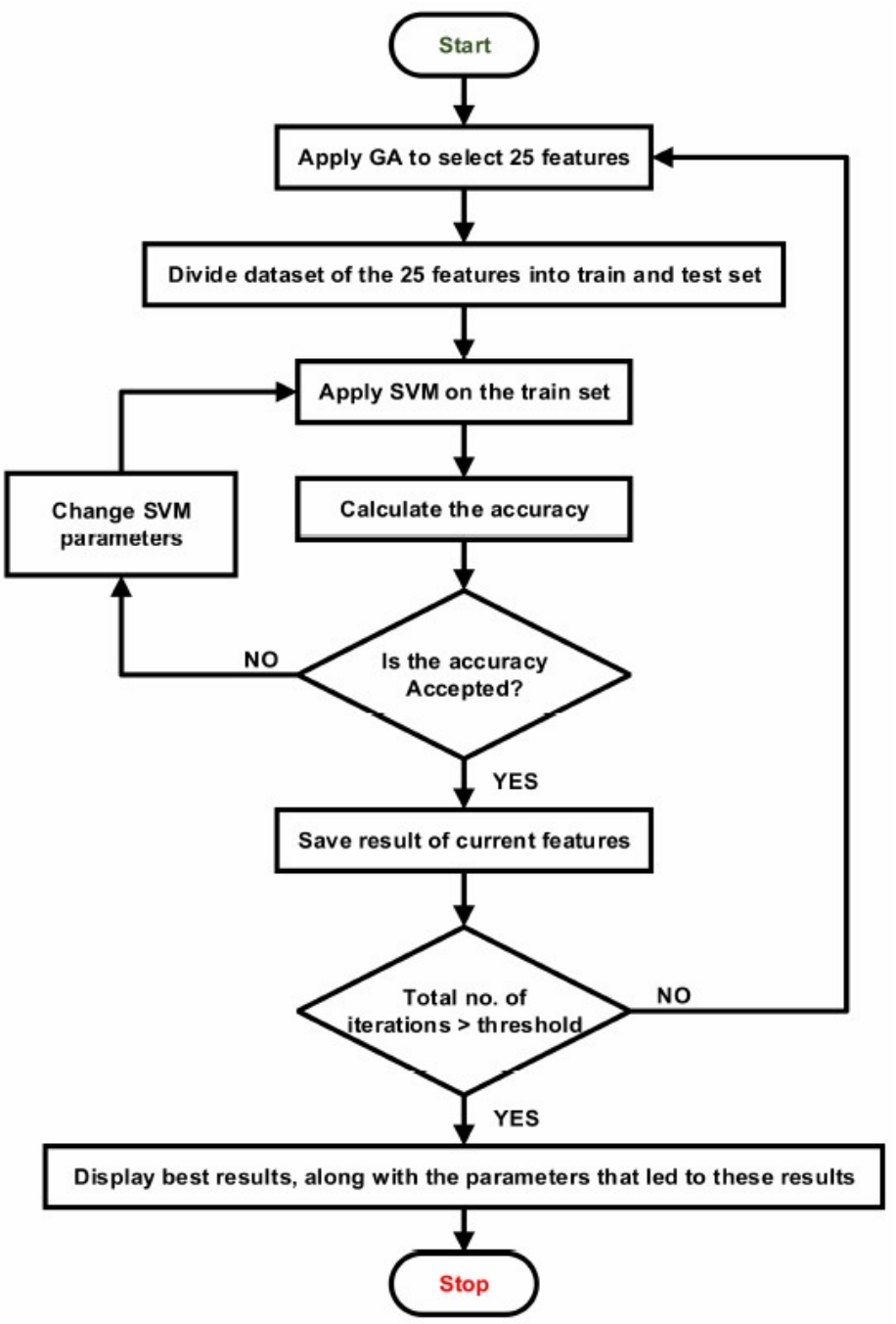

Рис. 3.3. Блок-схема запропонованої гібридної IDS

Якщо придатність не прийнята, змінюються параметри SVM, і SVM знову застосовується до тренувального набору для обчислення нової точності. Під не прийнятою мається на увазі, що точність менша за поріг. Поріг було встановлено на мінімальну точність, досягнуту іншими дослідниками, яка становила 94,86% [7]. Якщо результати прийняті, вони зберігаються для подальшого порівняння з результатами, отриманими з інших ітерацій різних виборів ознак. Наступним кроком є перевірка загальної кількості ітерацій; якщо вона більша за поріг, то ці результати разом із параметрами, які призвели до цих результатів, зберігаються, і процес зупиняється. Якщо ітерації менші за поріг, процес повторюється з першого кроку. На рисунку 3.3 показана блок-схема запропонованої гібридної IDS.

У цій роботі генетичний алгоритм на першому етапі виконувався для 100 поколінь. У кожному поколінні колекція ознак перевірялася за допомогою функції придатності на цьому зразку. Запропонований гібридний алгоритм IDS представлений в алгоритмі на рисунку 3.4.

Algorithm : Hybrid IDS using GA and SVM.

```
1: Apply Algorithm 1 to select features.
2: loop
3:    Create initial generation.
4:    for i=1 to n /*n is the number of folds*/
5:       Select 1/n of the population as a test set and (n−1)/n for training.
6:       Apply SVM to the current training set with specific hyperparameters.
7:       Evaluate the performance of the results using the fitness function.
8:    end for
```

Algorithm : *Cont.*

```
9:    performance of the current generation= average score of the results of n folds
10:   Save the results of step 6.
11: until the stop criteria are met.
12: Display the best result, along with the hyperparameters for the SVM that produced it.
```

Рис. 3.4. Гібридний алгоритм IDS

Отже, в цьому підрозділі представлено гібридну систему виявлення вторгнень для захисту даних у хмарних обчисленнях на основі

вдосконаленого генетичного алгоритму (GA) і алгоритму опорних векторних машин (SVM).

3.3. Особливості застосування гібридних систем виявлення вторгнень для мобільних пристроїв

Впровадження гібридної системи виявлення вторгнень у жодному разі не є новою чи новаторською ідеєю, але зробити це для PIDS за допомогою тригерів аномалії живлення в поєднанні з кореляцією атак Wi-Fi та Bluetooth у реальному часі – це сфера, яка досі не досліджена. Хоча цей підхід є інноваційним у багатьох відношеннях, він був би неможливий без багатьох попередніх дослідницьких зусиль. Енергозбереження в мобільних пристроях має першочергове значення. Якщо термін служби пристрою можна продовжити, користувачі можуть бути більш продуктивним і більш задоволеним використанням пристрою.

Очікування тривалого терміну служби батареї призвело до розробки системи Smart Battery System (SBS) [41]. SBS — це система, яка використовується для контролю, моніторингу та збереження заряду батареї в мобільних пристроях, починаючи від PID і закінчуючи мобільним медичним обладнанням. Інтелектуальна батарея використовує вбудовану електроніку для зберігання даних розумної батареї (напруги, струму, залишкової ємності, часу роботи до розрядження тощо) і робочих параметрів, що, у свою чергу, дозволяє SBS прогнозувати та оптимізувати роботу батареї протягом тривалого часу. час виконання мобільних пристроїв [41].

