Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Войченко Роман Олександрович

на здобуття ступеня вищої освіти магістра

Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 2301149.23.01.17 ПЗ

Виконав студент 2 курсу група КБЗІм-23 Роман ВОЙЧЕНКО

Керівник . техн. наук, доцент Юрій КЛЬОЦ

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Магістр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Войченку Роману Олександровичу

1 Тема роботи Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT

Керівник роботи канд.техн.наук, доцент Кльоц Юрій Павлович

Затверджено наказом ректора університету від 26 08 2024 № 60

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи : Виявлення аномалій поведінки пристроїв у безпроводових мережах IoT

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз фону алгоритму виявлення аномалій. Розробка фреймворку IOT-AD ,для виявлення аномалій серед взаємопов'язаних пристроїв. Реалізація методу виявлення аномальної поведінки у безпроводових мережах IoT. Дослідження аномалій в лініях зв'язку IoT мереж. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 02 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі	15.09.2024	Виконано
Визначення змісту, структури кваліфікаційної роботи	22.09.2024	Виконано
Підготовка першого розділу кваліфікаційної роботи	29.09.2024	Виконано
Підготовка другого розділу кваліфікаційної роботи	10.10.2024	Виконано
Підготовка третього розділу кваліфікаційної роботи	20.10.2024	Виконано
Підготовка статті/тези за темою кваліфікаційної роботи	4.11.2024	Виконано
Підготовка четвертого розділу кваліфікаційної роботи	17.11.2024	Виконано
Підготовка та оформлення ілюстративного матеріалу	24.11.2024	Виконано
Оформлення кваліфікаційної роботи	24.11.2024	Виконано
Попередній захист кваліфікаційної роботи	27.11.2024	Виконано
Захист кваліфікаційної роботи на засіданні ЕК	19.12.2024	Виконано

Студент _____ Роман ВОЙЧЕНКО

Керівник кваліфікаційної роботи _____ Юрій КЛЬОЦ

АНОТАЦІЯ

Тема кваліфікаційної роботи магістра: “Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT”

Автор роботи: Войченко Р.О.

Керівник роботи: Юрій КЛЬОЦ

Пояснювальна записка: 73 ст., 32 рис., 11 таб., - додат., 90 джерел.

Ключові слова: Інтернет речей (IoT), виявлення аномалій, аномалії мережевий трафік, аномалії взаємодії з пристроями, безпроводові мережі.

Об’єктом дослідження є пристрої у безпроводових мережах IoT.

Предметом дослідження є аномальна поведінка у безпроводових пристроях.

Наразі більшість методів виявлення аномалій в IoT передбачають значну участь людини та оптимізацію для локальних рішень. Теоретично аномалію легко зрозуміти, і фахівець із домену помітить аномальні дані, якщо йому дадуть достатньо часу. Однак існує кілька труднощів у розробці автоматизованої моделі в середовищі IoT. Це складно та не завжди можливо правильно визначити та класифікувати всі типи аномальних даних, особливо коли позначені навчальні дані доступні/недоступні лише частково.

В роботі було розглянуто проблему виявлення аномалій або вторгнень в мережі IoT. Потім було вибрано набір даних про мережеву активність з декількома атаками, який регулярно використовується для розробки NIDS і як орієнтир пропозицій. Далі представлено дизайн IoT-AD, який використовує механізми для виявлення аномалій на рівні пакетів, пов'язаних із взаємодією між пристроями IoT, також було розглянуто процес вибору пристрою, який може виступати в якості контролера IoT-AD, в останньому розділі розглянуто чотири типи аномалій, які можуть бути присутніми в безпроводових лініях зв'язку і корисні для виявлення в реальних операційних розгортаннях IoT.

11.12.24

ANNOTATION

Theme qualification work: "Method of detecting anomalous behavior of devices in IoT wireless networks"

Author of the work: Voichenko R.O.

Head of work: Yuriy KLOTS

Explanatory note: 73 pages, 32 figures, 11 tables, - addendum, 87 references.

Keywords: Internet of Things (IoT), anomaly detection, network traffic anomalies, device interaction anomalies, wireless networks.

The object of research is devices in wireless IoT networks.

The subject of research is anomalous behavior in wireless devices.

Currently, most IoT anomaly detection methods involve significant human involvement and optimization for local solutions. In theory, an anomaly is easy to understand, and a domain expert will spot anomalous data given enough time. However, there are several challenges in developing an automated model in an IoT environment. It is difficult and not always possible to correctly identify and classify all types of anomalous data, especially when the labeled training data is only partially available/unavailable.

The paper considered the problem of detecting anomalies or intrusions in the IoT network. A multi-attack network activity dataset was then selected, which is routinely used for NIDS development and as a reference for proposals. Next, the design of IoT-AD is presented, which uses mechanisms to detect anomalies at the packet level related to the interaction between IoT devices, the process of selecting a device that can act as an IoT-AD controller was also discussed, and the last section discusses four types of anomalies , which may be present in wireless communication lines and useful for detection in real operational IoT deployments.

11.12.24

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT – Internet of Things (Інтернет речей)

IoT-AD – IoT Anomaly Detector (Виявляє аномальну поведінку пристроїв)

LSTM – Довгострокова пам’ять

CNN – Згорткова нейронна мережа

AE – Авктокодер

SVM – Класифікатор опорних векторних машин

KNN – K-Nearest Neighbors

DT – Decision Tree

RF – Random Forest

NN – Neural Network

RSSI – Індикатор потужності прийнятого сигналу

SNR – Співвідношення сигнал/шум

PSD – Спектральна щільність потужностей

NUC – Intel Next Computing

ВСТУП

У середовищі Інтернету речей (IoT), наприклад, у розумному будинку, може бути багато взаємопов’язаних пристроїв. У таких умовах несправний або скомпрометований пристрій IoT може впливати на роботу інших. Інакше кажучи, аномальна поведінка одного пристрою здатна поширюватися на інші елементи мережі IoT.

У цій роботі зазначається, що не менш важливим завданням, ніж виявлення аномальної поведінки, є запобігання її поширенню серед інших пристроїв. Відповідно до цього запропоновано фреймворк IoT Anomaly Detector (IoT-AD), який може не тільки ідентифікувати аномальні пристрої, але й обмежувати вплив їхньої поведінки та відновлювати нормальну роботу системи.

Було створено прототип IoT-AD, який тестували на відкритих наборах даних пристроїв IoT, а також у реальному середовищі з невеликим тестовим стендом. Додатково IoT-AD порівнювали з існуючими підходами. Результати показали, що цей фреймворк здатен виявляти аномалії менш ніж за 2,12 мілісекунди з точністю дев’яносто вісім відсотків.

Наразі більшість рішень для виявлення аномалій в IoT передбачають значну участь людини й орієнтовані на локальні задачі. Хоча теоретично аномалії можна виявити, якщо надати експерту достатньо часу, автоматизація цього процесу стикається з низкою викликів. Зокрема, не завжди можливо правильно ідентифікувати та класифікувати всі типи аномальних даних, особливо за обмеженої доступності позначених навчальних наборів.

Крім того, поняття "нормальної поведінки" у багатьох сферах постійно змінюється та еволюціонує, що ще більше ускладнює задачу автоматизації.

Одним із таких прикладів є зміна кількості домогосподарств, що призводить до зміни попиту на електроенергію. Крім того, дані часто містять шум, і коли відношення сигнал/шум низьке, величина шуму нагадує справжні аномалії. Складність зростає в міру збільшення кількості взаємопов'язаних систем і різноманітності типів вхідних даних .

Виявлення аномалій у середовищі Інтернету речей (IoT) охоплює широкий спектр застосувань, деякі з яких уже значно розвинені, як-от мережева безпека, тоді як інші мають великий потенціал для зростання. Література на цю тему є різноманітною та розширюється, оскільки кількість публікацій постійно зростає, що вимагає регулярного оновлення аналізу.

Ця робота доповнює існуючі дослідження шляхом розширення класифікації алгоритмів виявлення аномалій та глибокого аналізу ключових тенденцій у цій галузі. У 2019 році пристрої IoT стали мішенню для 100 мільйонів атак лише за першу половину року. Очікується, що до 2025 року кількість IoT-пристроїв перевищить 64 мільярди. Через це захист пристроїв і мереж IoT, включаючи критично важливі об’єкти, як-от медичне обладнання чи автономні транспортні засоби, набуває все більшого значення.