Advanced Power Management (APM) і Advanced Configuration and Power Interface (ACPI) були створені з метою стандартизації методів енергозбереження за допомогою використання загальноприйнятих у промисловості інтерфейсів конфігурації. APM — це багаторівневий стандарт програмного забезпечення на основі базової системи введення-виведення (BIOS), який дозволяє програмному забезпеченню вищого рівня взаємодіяти

з операційними системами та драйверами пристроїв, щоб зменшити енергоспоживання без необхідності знати апаратні інтерфейси [42]. Основна ідея APM полягає в тому, щоб контролювати енергоспоживання системи на основі активності системи, тобто, якщо активність системи зменшується, зменшується й енергоспоживання системних ресурсів.

ACPI — це галузева специфікація, яка базується на старішому стандарті APM для подальшого вдосконалення інтерфейсів програмування для цілей управління живленням. Метою цієї специфікації є створення загальногалузевого стандарту для конфігурації керування живленням материнської плати. Живленням можна вдосконалити та стандартизувати в галузевому масштабі за допомогою створення специфікацій APM та ACPI. Це не тільки спрощує сферу керування живленням у комп'ютерних системах, а й покращує продуктивність і дозволяє подовжити термін служби тих пристроїв, які використовують обладнання, що живиться від батареї.

В [44] визначено потребу у виявленні атак виснаження батареї та створив життєздатний прототип для портативних комп'ютерів, який міг би досягти цього на основі кожного процесу. Цей підхід використовував параметри продуктивності системи, такі як навантаження ЦП, читання/запис диска та мережеві передачі, щоб спочатку оцінити коефіцієнти кореляції за допомогою моделі множинної лінійної регресії. Таким чином, коефіцієнти можна використовувати для моделювання та оцінки енергоспоживання системи в цілому. За допомогою моделі оцінки потужності можна виявити розряд батареї, коли витрати електроенергії перевищують оцінку протягом тривалого періоду часу. Іншою особливістю IDS є здатність відображати енергоспоживання для кожного процесу. Кожен процес відстежується, щоб дозволити виявити процеси, які споживають велику кількість використання процесора. Оскільки використання процесора є найбільшим фактором енергоспоживання, процес, спрямований на розрядження акумулятора, матиме більше використання процесора, ніж більшість інших процесів у системі.

В [45] також намагалися вирішити проблему атак із розрядженням акумулятора, створивши систему виявлення вторгнень на основі акумулятора (B-BID). Це була перша IDS на основі аномалії живлення, призначена для захисту PID. B-BID містить три модулі для моніторингу енергоспоживання та кореляції аномалій із мережевими підключеннями.

• Механізм виявлення вторгнень на хост (HIDE): цей модуль є механізмом на основі правил, який намагається виявити аномалії енергоспоживання на основі характеристик енергоспоживання пристрою та статичних порогів на основі станів живлення PID.

• Scan Port Intrusion Engine (SPIE): Цей модуль працює подібно до netstat на настільному або портативному ПК. Netstat — це програма командного рядка, яка використовується для моніторингу вхідних/вихідних мережевих з'єднань, статистики мережевого інтерфейсу та таблиць маршрутизації. Після того, як HIDE виявить атаку, SPIE реєструє запущені процеси та інформацію про мережеве підключення, включаючи: позначку часу, IP-адресу джерела, IP-адресу призначення, порт джерела та порт призначення. Ці дані дозволяють провести криміналістичний аналіз для виявлення джерел атак.

• Механізм трасування сигнатур аналізу хоста (HASTE): цей модуль намагається ідентифікувати атаки на основі сигнатур витрат енергії, створених за допомогою швидкого перетворення Фур'є (ШПФ). HASTE використовує процес, який "відрізняє домінуючу частоту (x) від піків амплітуди (y), послідовно створюючи унікальні графіки xy, які ефективно відрізняють атаки"

Мережеві атаки, такі як віруси, хробаки, троянські коні та переповнення буфера, тепер стали повсюдно, оскільки кількість мережевих користувачів зросла. Snort [2], широко використовуваний і високо оцінений IDS, може бути використаний для боротьби з цими атаками та захисту мережевих активів шляхом моніторингу потоків мережевих пакетів на наявність шкідливих дій. Оскільки Snort прийнято як галузевий стандарт

виявлення вторгнень із безкоштовною ліцензією з відкритим вихідним кодом, його було вибрано для впровадження модуля Wi-Fi IDS для MVP-IDS.

Експлойти Bluetooth стали популярним вектором для зловмисників, головним чином через зростання ступеню, до якого технологія розгортається [48]. В [49] розроблено мережевий Bluetooth IDS для виявлення мобільних пристроїв, що піддаються атаці, у пікомережах Bluetooth. Після виявлення атак застосовуються відповідні заходи, такі як «приманки», неправдиві повідомлення та клонування цілей, щоб зірвати або запобігти подальшій атаці. Завдяки цьому IDS і зібраним ним даним багато атак Bluetooth тепер мають відомі сигнатури. Атаки можна виявити за допомогою аналізатора протоколу Bluetooth і механізму правил для збігу трафіку атаки. Крім того, оскільки ця робота зробила неймовірний прорив у виявленні вторгнень Bluetooth і створила сигнатури для типових атак Bluetooth, її сигнатури були використані для розробки BADSS, модуля Bluetooth IDS для MVP-IDS.

3.4. Реалізація концепції системи виявлення атак і підписів Bluetooth

Одним із недоліків реалізації B-SIPS є те, що не було практичного способу співвіднести аномалії IC з трафіком атаки Bluetooth. BADSS намагається вирішити цю проблему, розробивши окремий модуль для моніторингу та виявлення зловмисних з'єднань Bluetooth. Як згадувалося в попередніх розділах, відсутність необроблених сокетів була серйозною перешкодою для розвитку цього дослідження, оскільки це був теоретичний підхід до моніторингу всіх пакетів у реальному часі для трафіку Wi-Fi і Bluetooth. Оскільки в .NET Compact Framework також немає реалізації необроблених сокетів Bluetooth, для модуля BADSS також довелося використати альтернативний підхід. Доповнюючи попередню роботу, BADSS реалізує другий відомий Bluetooth IDS для атак зі збігом сигнатур із записаних потоків пакетів Bluetooth.

3.4.1. Структура класифікації атак Bluetooth

Оскільки Bluetooth є відносно новою технологією та специфікацією протоколу, усі вразливості та недоліки впровадження на даний момент не виявлено та не усунено. Завдяки цьому зловмисники змогли використовувати пристрої через середовище Bluetooth. У цьому дослідженні було зібрано список поширених атак Bluetooth, як показано в таблиці 3.1, і реалізовано структуру для класифікації кожної атаки для кращого розуміння.

Таблиця 3.1.

Класифікація атак Bluetooth

#	Attack	Focus	Exploit
1	RedFang	Device Discovery	Bluetooth Specification
2	Btscanner	Device Discovery	Bluetooth Specification
3	Tbear	Device Discovery	Bluetooth Specification
4	BluePrint	Service Discovery	Device Discovery
5	PSM Scan	Service Discovery	Device Discovery
6	RFCOMM Scan	Service Discovery	Device Discovery
7	BlueBug	Information Theft	Authentication
8	BlueSnarf	Information Theft	Authentication
9	Btcrack	Information Theft	Authentication
10	CarWhisperer	Information Theft	Authentication
11	Helomoto	Information Theft	Authentication
12	BlueSmack	Denial of Service	Buffer Overflow
13	Nasty vCard	Denial of Service	Buffer Overflow
14	L2CAP Header Overflow	Denial of Service	Malformed Packets
15	HCIDumpCrash	Denial of Service	Malformed Packets
16	Nokia N70 DoS	Denial of Service	Malformed Packets
17	Bluetooth Stack Smasher	Denial of Service	Malformed Packets
18	Ping of Death	Denial of Service	Resource Consumption
19	Tanya	Denial of Service	Resource Consumption
20	BlueSpam	Denial of Service	Device Discovery
21	Blueper	Denial of Service	Device Discovery

Кожна атака класифікується за такими трьома компонентами: назва, фокус і експлойт.

• Назва: це загальна або загальна назва атаки.

• Фокус: ця класифікація використовується для опису наміру атаки. Причини атаки на пристрій залежать від того, що отримує зловмисник, успішно використовуючи цільовий пристрій. У цьому дослідженні пропонується класифікувати атаку Bluetooth на 4 окремі категорії:

1. Виявлення пристроїв: атаки цього жанру зосереджені на виявленні пристроїв у зоні дії атаки та отриманні їхніх адрес пристроїв Bluetooth. Цей тип атаки в основному використовується як інструмент пасивної розвідки для отримання цінної інформації про цільовий пристрій перед фактичною атакою на нього. У невидимому режимі пристрій ніколи не відповідає на сканування або запит. Таким чином, якщо зловмисник хоче атакувати пристрій у невидимому режимі, він повинен спочатку якимось чином отримати адресу цільового пристрою Bluetooth. Прикладами інструментів, які реалізують виявлення пристроїв Bluetooth, є RedFang, Btscanner, Tbear.

2. Виявлення служби: атаки з цієї категорії спрямовані на отримання типів послуг Bluetooth, які цільовий пристрій здатний виконувати. Подібно до атак виявлення пристрою, атаки виявлення служб збирають інформацію про ціль. Прикладами інструментів, які реалізують атаки виявлення служби Bluetooth, є BluePrint, PSM Scan і RFCOMM Scan.

3. Крадіжка інформації: багато людей зберігають конфіденційну інформацію про PID, яка може завдати шкоди жертві в разі викрадення. Цей тип атаки зосереджений на проникненні в пристрій для викрадення конфіденційної інформації користувача. Прикладами інструментів, які здійснюють атаки на крадіжку інформації через Bluetooth, є BlueBug, BlueSnarf, Btcrack, CarWhisperer і Helomoto.

4. Відмова в обслуговуванні (DoS): DoS-атаки використовуються, щоб зробити деякі служби або ресурси пристрою недоступними. Це може означати тимчасову відмову в службі або спричинення несправності пристрою, що потребує скидання всієї системи. Атаки такого характеру зазвичай спрямовані на недолік програмної реалізації протоколу або специфікації. Прикладами інструментів, які реалізують атаки DoS через

Bluetooth, є BlueSmack, Nasty vCard, L2CAP Header Overflow, HCIDumpCrash, Nokia N70 DoS, Bluetooth Stack Smasher, Ping of Death, Tanya, BlueSpam і нова атака, розроблена в цьому дослідженні, Blueper.

• Експлойт: атаки успішні, оскільки зловмисники знайшли слабке місце в цільовому пристрої та використовують його як вразливість, яку можна використовувати. Це дослідження пропонує класифікувати експлойти Bluetooth на 6 різних категорій:

1. Специфікація Bluetooth: Ця класифікація дається атаці, яка найчастіше спрямована на виявлення пристрою та спрямована на розвідку інформації про пристрій. Немає точної помилки експлуатації, скажімо, успіх цього типу атаки базується виключно на протоколах і операціях, викладених для зв'язку в специфікації Bluetooth. Атаки, які використовують специфікацію Bluetooth, зазвичай спрямовані на збір цільових адрес пристроїв, щоб зловмисник міг здійснювати більш витончені та нищівні атаки. Прикладами Bluetooth-атак, які використовують специфікацію Bluetooth, є RedFang, BTScanner і Tbear.

2. Виявлення пристрою: як правило, атаки в цій категорії успішні насамперед через виявлення цільового пристрою. Користувачі Bluetooth можуть пом'якшити цей експлойт, вимкнувши служби Bluetooth, коли вони не використовуються, або зберігаючи пристрій Bluetooth у режимі невидимості під час звичайних операцій. Хоча пристрої Bluetooth можна виявити, коли вони перебувають у режимі невиявленості, це набагато складніше та вимагає від зловмисника набагато більше зусиль. Атаки, які використовують виявлення пристрою, зазвичай спрямовані або на подальшу розвідку інформації про цільовий пристрій шляхом виявлення служби, або на запуск атак DoS. Прикладами Bluetooth-атак, які використовують виявлення пристрою, є BluePrint, PSM Scan, RFCOMM Scan, BlueSpam і Blueper.

3. Автентифікація: цей експлойт здебільшого спрямований на пристрої, на яких реалізовано специфікацію Bluetooth до версії 2.1. У специфікації Bluetooth до версії 2.1 були відомі недоліки в процесі сполучення та

автентифікації, які мали на меті дозволити пристроям безпечно спілкуватися. Атаки, які використовують слабкі версії процесу автентифікації Bluetooth, зазвичай спрямовані на крадіжку інформації, надаючи зловмисникам доступ до того, що пристрої жертви вважали безпечними каналами зв'язку. Прикладами Bluetooth-атак, які використовують процес автентифікації, є BlueBug, BlueSnarf, BTCrack, CarWhisperer і Helomoto.

4. Переповнення буфера: переповнення буфера — це недолік реалізації програмного забезпечення, який виникає, коли процес намагається зберегти дані за межами призначеного діапазону пам'яті, виділеного для нього розробником. Цей експлойт не має нічого спільного зі специфікацією Bluetooth або її недоліками. Це безпосередньо пов'язано з недоліками в реалізації програмного забезпечення, головним чином через те, що програмісти нехтують перевіркою введених користувачем даних або отриманих пакетів. Прикладами Bluetooth-атак, які використовують цільові пристрої через переповнення буфера, є BlueSmack і Nasty vCard.