Ситуація ускладнюється через велику кількість різновидів атак, їхню еволюцію, а також обмежені обчислювальні ресурси та ресурси пам’яті, доступні для IoT-пристроїв. Виявлення аномалій є критично важливим, оскільки навіть рідкісні аномалії можуть надати цінну інформацію в таких галузях, як медицина, фінанси, управління трафіком, енергетика та промислове виробництво. Наприклад, в азартних іграх методи виявлення аномалій використовуються для аналізу торгівельних моделей з метою виявлення інсайдерської діяльності, а в промисловості вони забезпечують безпеку обладнання під час виробництва.

1 АНАЛІЗ ФОНУ АЛГОРИТМУ ВИЯВЛЕННЯ АНОМАЛІЙ В IoT

Аномалія — це точка даних, яка не відповідає очікуваній поведінці у змодельованій системі. Вони представляють собою рідкісні події або спостереження, які суттєво відхиляються від звичних моделей або поведінки, що проявляються у певній точці даних, конкретному контексті, часовому інтервалі (наприклад, сезон або квартал) або в цілому наборі даних.

Основне завдання алгоритму виявлення аномалій полягає у виявленні місця їхнього виникнення та класифікації або визначенні причини їх появи.

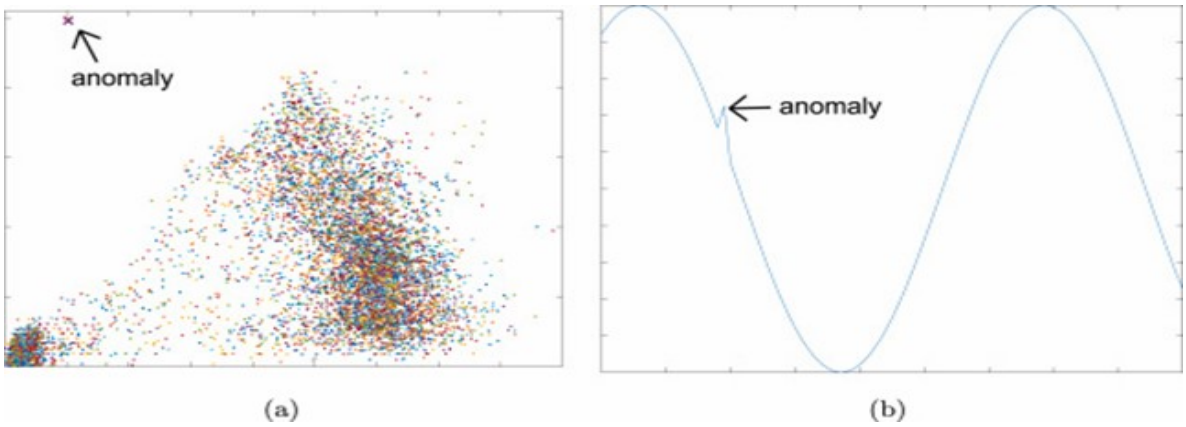

Рисунок 1.1 – Відображення аномалії в IoT

У бінарній класифікації аномаліївирішальною є апроксимаційна модель, яка найкраще відповідає очікуваній поведінці даних. Крім того, складність багатьох ситуацій вимагає окремої стратегії виявлення для кожної програми [1]. Приклади аномалій показано на рисунку 1.1.

1.1 Виявлення аномалій Інтернету речей

IoT класифікується на чотири категорії, які були створені на основі об’єднання класифікацій з попередніх досліджень, зокрема [2], [3]. Ці категорії визначаються залежно від підходу до вирішення проблеми, способу застосування,

типу використовуваного методу та затримки алгоритму. Ілюстративний огляд цих чотирьох категорій представлено на рисунку 1.2.

Цей розділ пропонує короткий опис класифікації аномалій, а також огляд деяких традиційних підходів, що застосовуються в контексті IoT.

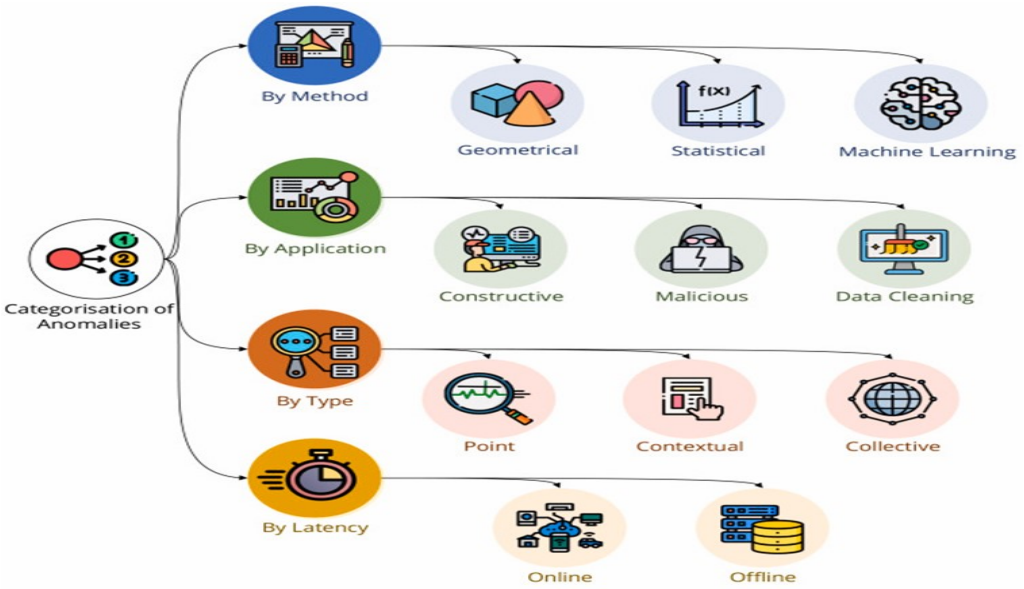

Рисунок 1.2 – Інформаційно - графічний огляд категоризації аномалій

За методами існують такі як геометричні, статистичні або машинне навчання. Геометричні методи базуються на припущенні, що коли стратегії на основі відстані та щільності представляють заданий набір даних, очікувані та аномальні дані розділяються.

У наборі точок даних ідея ізоляції або методів на основі щільності полягає в тому, що аномалії з'являються в розріджених областях . У цих методах для класифікації аномалій використовується або статичне, або динамічне порогове значення ' t ' для оціненої відстані 'd', яке подається як: (1) $d =< t$, Нормальний (нижче порогу)$> t$, Аномалія (вище порогу) Статистичні методи , такі як мінімальний обсяг спробувати змоделювати нормальні дані за допомогою математичних моделей і розподілів.

Підхід до мінімального об'єму спрямований на побудову nn-вимірного симплексу навколо хмари даних, яка представляє базову істину. Мета цього підходу — мінімізувати зайнятий об'єм симплексу, максимально включаючи точки даних

базової істини. Аномалії визначаються як дані, що знаходяться поза межами симплексу.

Ще одним методом прогнозування є експоненціальне згладжування, яке використовує попередні точки даних і параметр згладжування для передбачення майбутніх значень. У цьому випадку аномалії визначаються як точки, що відхиляються від прогнозованої моделі. Традиційні геометричні та статистичні методи мають глибоке теоретичне обґрунтування, але вони часто виявляються непридатними для реальних сценаріїв, де моделі даних мають значну часову залежність. Це зумовлює потребу у використанні підходів на основі машинного та глибокого навчання, які забезпечують більшу гнучкість і адаптивність.

Моделі машинного та глибокого навчання складають третю підкатегорію і набувають все більшої популярності. Вибір моделі залежить від типу даних. Наприклад, моделі довгострокової пам’яті (LSTM) і трансформаторні моделі оптимально працюють із послідовними даними, такими як аудіо, відео або часові ряди. Натомість згорточні нейронні мережі (CNN) і автокодери (AE) краще обробляють непослідовні типи даних, такі як зображення.

Ці алгоритми визначають нормальну та аномальну поведінку шляхом встановлення межі рішення, наприклад, за допомогою класифікаторів опорних векторних машин (SVM) або прогнозування майбутніх значень у потокових даних із мережами LSTM. Залежно від доступності міток для навчання, ці підходи поділяються на контрольовані, напівконтрольовані, самоконтрольовані та неконтрольовані методи.

Існує три основні шляхи категоризації аномалій за програмами: конструктивний, деструктивний і очищення даних.