5. Неправильно сформовані пакети: Подібно до переповнення буфера, неправильно сформовані пакети спричиняють несправність пристроїв через програмні реалізації специфікації Bluetooth, які не перевіряють належним чином введені користувачем дані або пакети, отримані до обробки пакетних даних. Атаки, які реалізують цей експлойт, зазвичай більш складні та вимагають від зловмисника створення пакетів Bluetooth із недійсними параметрами. Зазвичай це досягається за допомогою команд сигналізації за межами діапазону або недійсної довжини сигналу. Прикладами Bluetooth-атак, які використовують цілі шляхом надсилання неправильних пакетів, є L2CAP Header Overflow, HCIDumpCrash, Nokia N70 DoS і Bluetooth Stack Smasher.

6. Споживання ресурсів: цей експлойт застосовний лише тоді, коли зловмисник запускає DoS-атаку. Специфікація Bluetooth встановлює стандартні способи реагування пристроїв на певні типи пакетів і служб протоколу. Завдяки цьому зловмисники можуть споживати ресурси

пристрою або пропускну здатність Bluetooth, постійно заповнюючи цільові пристрої запитами на ресурси. Атаки такого характеру в основному використовуються, якщо зловмисник хоче перешкодити зв'язку Bluetooth з іншими пристроями або розрядити батареї PID. Приклади атак Bluetooth, які використовують цілі через споживання ресурсів є Ping of Death і Tanya.

3.4.2. Дизайн і огляд модуля система виявлення атак і сигнатур Bluetooth

Модуль BADSS створено для розпізнавання атак Bluetooth і складається з двох основних компонентів:

1. Аналізатор протоколу Bluetooth Merlin II використовувався для захоплення пакетів Bluetooth та експорту цих захоплень у текстові файли.

2. BADSS Intrusion Detection Engine (IDE) обробляє кожен текстовий файл захоплення пакетів, намагаючись зіставити шаблони трафіку файлу Bluetooth із сигнатурами атак, які містяться в його базі даних сигнатур.

Модуль BADSS і всі його взаємодіючі компоненти можна побачити на рисунку 3.5.

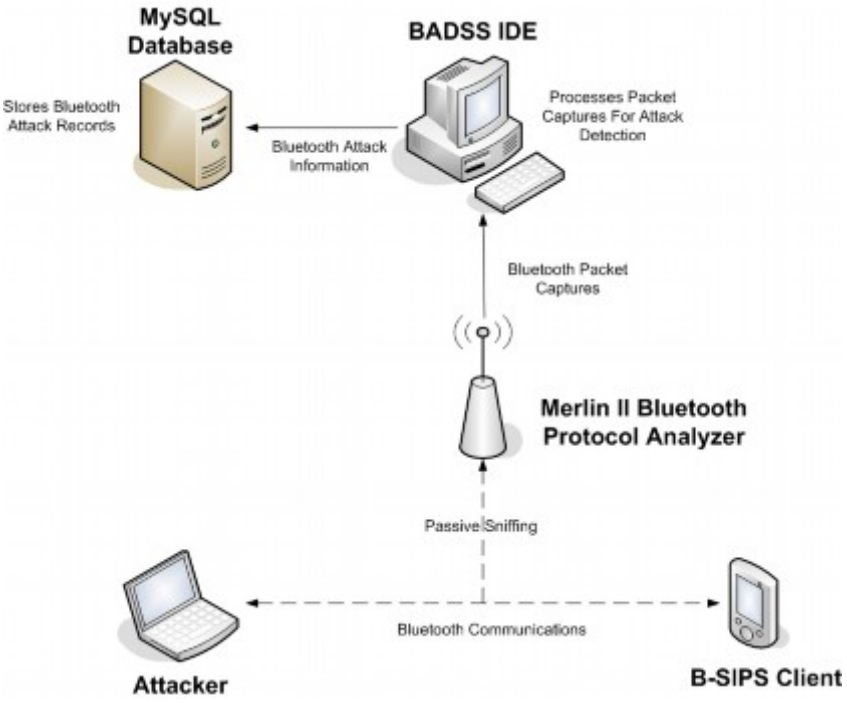

Рис. 3.5. Архітектура модуля BADSS

Щоб зрозуміти атаки Bluetooth, потрібно мати можливість побачити їх розкладання аж до рівня пакетів. Важко захиститися від атаки, не маючи можливості спостерігати за зв'язком між двома пристроями під час атаки. Щоб допомогти зрозуміти це, у цьому дослідженні використовувався протокол Bluetooth Merlin II.

Аналізатор, який дозволяв переглядати зв'язок Bluetooth на рівні пакетів. Merlin II не тільки захоплює передачі Bluetooth на рівні пакетів, але також має механізм препроцесора, який збирає кілька пакетів низького рівня в один пакет протоколу високого рівня, наприклад пакет LMP або L2CAP. Приклад захоплення пакетів Merlin II і повторного складання пакетів протоколу високого рівня показано на рисунку 3.6.

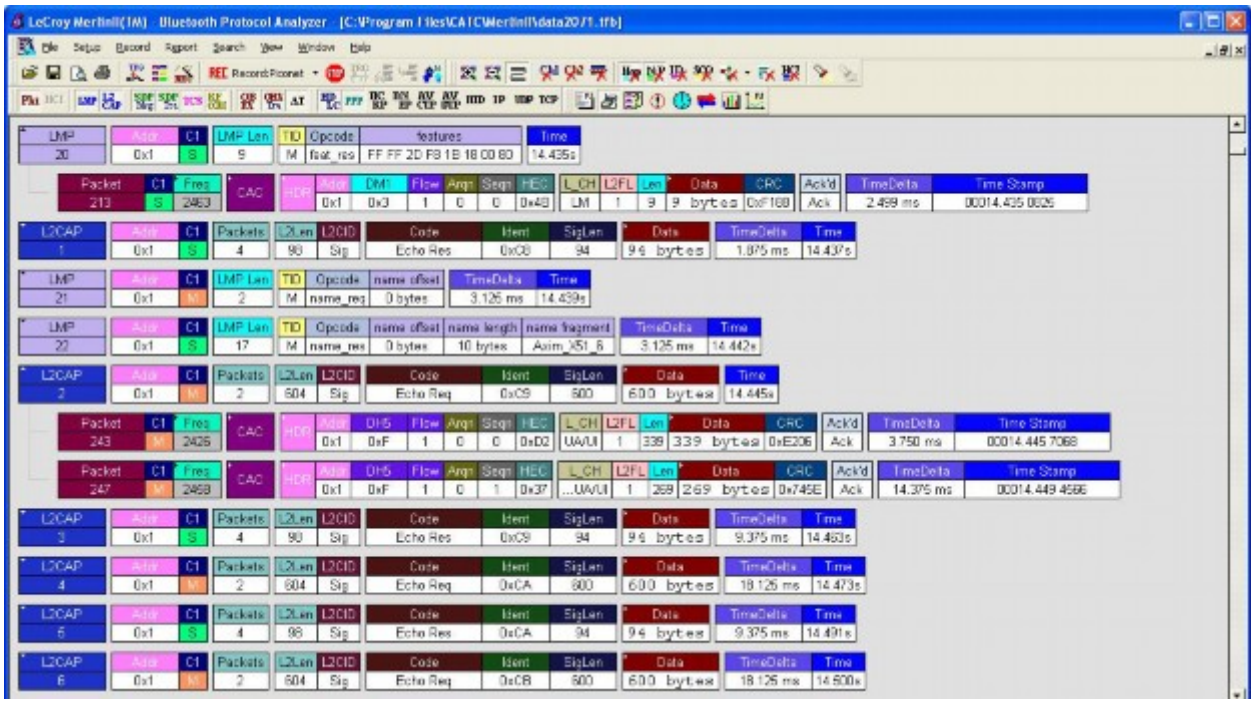

Рис. 3.6. Знімок екрана Merlin II із захопленням пакетів BlueSmack

3.4.3. Сигнатури для типових атак Bluetooth

Щоб розробити IDS на основі сигнатур для розпізнавання атак Bluetooth, необхідно створити сигнатури для типових атак. Раніше [49] розробив сигнатури атак на основі пакетів для всіх атак, крім двох,

перелічених у таблиці 3.1, а саме RedFang і Blueper. Ці дві нові атаки, а також пов’язані з ними сигнатури атак описані нижче.

1. RedFang: цей інструмент виявлення пристроїв використовується для пошуку пристроїв із підтримкою Bluetooth, які працюють у невидимому режимі в безпосередній близькості від зловмисника. Це інструмент грубої сили, який послідовно сканує адреси пристроїв Bluetooth неодноразово; надсилання запитів на ім’я на кожну адресу в діапазоні адрес пристрою Bluetooth, визначеному користувачем. Якщо пристрій відповідає на запит імені, зловмисник дізнається, що поблизу є пристрій із пов’язаною адресою пристрою Bluetooth. Коли цільовий пристрій відповідає на запит на ім’я, RedFang надсилає на цільовий пристрій запити версії та функцій, щоб надати зловмисникові ще більше цінної інформації. Коли зловмисник отримає адресу цільового пристрою Bluetooth, а також пов’язану з ним інформацію про пристрій, на ціль може бути здійснено більш складну та шкідливу атаку. Сигнатура атаки RedFang описана нижче та показана на рисунку 3.7.

Step:	Device	Action
1:	Attacker (Master)	Sends name request to target.
2:	Target (Slave)	Replies with name response.
3:	Attacker	Sends detach command terminating the connection.
4:	Attacker	Sends version request.
5:	Target	Replies with version response.
6:	Attacker	Sends feature request.
7:	Target	Replies with feature response.

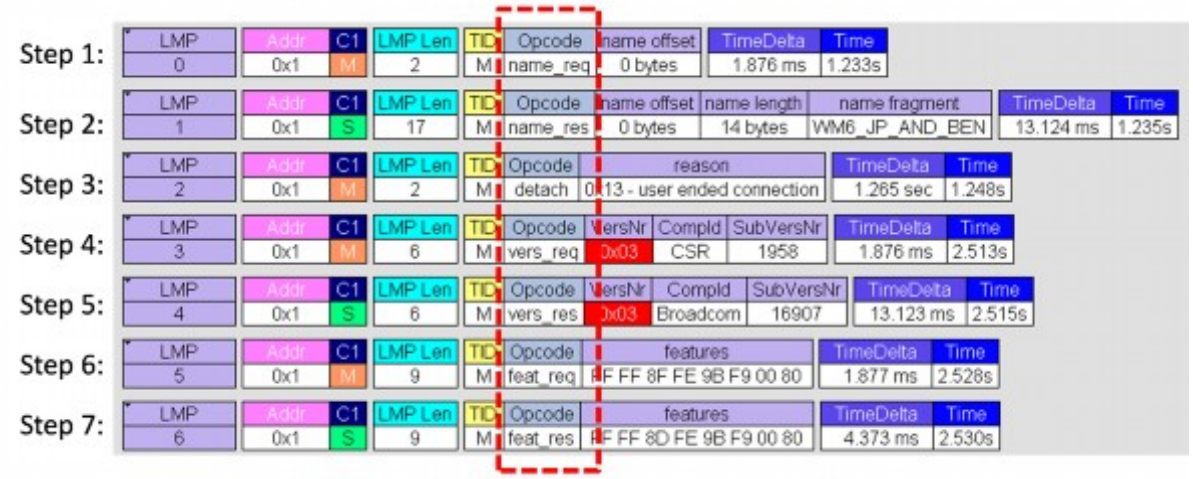

Рис. 3.7. Сигнатура атаки RedFang

Усі сім етапів спілкування між зловмисником і ціллю виконуються за 1,6 секунди або менше. Цей час було визначено шляхом повторного тестування та аналізу перехоплених пакетів RedFang. Багато доброякісних записів зв'язку Bluetooth законно містять ці пакетні транзакції для дійсного зв'язку. Тому для того, щоб розпізнати атаку RedFang, час має вирішальне значення.

2. Blueper: нещодавно розроблена атака спеціально для цього дослідження, Blueper спрямована на виснаження батареї та ресурсів пам'яті цільового PID. Для цього він використовує інструмент USSP-Push, щоб заповнити ціль вхідними файлами. Під час передачі файлу користувачеві пропонується виконати взаємодію, але водночас у фоновому режимі файл зберігається в пам'яті, доки користувач не підтвердить або не відхилить файл. Навіть якщо користувач відхиляє файл, атака не вплине, оскільки передача іншого файлу вже почалася. Зловмисник продовжує надсилати файли користувачеві, доки цільовий PID не вийде за межі діапазону, не вимкне радіо Bluetooth або повністю не розрядиться батарея PID. Сигнатура атаки Blueper описана нижче та показана на рисунку 3.8.