Конструктивні програми є корисними та сприяють продуктивності. Вони важливі для таких завдань, як моніторинг поведінки людей похилого віку, щоб запобігти падінням, використовуючи дескриптори зображень, або порівняння продуктивності між різними моделями, такими як багатошаровий перцептрон (MLP), k-найближчі сусіди (KNN) і класифікатори SVM. Інші приклади конструктивних програм включають використання навчання з підкріпленням для

застосувань безпілотних літальних апаратів (БПЛА), таких як розумне землеробство, або підхід федеративного навчання для програм розумного дому;
Деструктивні програми спрямовані на порушення звичних операцій з метою отримання фінансової вигоди або завдання шкоди мережам та даним додатків в Інтернеті речей. Вони можуть порушити важливі бізнес-процеси та негативно вплинути на суспільство. Прикладом є дослідження кібератак IoT, які були розглянуті в роботах, таких як стаття Alsheikh et al. Такі програми вимагають застосування рішень, як RAPPER і NBaIoT, що використовують автокодери (AE) для запобігання атак або реагування після інциденту. Програми для очищення даних зосереджуються на усуненні небажаних даних, таких як стрибки або шум, що виникають в результаті датчиків. Прикладом є використання глибоких згорткових нейронних мереж (CNN), таких як DeepAnT, для очищення вхідного сигналу. Аномалії можна класифікувати за кількома типами. Перший тип це точкові аномалії які виникають, коли окрема точка даних значно відрізняється від очікуваної поведінки. Прикладом є виявлення шахрайства з кредитними картками. Другий тип це контекстуальні які аномалії виникають, коли подія чи точка даних є аномальною лише в певному контексті. Наприклад, порівняння кількох точок на одну й ту ж точку даних не завжди вказує на аномальну поведінку. Третій тип це колективні аномалії які є випадками, коли аномалія виявляється при групуванні точок даних, що вказує на незвичний тренд або патерн у великому наборі даних.

Контекстуальна аномалія виникає, коли поведінка або характеристики даних оцінюються з урахуванням контексту. Наприклад, порушення правил дорожнього руху може бути визнано аномальним тільки в певних географічних умовах чи в залежності від часу доби.

На відміну від точкових або контекстних аномалій, колективні аномалії виявляються, коли аномальність проявляється не в окремих точках даних, а в цілій групі даних. Це може включати в себе ситуації, коли аномалія спостерігається при обробці великого обсягу інформації, наприклад, використання електрокардіограм для виявлення порушень у серцевому ритмі людини.

Алгоритми виявлення аномалій можуть бути онлайн або офлайн, залежно від того, на якому етапі дані обробляються. Онлайн-алгоритми обробляють дані в реальному часі, аналізуючи одну точку даних або невелике вікно без доступу до всіх попередніх введених даних. Прикладами онлайн-методів є IoT-Keeper, який використовує нечіткі C-середні, а також методи, застосовані в ансамблевому підході від Hedde et al.

Офлайн-алгоритми, в свою чергу, працюють з повним набором даних, що дозволяє їм використовувати більш складні та ресурсоємні методи, але це може зажадати більше часу для обробки. Наприклад, стаття Wu et al. описує методи, що поєднують LSTM (довгострокову пам'ять) з Gaussian Naive Bayes, дозволяючи завершити навчання в автономному режимі та розгорнути модель для онлайн-обробки.

1.2 Огляд машинного навчання для виявлення аномалій в мережах IoT.

Пристрої Інтернету речей (IoT) стали об'єктом понад 100 мільйонів атак у першій половині 2019 року. З прогнозами, що до 2025 року кількість пристроїв IoT перевищить 64 мільярди, необхідність у захисті цих пристроїв, таких як медичні прилади або автономні автомобілі, стає надзвичайно важливою. Проблема ускладнюється великим спектром можливих атак та їх еволюцією, а також обмеженими обчислювальними та зберігаючими ресурсами на самих пристроях.

У цьому контексті було розглянуто систему виявлення вторгнень (IDS) для мереж IoT з урахуванням сучасних технологій. Для тестування та порівняння рішень вибрано публічний набір даних CIDDS-001, що дозволяє порівняти кілька алгоритмів машинного навчання. Важливо зазначити, що отримання відтворюваних результатів є відносно легким завданням на поточному рівні розвитку технологій.

Також було розглянуто важливість вбудовування цих алгоритмів у контекст IoT, підкреслюючи необхідність застосування простих правил для покращення ефективності. Однак вибір правильного набору даних для розробки та оцінки

алгоритмів на основі машинного навчання для систем виявлення вторгнень (NIDS) не завжди є очевидним і може бути складним завданням. Одним з найбільш популярних наборів даних є KDD cup99, але він має ряд обмежень, зокрема наявність зайвих параметрів, використання частини набору даних як тестових у попередніх дослідженнях та занадто велика довжина, що змушує використовувати лише частину даних.

Натомість набір даних CIDDS-001, описаний Ring et al., є сучасним і менш складним для обробки. Цей набір даних містить атаки грубої сили SSH, DoS, сканування портів та інші атаки, захоплені з реальних сценаріїв. Завдяки цьому дослідники можуть аналізувати атаки в поєднанні з легітимним трафіком, що підвищує його цінність для тестування IDS-систем.

Набір даних містить 14 особливостей які наведено в таблиці 1.1.

Таблиця 1.1 – Особливості в наборі даних CIDDS-001

id	Attribute Name	Attribute Description
1	Src IP	Source IP Address
2	Src Port	Source Port
3	Dest IP	Destination IP Address
4	Dest Port	Destination Port
5	Proto	Transport Protocol (e.g. ICMP, TCP, orUDP)
6	Date first seen	Start time flow first seen
7	Duration	Duration of the flow
8	Bytes	Number of transmitted bytes
9	Packets	Number of transmitted packets
10	Flags	OR concatenation of all TCP Flags
11	Class	Class label (Normal, Attacker, Victim)
12	AttackType	Type od Attack (PortScan, DoS, Bruteforce, PingScan)
13	AttackID	Unique Attack id
14	AttackDescription	Additional sinformation about the set attack parameters

В експерименті з набором даних CIDDS-001 використовувалися кілька підходів для підготовки даних до класифікації. Цільовою змінною було визначено атрибут "Class", який вказує, чи є запис аномалією (жертва або зловмисник).

Функції, які явно корелюють з класом, такі як "AttackType", "AttackID" і "AttackDescription", були видалені, оскільки вони не додавали додаткової цінної інформації для класифікації.

Оскільки IP-адреси були анонімізовані і не несли додаткової інформативності, вони також були виключені з аналізу. Для категоріальних змінних, таких як "Flags", "Class" та "Proto", було використано одногаряче кодування (one-hot encoding) для перетворення їх у числові формати, придатні для машинного навчання.

Для виконання експерименту була використана підмножина спостережень за тиждень, оскільки вона містить 42 з 92 типів атак у наборі. Хоча набір даних містить більше 8 мільйонів рядків, менш ніж 20% з них є аномаліями, що створює проблему незбалансованості класів. Це може призвести до "ефекту маскування", коли клас з більшою кількістю екземплярів домінує в результатах моделі, зменшуючи точність виявлення аномалій.

Для подолання цієї проблеми в експерименті було виконано перебалансування класів. Оскільки клас більшості представлений великою кількістю екземплярів, було використано підвибірку для зменшення кількості таких екземплярів, що дозволяє краще збалансувати дані. Як альтернативу, можна також застосувати методи передискретизації для класу меншості, такі як генерація нових синтетичних екземплярів, наприклад, за допомогою методу SMOTE (Synthetic Minority Over-sampling Technique).

Набір даних CIDDS-001 був зібраний в 2017 році в емульованому середовищі малого бізнесу та містить трафік за чотири тижні. Він включає як атаки з реального Інтернету, так і звичайний трафік, що дозволяє досліджувати як аномальні, так і звичайні ситуації для ефективного тестування систем виявлення вторгнень (IDS).

У нашому випадку краще зробити такі дії:

– перетасувати дані,

– залишити половину даних для остаточного оцінювання,

– підвибірку, іншу половину, щоб зберегти близько 180000 екземплярів на клас.

1.3 Визначення аномалій у бездротових мережах

Аномалія – це відхилення від очікуваної або нормальної поведінки в системі. Вона може мати різні форми залежно від контексту, в якому розглядається, і визначення може варіюватися між різними дослідницькими напрямами. Наприклад, аномалія може бути сприйнята як виняток або сюрприз, віддалений об'єкт або особливість в даних, і все це залежить від предметної області або застосування.

У випадку бездротових сенсорних мереж, таких як мережі IoT або локальні викиди, дослідники часто класифікують аномалії за їх просторово-часовими характеристиками. Лавін та ін. використовують еталонні набори даних для виявлення аномалій в хмарних мережах, але вони не визначають чітко типи аномалій. Їхні набори даних можуть включати різні аномалії, що дозволяє оцінити продуктивність алгоритмів.

Юрдак та ін. пропонують більш деталізовану класифікацію аномалій, де визначають часові, просторові та просторово-часові аномалії, які характерні для моніторингу роботи бездротових сенсорів. Це включає такі аномалії, як скидання вузлів, відмови вузлів, а також зміни в поведінці мереж і даних, що передаються через ці мережі.