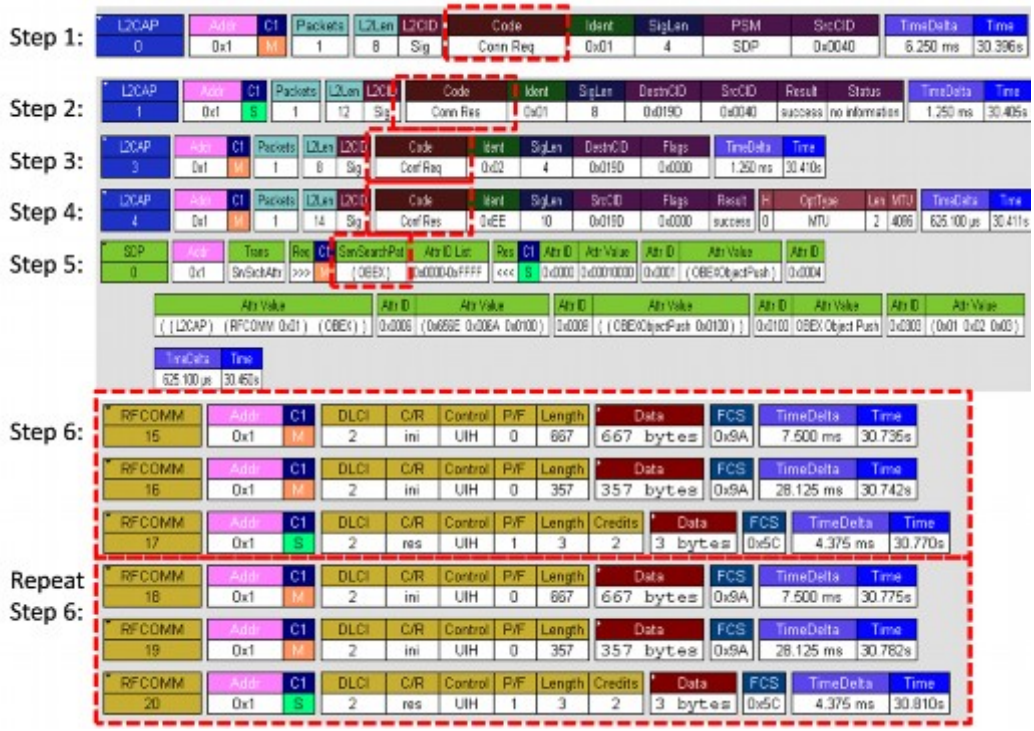

Рис. 3.8. Сигнатура атаки Blueper (початок)

Step:	Device	Action
1:	Attacker	Sends connection request to target.
2:	Target	Replies with connection response.
3:	Attacker	Sends configure request.
4:	Target	Replies with configure response.
5:	Attacker	Sends OBEX service search pattern.
6:	Attacker	Sends file through RFCOMM protocol.
7:	Attacker	Repeat Step 6.

Рис. 3.8. Сигнатура атаки Blueper (закінчення)

Оскільки кроки з 1 по 5 — це просто налаштування з'єднання, їх легко розпізнати. Однак кроки 6 і 7 виявляється значно важче виявити. Оскільки файли, надіслані зловмисником, можуть мати будь-який розмір, сигнатура атаки Blueper є дуже загальною. Він працює на основі зіставлення шаблонів, який намагається знайти повторювані набори пакетів, що передаються між зловмисником і цільовими пристроями, які є ідентичними. Коли буде досягнуто порогове значення для заданої кількості повторюваних шаблонів передачі файлів, сигнатуру атаки було успішно зіставлено.

BADSS IDE — це фактична програма, яка обробляє потоки пакетів Bluetooth і містить сигнатури атак для всіх атак, перелічених у таблиці 3.1. Вона приймає експортований текстовий файл, що містить потік пакетів Bluetooth від аналізатора протоколу Bluetooth Merlin II як вхідні дані. Потім він аналізує кожен пакет із текстового файлу та зберігає його в списку пакетів. Далі BADSS IDE намагається знайти збіги між трафіком у списку пакетів і сигнатурами атак, які зберігаються в базі даних сигнатур атак. Якщо збіг виявлено, BADSS IDE вставляє запис атаки в базу даних атаки BADSS.

3.4.4. Тестування розпізнавання атак

Як і більшість програмних систем, BADSS тестувалося поступово під час розробки. Коли кожен сигнатур атаки додавався до бази даних сигнатур, проводилися тести, щоб визначити належну функціональність. Для виконання цих тестів було отримано захоплення пакетів Bluetooth від [49] і

аналізатора Merlin II. Щоб сигнатура атаки була ефективною, вона повинна не тільки розпізнавати атаки, але й не створювати надто багато помилкових спрацьовувань для законного трафіку.

Після того, як усі сигнатури атак було додано до бази даних сигнатур атак BADSS IDE, комплексне тестування було виконано. Це включало збирання групи файлів захоплення пакетів Bluetooth, усі з яких послідовно аналізувалися BADSS IDE. Група із 104 файлів захоплення містила законний зв'язок Bluetooth, а також трафік Bluetooth, записаний від типових атак, перелічених у базі даних сигнатур атак BADSS IDE. Як показує таблиця 3.2 то BADSS IDE має 100% рівень виявлення атак, створюючи лише 2,97% хибнопозитивного виявлення.

Таблиця 3.2.

Показники виявлення атак BADSS із файлів захоплення пакетів

Attack	Detection Rate	False Positive Rate
RedFang	3/3	0/101
Btscanner	3/3	0/101
Tbear	3/3	0/101
BluePrint	3/3	0/101
PSM Scan	3/3	0/101
RFCOMM Scan	3/3	0/101
BlueBug	3/3	0/101
BlueSnarf	3/3	0/101
Btcrack	3/3	0/101
CarWhisperer	3/3	3/101
Helomoto	3/3	0/101
BlueSmack	3/3	0/101
Nasty vCard	3/3	0/101
L2CAP Header Overflow	3/3	0/101
HCIDumpCrash	3/3	0/101
Nokia N70 DoS	3/3	0/101
Bluetooth Stack Smasher	6/6	0/101
Ping of Death	3/3	0/101
Tanya	3/3	0/101
BlueSpam	3/3	0/101
Blueper	3/3	0/101
Total	**66/66 = 100%**	**3/101 = 2.97%**

BADSS IDE виявлятиме лише ті атаки Bluetooth, зазначені в її базі даних сигнатур атак, і якщо вони нові то їх можна легко додати як підпис

атаки. Це було зроблено для забезпечення зростання та реалізовано за допомогою наявності окремих модулів у BADSS IDE для кожної сигнатури атаки. Тому, якщо розроблено нову сигнатуру атаки, до бази коду додається модуль, і виклик цього модуля дозволить IDE BADSS розпізнати атаку з цього моменту. Як було показано і підтверджено цим дослідженням, атаки Bluetooth можуть бути розпізнані IDS на основі пакетів, якщо для моніторингу та аналізу зв'язку Bluetooth використовуються відповідні інструменти.

Модуль BADSS надзвичайно успішно впорався із завданням розпізнавання атак Bluetooth. BADSS IDE забезпечує 100% рівень виявлення атак із лише 2,97% коефіцієнтом помилкових спрацьовувань. Ці хибні спрацьовування виникають через законний трафік, який не відповідає специфікації Bluetooth. CarWhisperer — це атака Bluetooth, яка обходить процес автентифікації для захисту двостороннього з'єднання. Деякі законні захоплення пакетів, оцінені під час тестування, не відповідали специфікації, і тому BADASS IDE розпізнала їх як атаку.