Враховуючи різні аспекти застосування, інші дослідження також визначають аномалії з урахуванням конкретних типів мереж і рівнів, наприклад, Sheth та ін. вивчають аномалії на фізичному рівні в бездротових мережах IEEE 802.11, такі як приховані аномалії терміналу, ефект захоплення або зміни потужності сигналу. Гупта та ін. визначають аномалії в мультихопових мережах, включаючи чорні діри, провалля, вибіркове пересилання та інші аспекти, пов'язані з поведінкою мережі.

У мережах бездротових датчиків, де обмін даними між пристроями здійснюється через відео, голос чи датчики, аномалії часто з’являються, коли пристрої або мережа скомпрометовані або погіршена їхня працездатність. У нормальних умовах всі пристрої функціонують без перебоїв, але коли з'являються аномалії, це може призвести до погіршення якості обслуговування або порушення роботи системи.

Тому, для ефективного виявлення аномалій у таких складних системах, як бездротові мережі IoT, важливо враховувати різні типи аномалій і застосовувати методи, що дозволяють аналізувати великі обсяги даних у реальному часі з урахуванням просторово-часових характеристик.

Те, як аномалії впливають на якість обслуговування користувача, суворо пов'язане з типом аномалії. Тому в цьому розділі я вив чотири типи аномалій, які можна спостерігати в лініях зв'язку бездротових мереж, які в основному були виявлені при нашій оцінці реальних експериментів. Обговоримо типи аномалій:

- раптова деградація,
- раптова деградація з відновленням,
- миттєва деградація (стрибок),
- повільна деградація.

Раптова деградація це - аномалія деградації мож, яка бути математично представлена ступінчастою функцією зі спадним нахилом, як показано на рисунку

Рисунок 1.3 – Раптова деградація

У нашому випадку йдеться про раптову й стійку зміну стану з'єднання. Хоча теоретично можливе різке збільшення нахилу, зазвичай це призводить до покращення надійності зв'язку, тому такі зміни не вважаються аномаліями.

З точки зору користувача, симптоми можуть включати недоступність, автономність і відсутність зв'язку з послугами. Щодо мережі, це може означати, що

передавач перестає генерувати електромагнітне поле, або приймач не здатен отримувати дані.

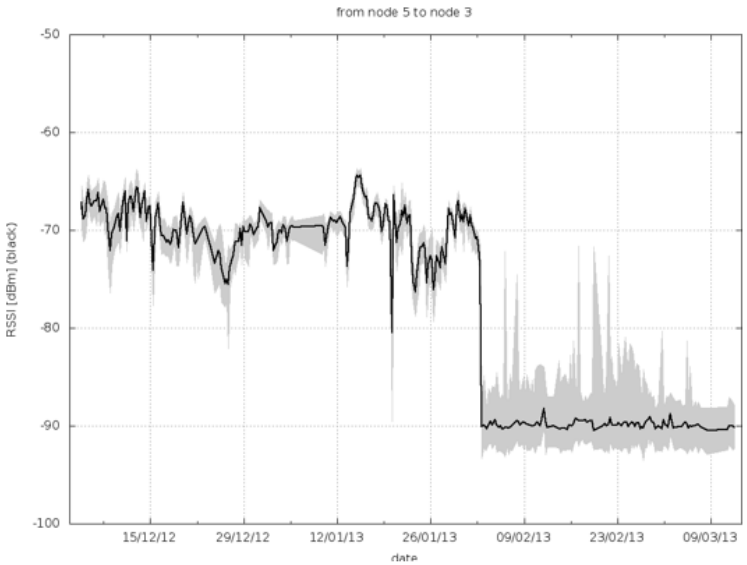

Рисунок 1.4 – Раптова деградація без відновлення між Вузлами 5 і 3

Раптова деградація з відновленням (SuddenR) — це тип аномалії, коли деградація з відновленням може бути математично описана як ступінчаста функція з спадним нахилом, як показано на рисунку 1.4. У цьому випадку стан з'єднання різко змінюється, залишається в новому стані протягом тривалого періоду, а потім повертається до попереднього стану.

Такий вид аномалії є складним для виявлення, оскільки зміни стану можуть виглядати як тимчасові коливання або шум у даних. Для аналізу таких сценаріїв необхідно застосовувати методи, які здатні розпізнавати як самі зміни стану, так і їх тривалість, що дає змогу розрізняти справжні аномалії від короткочасних нестабільностей. Це потребує врахування як тимчасових закономірностей, так і контексту даних, в якому відбуваються ці зміни. Наприклад, алгоритми, що враховують історичні тренди та типові патерни, можуть допомогти зменшити помилкові спрацювання.

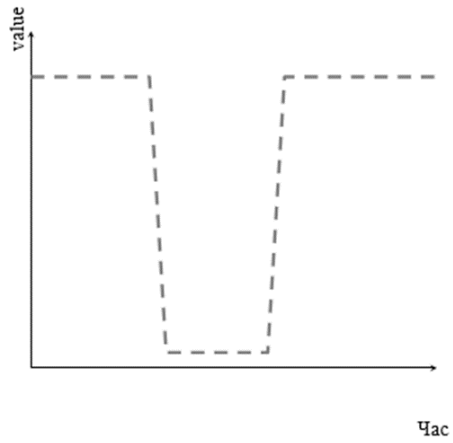

Рисунок 1.5 – Раптова деградація з відновленням

З симптомів можна виділити, що з точки зору користувача, надані послуги можуть стати повільними та недоступними протягом певного періоду часу, а пізніше повернутися до своєї звичайної роботи. З точки зору мережі, у разі раптової деградації при відновленні або передавач тимчасово припиняє генерувати електромагнітне поле, або приймач тимчасово не може його приймати.

Можливі причини: Цей тип деградації може бути викликаний перевантаженням буфера, що призводить до накопичення даних і затримок у їх обробці, а також програмною помилкою, яка може спричинити неправильну роботу системи. Це проілюстровано на рисунку 1.6, де сторожовий тайм-аут виконує примусове перезавантаження пристрою, але при цьому рація залишається в надмірно активному стані, що вимагає повторного калібрування для відновлення нормальної роботи. Додатковими факторами можуть бути перешкоди в середовищі, наприклад, об'єкти, що блокують зв'язок на певний час, або використання глушилки сигналу, встановленої на військовій техніці, яка тимчасово перебиває зв'язок під час проїзду. Подібні умови можуть виникати як у природних, так і в штучно створених ситуаціях, що вимагає від системи здатності до швидкої адаптації та мінімізації наслідків деградації. Це вимагає від системи використання резервних каналів зв'язку, алгоритмів самовідновлення та проактивного моніторингу для швидкого реагування на зміни в середовищі. Крім того, важливим є впровадження механізмів шифрування і захисту даних, щоб забезпечити стійкість до спроб навмисного втручання або перехоплення сигналу.

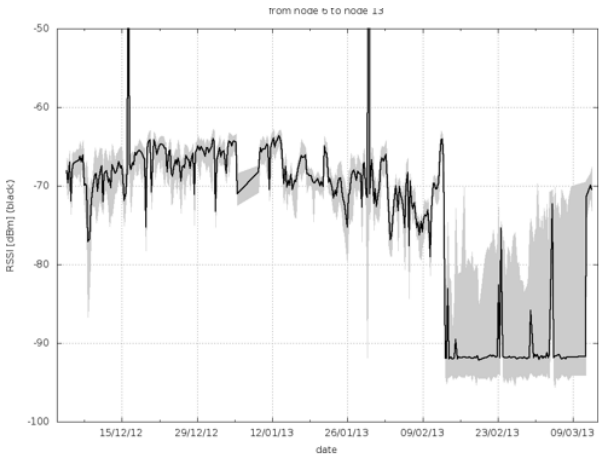

Рисунок 1.6 – Раптова деградація відновлення між Вузлом 6 та Вузлом 13

Миттєва деградація (InstaD) — це тип аномалії, при якій деградація стану ланки відбувається миттєво, і це може бути математично представлено ступінчастою функцією з різким спадаючим нахилом, що створює раптовий сплеск, як показано на рисунку 1.7. У такому випадку стан ланки змінюється дуже швидко, але незабаром повертається до попереднього стану. Миттєва деградація може проявлятися як втрати інформації або короткочасні збої, які не впливають на загальну стабільність системи.