Висновки до розділу

У розділі здійснено аналіз та імплементацію моделей і алгоритмів для побудови багатовекторної програмної системи виявлення вторгнень. Дослідження охоплює різні підходи до створення ефективних систем захисту, що поєднують сигнатурні та аномалійно-орієнтовані методи виявлення загроз, а також застосування гібридних систем з використанням методів машинного навчання.

Розглянуто сигнатурні системи виявлення вторгнень, які базуються на порівнянні мережевих подій з попередньо визначеними шаблонами загроз. Такий підхід забезпечує високу точність виявлення відомих типів атак, однак має обмеження у виявленні нових, невідомих загроз. Це спонукає до

використання додаткових методів для забезпечення більшої гнучкості та адаптивності системи.

Проаналізовано системи виявлення аномалій, які базуються на моделюванні нормальної поведінки мережі та виявленні відхилень від цієї поведінки. Такий підхід є більш чутливим до нових видів атак, проте може генерувати більшу кількість помилкових спрацьовувань. Це підкреслює важливість точного налаштування моделей для зниження хибнопозитивних результатів.

Представлено схему гібридної системи виявлення вторгнень, яка поєднує переваги сигнатурних та аномалійно-орієнтованих методів разом із можливостями машинного навчання. Використання алгоритмів машинного навчання дозволяє автоматизувати процес виявлення аномалій та вдосконалити розпізнавання нових загроз, забезпечуючи при цьому високу точність і швидкість аналізу даних.

Розглянуто особливості застосування гібридних систем виявлення вторгнень для мобільних пристроїв, зокрема виклики, пов’язані з обмеженими ресурсами таких пристроїв. Зазначено, що інтеграція гібридних систем в мобільні пристрої може підвищити ефективність захисту без суттєвого зниження продуктивності.

Реалізовано концепцію системи виявлення атак і підписів Bluetooth, що включає структуру класифікації атак та розробку модулів для виявлення загроз у бездротових мережах на основі Bluetooth. Зокрема, розроблено набір сигнатур для типових атак на Bluetooth-пристрої, що забезпечує можливість їх швидкого ідентифікації.

Проведено тестування системи розпізнавання атак, яке підтвердило ефективність розроблених алгоритмів та моделей у виявленні широкого спектра загроз, включаючи нові атаки на протокол Bluetooth. Результати тестування демонструють високу точність і швидкість виявлення, що свідчить про потенціал використання запропонованих підходів у реальних сценаріях.

ВИСНОВКИ

В магістерській роботі досліджено моделі та методи побудови багатовекторної програмної системи виявлення вторгнень. У дослідженні предметної області виявлення вторгнень та атак на програмні системи проаналізовано ключові аспекти, пов'язані з забезпеченням безпеки інформаційних систем. Розглянуто сучасні методи виявлення вторгнень, їх основні елементи та характеристики, що дозволяють ефективно виявляти загрози в різних середовищах.

Описано середовище дослідження та основні принципи роботи систем виявлення вторгнень, що дає змогу зрозуміти контекст, у якому функціонують ці системи. Важливим аспектом є розгляд особливостей роботи з різними типами атак та механізмів, що дозволяють ідентифікувати загрози.

Розглянуто методологію побудови багатовекторної портативної системи виявлення вторгнень (MVP-IDS), яка забезпечує високу ефективність завдяки використанню декількох підходів до виявлення загроз. Це включає поєднання сигнатурних та аномалійно-орієнтованих методів, що дозволяє більш точно ідентифікувати як відомі, так і нові види атак.

Надано детальний опис основних елементів методології, зокрема алгоритмів та моделей, що використовуються для ідентифікації загроз. Розглянуто вдосконалення MVP-IDS, які підвищують адаптивність та точність системи, забезпечуючи ефективний захист у динамічних середовищах з високим рівнем загроз.

Проведено аналіз характеристик різних пристроїв з точки зору їх вразливостей до атак та вторгнень. Цей аналіз дозволяє виявити слабкі місця у системах безпеки та розробити стратегії для їх зміцнення. Особливу увагу приділено пристроям, що використовуються у бізнесі та медицині, оскільки вони є особливо чутливими до атак і потребують надійного захисту.

Дослідження підкреслює важливість інтеграції нових підходів до виявлення загроз, які враховують швидку змінність сучасного кіберпростору. Запропоновані методи можуть стати основою для створення більш адаптивних і ефективних систем безпеки, що враховують різноманітні вектори атак та специфіку застосування в різних галузях.

Отже, ефективна система виявлення вторгнень має поєднувати декілька методологічних підходів, що дозволяє знизити ризик помилкових спрацьовувань та підвищити точність ідентифікації загроз. Використання сучасних алгоритмів та моделей є ключовим для створення надійних систем захисту, що відповідають потребам безпеки сучасних інформаційних середовищ.

Висновки розділу підкреслюють, що поєднання різних підходів до виявлення вторгнень, зокрема гібридних моделей на основі машинного навчання, є перспективним напрямом для забезпечення високого рівня безпеки в сучасних програмних системах. Реалізація таких рішень дозволяє ефективно протидіяти загрозам і забезпечувати надійний захист як для мобільних пристроїв, так і для мереж з підтримкою Bluetooth.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. T.K. Buennemeyer, "Battery-Sensing Intrusion Protection System (B-SIPS)," Doctoral Dissertation, Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg,VA, 2008.
2. Thomas S. Heydt-Benjamin Daniel Halperin, Kevin Fu, Tadayoshi Kohno, William H. Maisel, "Security and Privacy for Implantable Medical Devices," http://www.secure-medicine.org/PervasiveIMDSecurity.pdf, 2008.
3. Mike Roberts and Daniel Beaumont, "Bluetooth Brings Mobility to Health Care," Planet Wireless, pp. 11-15, 2002.
4. Larry Shaughnessy, "Double Amputee Walks Again Due to Bluetooth," http://www.cnn.com/2008/TECH/01/25/bluetooth.legs/index.html, 2008.
5. Barnaby J. Feder, "A Heart Device is Found Vulnerable to Hacker Attacks," http://www.nytimes.com/2008/03/12/business/12heart-web.html, 2008.
6. Tom Paulson, "Hackers can attack heart devices," http://seattlepi.nwsource.com/local/354617_defibhack12.html, 2008.
7. Declan McCullah, "Obama's new BlackBerry: The NSA's secure PDA?," http://news.zdnet.com/2100-9595_22-262060.html, 2009.
8. John McHale, "Wireless devices link soldiers on the digital battlefield," http://mae.pennnet.com/display_article/89485/32/ARTCL/none/none/1/Wireless-devices-link-soldiers-on-the-digital-battlefield/, 2001.
9. International Online Defense Magazine, "Secure PDA Phone," http://defense-update.com/products/s/secure-PDAP.htm, 2004.
10. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues For Ubiquitous Computing," Computer, vol. 35, pp. 22-26, 2002.
11. T. Martin, M. Hsiao, Ha Dong, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in Pervasive Computing and Communications (PerCom '04), pp. 309-318, 2004.