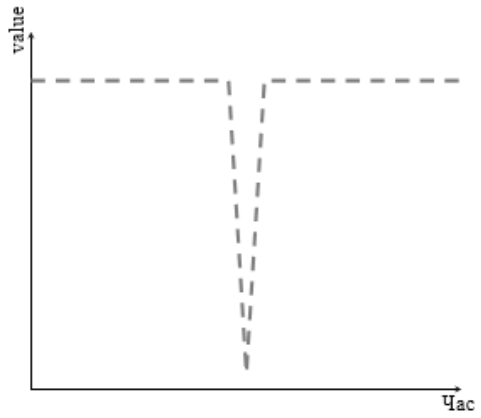

Рисунок 1.7 – Миттєва деградація

З точки зору користувача, миттєва деградація може проявлятися як короткочасні затримки в реальному часі, в той час як інші сервіси, не пов'язані з реальним часом, можуть продовжувати працювати без змін. З точки зору мережі, це може призвести до того, що передавач зазнає значного затухання сигналу, або

приймач тимчасово не здатен отримувати дані через сильні перешкоди або надмірний шум.

Можливі причини цього типу деградації включають миттєві перешкоди, зіткнення сигналів, помилки квантування або зчитування, а також раптові насичення в електронних компонентах трансивера. Як показано на рисунку 1.8, аномалії можуть бути спричинені такими зовнішніми факторами, як пристрої, що працюють на тій самій частоті, надмірний фоновий шум, багатопроменеве згасання та інші проблеми, пов'язані з середовищем поширення сигналу.

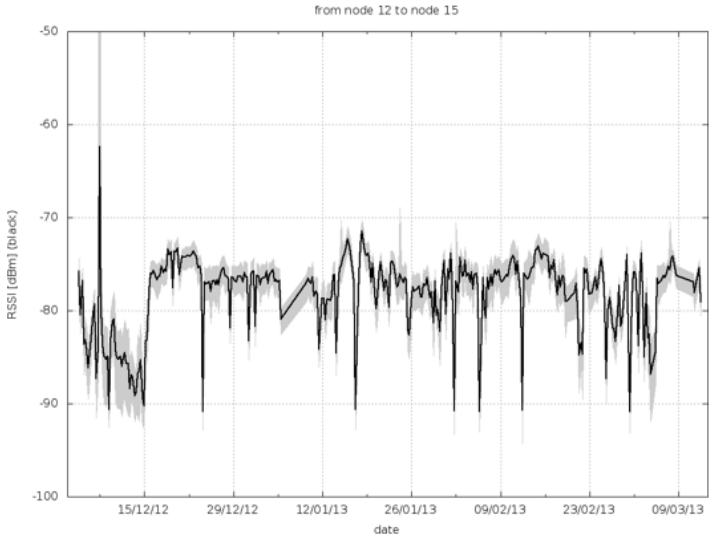

Рисунок 1.8 – Спайкоподібна миттєва деградація між вузлами 13 і 15

Повільна деградація (SlowD) – це аномалія, яка може бути математично представлена як нормалізована лінійна функція з незначним спадаючим нахилом, як це показано на рисунку 1.9. У цьому випадку стан зв'язку змінюється поступово та непомітно протягом тривалого періоду часу, і ці зміни можуть залишатися незворотними. Повільна аномалія деградації може призвести до втрати інформації та переривань через певний час.

Аномалія повільної деградації може залишатися непоміченою протягом тривалого часу, оскільки користувачі можуть не відчувати змін у якості обслуговування одразу. Проте, коли досягаються певні порогові значення,

користувачі починають помічати погіршення якості обслуговування. Якщо методи компенсації вичерпано, зв'язок може перерватися, а послуги стати недоступними

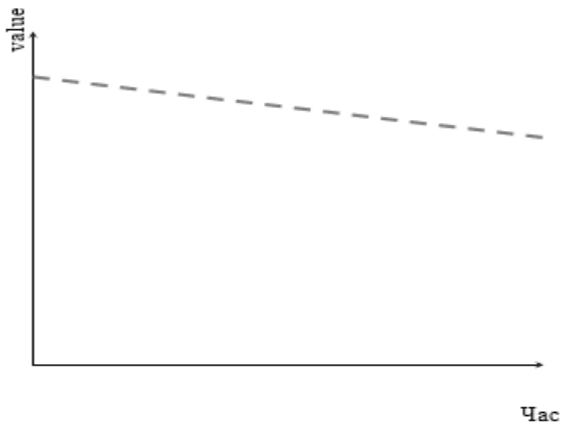

Рисунок 1.9 – Повільна деградація

.

З точки зору мережі, це може означати, що передавач поступово втрачає здатність генерувати достатнє електромагнітне поле для підтримки необхідного рівня сигнал/шум, або приймач не може збирати достатньо електромагнітного випромінювання для коректного декодування даних, що іноді викликано старінням компонентів.

1.4 Підходи до автоматизованого виявлення аномалій

Зважаючи на вищезазначені аномалії зв'язків, встановлення фіксованих порогових значень для виявлення аномальних вимірювань може допомогти виявляти викиди. Проте, як показано, підходи, засновані на фіксованих порогах, не можуть адаптуватися до змін у поведінці даних, що робить вибір порогу складним і може призвести до зниження ефективності, особливо в реальному часі.

Правила часових значень — це ще один простий спосіб виявлення аномалій на рівні каналу, які можуть бути встановлені на основі досвідченого порогу або з використанням чисельних методів. Однак, як вже обговорювалось, існує кілька способів виявлення аномалій. Наприклад, аналізуючи RSS-розподіл на рисунках

1.3–1.9, можна побачити, що для аномалій SuddenD, SuddenR і SlowD розподіл RSS змінюється значно, що дозволяє легко відрізнити ці аномалії. Аномальна ланка має більший розкид RSS, а її середнє і медіанне значення змінюються.

Виявлення раптової деградації (SuddenD) потребує діагностики різких спадів, що не відновлюються протягом певного часу. Виявлення SuddenR включає в себе виявлення раптового падіння сигналу, після чого він відновлюється до початкового рівня протягом певного часу. Аномалії InstaD і SuddenR мають схожі характеристики, але InstaD повертається до початкового рівня сигналу дуже швидко.

Для виявлення аномалії SlowD необхідно спостерігати за розподілами протягом тривалого часу, оскільки зміни можуть бути дуже повільними. Раптові зміни також можна виявити в частотній області, де для SuddenD і SuddenR це добре видно на низьких частотах, як показано на рисунках 1.10 та 1.11. Аномалії, пов'язані з ін'єкцією, важко відрізнити між InstaD і SlowD в частотній області.

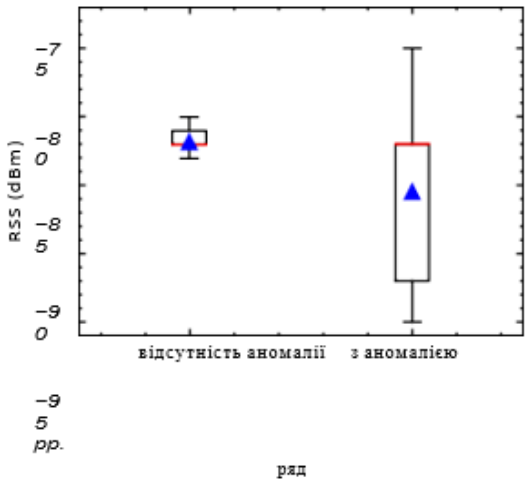

Рисунок 1.10 – Перспектива агрегованих функцій

На основі поданих даних видно, що вплив ін'єкційних аномалій стає більш помітним при аналізі інших параметрів у часово-частотній області. Це підкреслює важливість використання вдосконалених методів обробки сигналів для точного виявлення та оцінки таких аномалій, а також для побудови більш стійких моделей, здатних адаптуватися до змін у часово-частотній області.

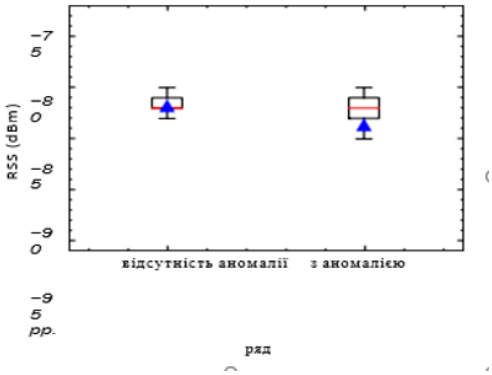

Рисунок 1.11 – Перспектива агрегованих функцій

Вплив ін'єкційних аномалій проявляється у вигляді відхилень, які не завжди можна виявити в часовій області, але стають очевидними при аналізі частотних характеристик сигналу. Це дозволяє точніше визначати джерела аномалій і їх природу, відкриваючи можливості для більш глибокого розуміння та усунення проблем.

1.5 Висновки

Було розглянуто проблему виявлення аномалій і вторгнень у мережах IoT. Спершу було окреслено контекст проблеми та представлені різні підходи, що описані в літературі. Особлива увага була приділена методам машинного навчання, які дозволяють навчатися безпосередньо на даних, виявляючи важливі ознаки без використання спеціалізованих мережевих моделей або сигнатур.

Цей розділ описує чотири типи аномалій, які можуть виникати в бездротових лініях зв'язку і які є корисними для виявлення в реальних умовах експлуатації IoT. Було показано, що ці аномалії виявлялися під час реальних розгортань IoT, зокрема на випробувальному стенді LOG-a-TEC, і мали значний вплив на очікувану роботу системи.

На основі цього досвіду були розроблені моделі для виявлення кожного типу аномалій, враховуючи п'ять різних способів представлення даних та шість різних

методів машинного навчання, таких як дерева рішень, випадкові ліси, метод опорних векторів, нейронні мережі, кластеризація та байєсові підходи. Ці моделі дозволяють не лише класифікувати аномалії, але й прогнозувати їх можливу появу, забезпечуючи ефективне управління загрозами.

Впровадження таких рішень у мережу IoT вимагає уваги до можливих обчислювальних витрат, адже IoT-пристрої часто мають обмежені ресурси процесора та пам’яті. Для маршрутизаторів або мережевих контролерів потрібно мати модуль для захоплення вхідного трафіку, який може фільтрувати, зберігати та попередньо обробляти дані у реальному часі. Класифікатори, які, після навчання за допомогою дерев рішень або випадкових лісів, можуть бути успішно реалізовані, забезпечують високу точність виявлення аномалій завдяки їх здатності адаптуватися до змін у поведінці трафіку. Додатково, ці модулі повинні бути оптимізовані для роботи у реальному часі, мінімізуючи затримки та споживання ресурсів.

2 РОЗРОБКА ФРЕЙМВОРКУ IOT-AD, ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ СЕРЕД ВЗАЄМОПОВ'ЯЗАНИХ ПРИСТРОЇВ IOT

З розповсюдженням Інтернету речей (IoT) в реальність втілились різноманітні середовища, зокрема розумні будинки. Вони складаються з багатьох IoT-пристроїв, що можуть бути вироблені різними постачальниками, але взаємопов'язані між собою та налаштовані відповідно до уподобань користувачів (наприклад, розумний термостат, який підтримує задану користувачем температуру).

Існують платформи для контролю пристроїв IoT, як-от IFTTT, Samsung SmartThings та Apple HomeKit, які забезпечують інтеграцію послуг, наданих пристроями різних виробників. Проте, коли ці пристрої починають демонструвати поведінку, що не відповідає налаштуванням користувачів або дають недостовірні показання, це розглядається як аномалія.

У контексті взаємопов'язаної природи IoT-пристроїв аномалія, що виникає в одному пристрої, може поширюватися та впливати на інші пристрої в мережі, створюючи потенційну загрозу стабільності всієї системи. Це особливо критично для великих IoT-мереж, які використовуються в розумних будинках, промислових середовищах або системах охорони здоров'я, де збої можуть призвести до значних фінансових втрат або навіть ризику для життя. Тому важливо не тільки виявляти такі аномалії, а й розробляти стратегії для їх ефективного стримування, щоб уникнути каскадного впливу на інші пристрої.

Прикладом такого сценарію може бути ситуація, коли несправний або скомпрометований датчик руху починає відправляти неправдиві сигнали про рух, що взаємодіють із підключеним датчиком диму, активуючи його навіть за відсутності реальної небезпеки. Це може призвести до хибної тривоги, яка не лише створює незручності для користувача, але й може викликати спрацьовування інших систем, таких як автоматичне відчинення дверей, активація спринклерної системи або виклик екстрених служб. У гіршому випадку такі ситуації можуть бути

використані зловмисниками для дестабілізації системи або маскування реальних загроз.

Щоб запобігти подібним ситуаціям, необхідно впроваджувати механізми моніторингу взаємодії між IoT-пристроями, а також алгоритми верифікації достовірності сигналів. Наприклад, при отриманні сигналу від датчика руху система може автоматично перевіряти його кореляцію з іншими даними, такими як відео з камер спостереження, для підтвердження наявності руху. Крім того, застосування стратегії ізоляції скомпрометованих пристроїв або сегментування мережі може допомогти мінімізувати ризик каскадних збоїв. (як показано на рисунку 2.1).

2.1 Аномалії в системі розумного будинку

В результаті аномальної взаємодії несправного або скомпрометованого датчика руху з іншими пристроями, такими як датчик диму, розумні датчики вікон і замки, виникає серйозна проблема.

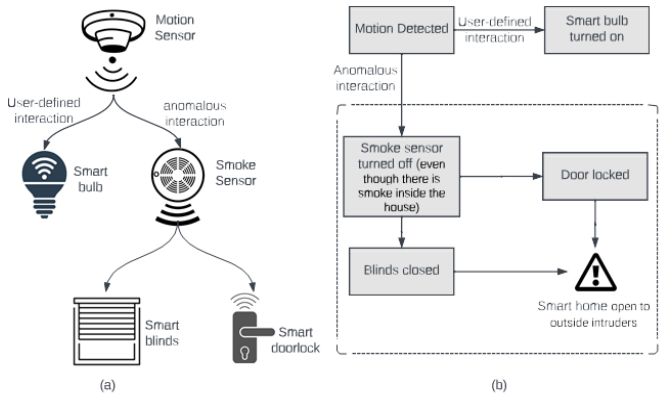

Рисунок 2.1 – Де (a) Взаємодія між пристроями IoT; (b) Поширення аномалії на пристроях IoT

Зокрема, коли датчик руху активує датчик диму, це може призвести до того, що автоматично відкриються вікна і розблокуються двері, щоб мешканці могли

покинути будинок через дим. Однак у цьому випадку це створює можливість для сторонніх осіб потрапити до будинку, що робить його вразливим до злому.

Раніше було проведено низку досліджень, що виявили різні типи аномалій у мережах IoT і запропонували методи їх виявлення. Більшість з цих досліджень фокусувалися на двох основних типах аномалій: аномаліях на рівні пакетів, пов'язаних з мережевим трафіком, що генерується IoT-пристроями під час зв'язку з платформами контролерів, хмарними службами або іншими пристроями IoT, а також аномаліях, що стосуються стану або поведінки пристроїв, виявлених на основі аналізу їхнього часу роботи та взаємодії.

Попередні дослідження зосереджувалися на методах виявлення аномалій, але не приділяли уваги механізмам, що дозволяють пом'якшувати наслідки аномалій, які можуть поширюватися від одного пристрою IoT до іншого, тим самим впливаючи на роботу кількох пристроїв в середовищі IoT. Крім того, не було розглянуто механізми, які дозволяють постраждалим пристроям IoT відновлюватися після таких поширених аномалій.

Просте виявлення аномалій та ізоляція пристроїв, що зазнали збоїв, може бути недостатнім для реальних сценаріїв, таких як розумні будинки. Оскільки пристрої в таких середовищах тісно взаємопов'язані, аномалії можуть поширюватися між ними, перш ніж їх буде виявлено. Тому важливо впровадити механізми, які дозволяють пом'якшити наслідки таких аномалій.

Цей розділ зосереджено на дослідженні кількох важливих аспектів. По-перше, розглядається створення структури, здатної виявляти аномалії на рівні пакетів, що виникають у процесі взаємодії між пристроями IoT. Особливу увагу приділено механізмам і підходам, які дозволяють ідентифікувати такі аномалії для забезпечення безперебійної роботи системи. По-друге, аналізується, як ця структура може сприяти відновленню уражених пристроїв IoT після поширених аномалій, забезпечуючи їх повернення до стабільного стану таким чином, щоб функціонування мережі виглядало безперервним і незмінним. Для вирішення цих завдань було запропоновано IoT Anomaly Detector (IoT-AD) — систему, яка виявляє аномалії на рівні пакетів і взаємодії між пристроями IoT та пом'якшує їх вплив,

дозволяючи пристроям відновлюватися після таких аномалій. IoT-AD функціонує як розширена система для управління пристроями IoT, яка виявляє аномалії в середовищах IoT та сприяє відновленню пристроїв після збоїв.

Основний внесок цієї роботи полягає в тому, що була розроблена та представлена структура IoT-AD, яка включає механізми виявлення аномалій на рівні пакетів і взаємодії між пристроями IoT, а також підтримку стабільного стану пристроїв протягом часу та їх відновлення після аномалій. Прототип IoT-AD буде оцінений на основі наборів даних відкритих пристроїв IoT та реального розгортання на тестовому стенді IoT. Оцінка також буде проведена у порівнянні з іншими підходами для виявлення аномалій у середовищах IoT. Результати показують, що IoT-AD є ефективною та швидкою системою, здатною виявляти аномалії в IoT пристроях за менше ніж 2,12 мс з точністю до 98%.