12. MSDN, "TCP/IP Raw Sockets," http://msdn.microsoft.com/en-us/library/ms740548.aspx, 2008.
13. LeCroy, "Merlin II Analyzers," http://www.lecroy.com/tm/products/ProtocolAnalyzers/MerlinII.asp?menuid=60, 2008.
14. Craig Freudenrich Ph.D. and Carmen Carmack, "How PDAs Work," http://electronics.howstuffworks.com/gadgets/travel/pda.htm/printable, 2009.
15. Mobile Tech Review, "What is a PDA?," http://www.mobiletechreview.com/genfaq.shtml, 2009. 95
16. Jo Best, "Analysis: What is a smart phone?," http://networks.silicon.com/mobile/0,39024870,39156391,00.htm, 2006.
17. Liane Cassavoy, "What Makes a Smartphone Smart?," http://smartphones.about.com/od/smartphonebasics/a/what_is_smart.htm, 2009.
18. David Needle, "Smartphones Take Center Stage," http://www.wi-fiplanet.com/news/article.php/3551686, 2005.
19. Gartner, "Gartner Says Worldwide Smartphone Sales Reached Its Lowest Growth Rate With 3.7 Per Cent Increase in Fourth Quarter of 2008," http://www.gartner.com/it/page.jsp?id=910112, 2009.
20. Michelle Megna, "2009 Smartphone Sales: Dipping Sharply," http://itmanagement.earthweb.com/cnews/article.php/3810521/2009%20Smartphone%20Sales:%20Dipping%20Sharply.htm, 2009.
21. William Stallings, Cryptography and Network Security: Principles and Practices, 4 ed. Upper Saddle River, NJ: Prentice Hall, 2006.
22. Microsoft MSDN, "Data Confidentiality," http://msdn.microsoft.com/en-us/library/aa480570.aspx, 2009.
23. Ed Skoudis with Tom Liston, Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Upper Saddle River, NJ: Pearson Education, Inc., 2006.

24. Andrew Tanenbaum, Computer Networks, Second ed. Englewood Cliffs, NJ: Prentice Hall, 1988.
25. Douglas Comer, Internetworking with TCP/IP vol. I: Principles, Protocols, and Architecture. Upper Saddle River, NJ: Prentice Hall, 1995.
26. Larry Peterson and Bruce Davie, Computer Networks: A Systems Approach, 4 ed. San Francisco, CA: Morgan Kaufman Publishers, 2007.
27. H. Labiod, H. Afifi, and C. De Santis, Wi-Fi, Bluetooth, Zigbee and WiMax. The Netherlands: Springer, 2007.
28. T. Karygiannis and L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices," http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf, November 2002.
29. J. Bray and C.F. Sturman, Bluetooth Connect Without Cables. Upper Saddle River, NJ: Prentice Hall PTR, 2001.
30. K. Scarfone and J. Padgette, "Guide to Bluetooth Security," http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf, 2009.
31. Denning, D.E. (1987). "An Intrusion Detection Model." IEEE Transactions on Software Engineering, 13(2), 222-232.
32. Lee, W., & Stolfo, S.J. (1998). "Data Mining Approaches for Intrusion Detection." Proceedings of the 7th USENIX Security Symposium, 79-93.
33. Lunt, T. (1993). "A Survey of Intrusion Detection Techniques." Computers & Security, 12(4), 405-418.
34. Kruegel, C., & Toth, T. (2003). "Using Decision Trees to Improve Signature-Based Intrusion Detection." Proceedings of the 6th International Workshop on the Recent Advances in Intrusion Detection (RAID).
35. Zhang, Y., & Lee, W. (2000). "Intrusion Detection in Wireless Ad-Hoc Networks." Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), 275-283.
36. Debar, H., Dacier, M., & Wespi, A. (2000). "A Revised Taxonomy for Intrusion Detection Systems." Annales des Télécommunications, 55(7-8), 361-378.

37. Sundaram, A. (1996). "An Introduction to Intrusion Detection." Crossroads ACM Student Magazine, 2(4), 3-7.
38. Gupta, B., Tewari, A., Jain, A.K., & Agrawal, D. (2018). "Big Data Security and Privacy Issues in Internet of Things." Lecture Notes in Networks and Systems, 94-124.
39. Kemmerer, R.A., & Vigna, G. (2002). "Intrusion Detection: A Brief History and Overview." IEEE Computer, 35(4), 27-30.
40. Roesch, M. (1999). "Snort: Lightweight Intrusion Detection for Networks." Proceedings of the 13th USENIX Conference on System Administration (LISA), 229-238.
41. Anderson, J.P. (1980). "Computer Security Threat Monitoring and Surveillance." Technical Report, James P. Anderson Co.
42. Almgren, M., & Jonsson, E. (2004). "Using Hidden Markov Models to Detect Intrusions." Proceedings of the 9th Nordic Workshop on Secure IT Systems.
43. Buczak, A.L., & Guven, E. (2016). "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
44. Xie, P., Tang, Y., & Wu, J. (2010). "A Bayesian Network Approach to Assessing the Reliability of Wireless Sensor Networks." Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems.
45. Shon, T., & Moon, J. (2007). "A Hybrid Machine Learning Approach to Network Anomaly Detection." Information Sciences, 177(18), 3799-3821.
46. Nguyen, H.L., & Ray, S. (2008). "A Real-Time Network Intrusion Detection System Using Adaptive Neural Networks." Proceedings of the 13th IEEE Symposium on Computers and Communications.
47. Wang, H., Zhang, Y., & Shin, K.G. (2002). "Detecting SYN Flooding Attacks." Proceedings of the IEEE INFOCOM Conference, 1530-1539.

48. Valdes, A., & Skinner, K. (2001). "Adaptive, Model-Based Monitoring for Cyber Attack Detection." Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX).
49. Mehra, P., & Kumar, S. (2018). "A Study on Hybrid Intrusion Detection System Using Machine Learning." Journal of King Saud University - Computer and Information Sciences.
50. Liao, H.J., Lin, C.H.R., Lin, Y.C., & Tung, K.Y. (2013). "Intrusion Detection System: A Comprehensive Review." Journal of Network and Computer Applications, 36(1), 16-24.
51. Can, Ö., & Sahingoz, O.K. (2015). "A Survey of Intrusion Detection Systems in Wireless Sensor Networks." Proceedings of the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO).
52. Mukherjee, B., Heberlein, L.T., & Levitt, K.N. (1994). "Network Intrusion Detection." IEEE Network, 8(3), 26-41.
53. Sommer, R., & Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." IEEE Symposium on Security and Privacy, 305-316.
54. Bace, R.G., & Mell, P. (2001). "NIST Special Publication on Intrusion Detection Systems (IDS)." National Institute of Standards and Technology (NIST).