2.2 Виявлення аномалій в пристроях IoT.

Метою виявлення аномалій в IoT є виявлення поведінки, що відхиляється від типових патернів. У попередніх дослідженнях були використані різні методи для виявлення аномалій в середовищі IoT, зокрема аналіз трафіку, сигнатури на рівні пакетів та семантичні моделі.

Homonit — це фреймворк для платформи Samsung SmartThings, який виявляє аномалії шляхом відстеження зашифрованих трафіків активності розумних пристроїв та порівняння з очікуваною поведінкою, що базується на вихідному коді.

HADES-IoT — легкий фреймворк для виявлення аномалій на основі хостів, здатний проактивно виявляти та запобігати виконанню несанкціонованих функцій на пристроях IoT.

IoT-Praetor використовує модель опису використання пристроїв для профілювання комунікаційних і взаємодійних патернів між пристроями IoT та виявлення аномалій в реальному часі.

Семантичний підхід, запропонований Wang et al. під назвою HAWatcher, використовує семантичну інформацію пристроїв (програми, типи пристроїв, місця розташування, журнали подій) для створення кореляцій і подальшого симулювання середовища розумного дому для виявлення аномалій на основі поведінки.

HomeSnitch фокусується на програмно-визначених мережах для відстеження зв'язків між пристроями та серверами, класифікації дій пристроїв та виявлення аномальних поведінок.

Серед інструментів для виявлення аномалій у середовищі IoT можна виділити PingPong, який слугує для вилучення підписів на рівні пакетів, зокрема для подій пристроїв, таких як вмикання чи вимикання розумної розетки, що дозволяє ефективно виявляти аномалії в мережах розумних будинків. Ще одним прикладом є Orpheus — інструмент, який аналізує журнали подій та системні логи для виявлення експлойтів і атак у реальному часі. Сюй та інші запропонували систему, яка аналізує трафік домашньої мережі за допомогою фільтра Bloom, виявляючи аномальні патерни трафіку. Лі та його співавтори розробили легкий статистичний підхід для навчання пристроїв IoT, що базується на аналізі системної інформації, такої як використання процесора, пам'яті чи пропускна здатність мережі, з метою виявлення аномалій. Вони також запропонували метод, який дозволяє визначати атаки на пристрої IoT через моніторинг енергоспоживання компонентів, таких як центральний процесор або мережеві системи. Існують також системи, що використовують фізичні рівні для виявлення аномалій, зокрема на основі таких параметрів, як індикатор потужності прийнятого сигналу (RSSI), спектральна щільність потужності (PSD) та співвідношення сигнал/шум (SNR). Мартінс et al. використовували RSSI-дані для виявлення періодів активності та тиші пристроїв IoT та виявлення аномалій. Тан et al. запропонували структуру виявлення аномалій для бездротових сенсорних мереж, використовуючи дані RSSI. Раджендран et al. представили SAIFE — методику аналізу PSD бездротового спектра для виявлення аномалій в середовищах IoT. Однак використання фізичних рівнів для виявлення аномалій має певні труднощі, такі як чутливість до шуму та залежність результатів від відстані між пристроєм відправником та приймачем.

2.3 Машинне навчання для виявлення аномалій пристроїв IoT.

Завдяки останнім досягненням у галузі технологій, машинне навчання стало потужним інструментом для виявлення аномалій через виявлення відхилень від типових патернів даних. Для виявлення аномальних шаблонів у розумних будинках, Інь et al. та Яккула et al. використовували однокласні векторні машини підтримки (SVM), навчаючи моделі на основі даних від сенсорів.

Рамапатруні et al. застосували приховані марковські моделі для аналізу даних мережі розумного будинку, з метою виявлення аномалій. Фахад et al. використали алгоритм просторової кластеризації, заснований на щільності, для розпізнавання активностей користувачів, тоді як Тріманда et al. застосували той самий алгоритм для кластеризації пар пакетів і виявлення аномалій у мережевому трафіку. Поєднання аналізу головних компонент та алгоритму ковзного вікна, як запропонували Wu et al., дозволяє виявляти дії користувача шляхом аналізу Wi-Fi сигналів. Бранч et al. використовували метод машинного навчання на основі KNN для виявлення аномальних викидів, тоді як Нарудін et al. застосовували наївні алгоритми Байєса та метод Random Forest для виявлення шкідливого програмного забезпечення на основі аномалій.

Для мінімізації наслідків, спричинених аномаліями, необхідно впроваджувати методи профілактики та відновлення. Ной et al. запропонували стохастичний алгоритм додавання трафіку, який генерує трафік для приховування метаданих, тим самим зберігаючи конфіденційність дій користувачів.

Гаурав et al. розробили структуру, що підвищує безпеку в розумному будинку через контроль доступу на основі атрибутів. Однією з переваг цього підходу є здатність точніше визначати політики безпеки та враховувати умови навколишнього середовища для прийняття рішень щодо доступу. Ямаучі et al. представили систему, яка виявляє аномальні події через аналіз послідовностей подій і скидання пакетів, пов'язаних із аномаліями.

У таблиці 2.1 порівнюються конструктивні особливості IoT-AD з попередніми підходами. Більшість попередніх робіт зосереджувалися на виявленні

аномалій у пристроях IoT через аналіз трафіку або взаємодії між пристроями. Наприклад, PingPong аналізує послідовності пакетів для створення сигнатур подій IoT і виявлення аномалій, а HAWatcher використовує кореляції між подіями різних пристроїв для ідентифікації аномалій. IoT-Praetor і Homonit орієнтовані на платформу Samsung SmartThings.

Однак, одна з основних проблем попередніх підходів полягає в тому, що вони не пропонують механізмів для відновлення пристроїв IoT після аномалій та повернення їх до стабільного стану. IoT-AD, в свою чергу, не тільки використовує аналіз трафіку та взаємодії для виявлення аномалій, що можуть поширюватися серед пристроїв IoT, але й надає інструменти для відновлення цих пристроїв, дозволяючи їм повернутися до останнього відомого стабільного стану після аномальної події.

Таблиця 2.1 – Порівняння конструктивних властивостей IoT-AD та інших попередніх пов'язаних робіт

	Гоманіт	IoT-Praetor	HAWatcher	Рінг-понг	Ямаучі	Інтернет-речей (IoT-AD)
Аномалія трафіку Виявлення	Y	Y	N	L	N	*Y*
Аномалія взяємодії Виявлення	L	Y	Y	N	Y	*Y*
Стабільний стан Відновлення	N	N	N	N	L	*Y*

Пристрої IoT часто мають обмежені ресурси, оскільки вони створюються для виконання мінімальних і специфічних функцій з метою зниження вартості та складності. Це робить їх вразливими до збоїв та атак, що, в свою чергу, може призвести до виникнення аномалій у середовищі IoT. У цьому розділі розглядаються два основних типи аномалій: ті, що виникають через несправності пристроїв, і ті, що спричинені зловмисними атаками на пристрої IoT.

Аномалії через несправність пристроїв IoT: Оскільки пристрої IoT мають обмежену обчислювальну потужність і ресурси, вони часто схильні до збоїв, як апаратних, так і програмних. Часто в таких пристроях відсутні механізми для виявлення несправностей, що ускладнює своєчасне виявлення та усунення проблем.

Програмні збої можуть призвести до таких проблем, як фантомні команди, затримки в оновленні статусу чи втрати подій, що виникають через неполадки в системах або коді. Апаратні несправності, наприклад, несправні компоненти або плати, можуть спричинити помилки в командних процесах або спотворення даних. Як приклади, несправний датчик руху може неправильно зафіксувати присутність людини, а зламані конденсатори можуть спричинити збої в обміні даними між пристроями. Такі несправності можуть викликати несподівані зміни в поведінці пристроїв або їх взаємодії, наприклад, термостат може вмикати вентилятор, навіть якщо температура не змінилася, що є аномалією.

Аномалії через скомпрометовані пристрої IoT: Оскільки пристрої IoT обмежені в своїх ресурсах, вони можуть стати мішенню для зловмисників, які шукають способи скомпрометувати їх. Наприклад, через слабкі паролі або вразливості в мережі зловмисники можуть отримати доступ до пристроїв IoT. Після цього вони можуть змінювати поведінку пристроїв, видаючи фальшиві показання чи поширюючи аномалії через взаємодію з іншими пристроями. Це може привести до некоректних або шкідливих дій пристроїв у мережі, що є результатом їх скомпрометованої поведінки.

Таким чином, як несправності, так і атаки можуть викликати аномалії в середовищі IoT, змінюючи звичайну поведінку пристроїв і порушуючи їх взаємодію з іншими елементами системи.

Крім того, зловмисники можуть використовувати скомпрометований пристрій IoT для доступу до інших IoT-пристроїв, що сталося під час атаки ботнету Mirai.

2.4 Огляд дизайну IoT-AD

У контексті IoT-AD середовище IoT, таке як розумний будинок, покладається на контролер як на ключовий елемент управління та моніторингу. Контролер виступає не лише як вузол, що забезпечує зв'язок між IoT-пристроями, але й як аналітичний центр, який обробляє величезний обсяг даних у режимі реального часу. Він аналізує мережевий трафік, визначаючи потенційні аномалії, оцінює закономірності у взаємодії між пристроями та на основі отриманих результатів приймає рішення, спрямовані на забезпечення безперебійної роботи системи. Наприклад, контролер може ідентифікувати підозрілі дії, такі як нетипові запити від одного з пристроїв, і, залежно від політики безпеки, тимчасово ізолювати пристрій або сповістити користувача про потенційну загрозу. Завдяки цьому контролер не лише керує змінами стану пристроїв, але й служить бар'єром для поширення аномалій, забезпечуючи безпеку та стабільність середовища IoT.

Кожен пристрій IoT обмінюється даними з контролером через мережеві пакети, які передаються за допомогою протоколів прикладного рівня. Оскільки пристрої IoT є гетерогенними (вони можуть бути від різних постачальників і використовувати різні програмні стеки), кожен пристрій може застосовувати власні протоколи для зв'язку з контролером.

Для забезпечення ефективної взаємодії контролер повинен підтримувати механізми автоузгодження протоколів і стандарти інтероперабельності, що дозволяє мінімізувати конфлікти між пристроями. Крім того, використання моделей машинного навчання дає змогу контролеру адаптуватися до змін у поведінці пристроїв і виявляти нові типи загроз у реальному часі. Такий підхід сприяє побудові надійної та безпечної інфраструктури IoT, яка здатна реагувати на виклики сучасного цифрового середовища. Це забезпечує високу гнучкість і стійкість системи до можливих збоїв.

IoT-AD реалізується в п'яти етапах, що представлені на рисунку 2.2, і ці етапи контролер виконує за допомогою відповідних дій.

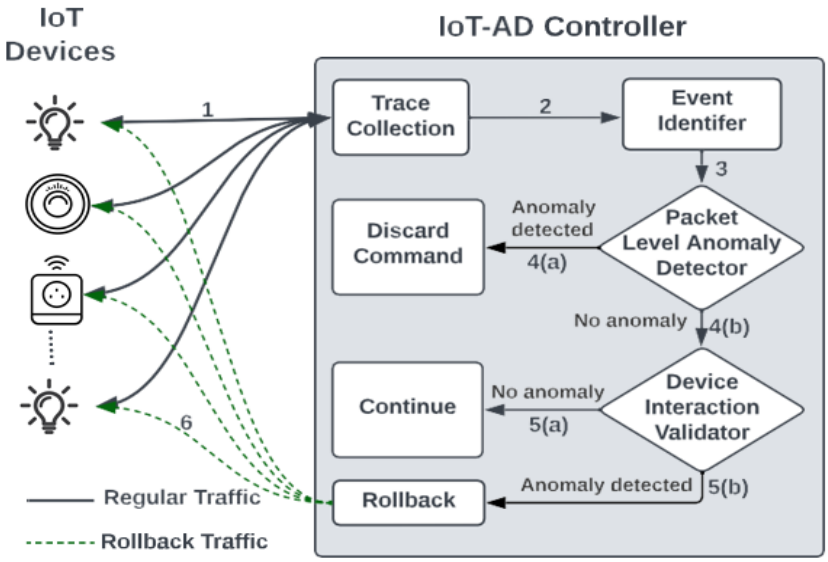

Рисунок 2.2 – Робочий процес роботи IoT-AD

Моніторинг пристроїв у системі IoT-AD передбачає, що контролер постійно контролює всі пристрої IoT, збираючи їх показники з часом. Ці показники передаються через локальну мережу у вигляді серії пакетних обмінів. Для кожного пристрою контролер визначає події, що впливають на його стан, та зберігає інформацію про стан пристрою на певні проміжки часу. Наприклад, коли розумна лампочка вмикається, контролер отримує сигнал від пристрою і оновлює її статус на «увімкнено».

Виявлення аномалій на рівні пакетів означає, що контролер аналізує мережевий трафік, що передається між пристроями. Сигнатури цих пакетів використовуються для виявлення аномалій, і якщо виявляється аномалія на рівні пакета, контролер відкидає подію.

Крім того, контролер також аналізує взаємодії між пристроями. Наприклад, якщо датчик руху виявляє присутність людини і активує розумне світло, це нормальна взаємодія. Проте якщо цей датчик випадково активує детектор диму, це буде вважатися аномалією, оскільки така взаємодія нелогічна. Контролер перевіряє ці взаємодії та виявляє будь-які аномалії, пов'язані з ними.

Концепція відкату означає, що при виявленні аномалії контролер визначає, як вона поширилася серед пристроїв IoT. Наприклад, якщо аномалія у взаємодії між

пристроями викликає непотрібну реакцію (наприклад, детектор руху спрацьовує детектор диму), це може призвести до серйозніших помилок, таких як розблокування розумних дверей. У такому випадку контролер аналізує, які пристрої були впливами аномалії, і повертає їх до останнього стабільного стану, як ніби аномалія не сталася.

У цьому розділі детально буде представлено компоненти дизайну IoT-AD. Перелік умовних позначень і абревіатур, що використовуються при проектуванні IoT-AD, наведено в таблиці 2.2.

Таблиця 2.2 – Перелік умовних позначень і скорочень, що використовуються при проектуванні IoT-AD

Символ/абревіатура	Опис
Роз'єми L2	Поля заголовка зв'язкового рівня
Роз'єми L4	Поля заголовка транспортного рівня
Роз'єми L3	Поля заголовків мережевого рівня
Син	Прапорець синхронізації TCP
АКК	Прапорець підтвердження TCP
Плавник	Прапорець фінішу TCP
TCP cmd	Команда TCP
TCP rsp	Відповідь TCP
Подія e	Подія, виявлена контролером

У IoT-AD контролер виконує важливу роль в управлінні всіма пристроями IoT в середовищі та виконанні операцій, таких як виявлення аномалій на рівні пакетів і перевірка взаємодії між пристроями. Як контролер може виступати різні пристрої з достатніми ресурсами, наприклад, смарт-телевізори, розумні холодильники, WiFi-мережеві маршрутизатори або розумні концентратори.

Контролер взаємодіє з пристроями IoT через бездротове з'єднання, моніторить їх стан і збирає дані (показники) за певні проміжки часу. Це може бути періодичне оновлення інформації про стан пристрою або оновлення при зміні стану пристрою. Наприклад, контролер може отримати нові показники температури або спостерігати за аномаліями в мережевому трафіку, відкидаючи події, які не відповідають нормі.

Крім того, контролер перевіряє взаємодії між пристроями через мережу. Коли один пристрій ініціює дію (наприклад, увімкнення розумної лампочки), це викликає подію. Взаємодія між пристроями може бути зафіксована, коли стан пристрою оновлюється через контролер. Ці події можуть бути складними, якщо одна подія ініціює кілька змін у різних пристроях, наприклад, датчик руху може активувати кілька пристроїв одночасно.

Контролер також відстежує обміни пакетами між пристроями через хмару або локальну мережу. Він може записувати заголовки пакетів (наприклад, IP-адреси, порти, довжини пакетів) та позначки часу кожного пакету. Це дозволяє контролеру аналізувати моделі взаємодії між пристроями та вести журнал подій для кожного пристрою. Коли, наприклад, пристрій обмінюється даними з хмарним сервером для оновлення програмного забезпечення або отримання команд від користувача, це також ідентифікується як подія в системі.

Усі ці операції дозволяють контролеру ефективно управляти пристроями IoT, забезпечуючи моніторинг, виявлення аномалій і підтримку стабільної взаємодії між пристроями. Крім того, контролер може зберігати історію подій, що дозволяє аналізувати роботу системи та виявляти довгострокові закономірності. Це сприяє вдосконаленню алгоритмів управління та підвищенню загальної ефективності екосистеми IoT. Такий підхід дозволяє швидко реагувати на потенційні загрози та запобігати можливим збоям у роботі системи.

На рисунку 2.3 показаний приклад обміну пакетами між двома пристроями IoT через контролер в IoT-AD. Спочатку встановлюється TCP-з'єднання між пристроєм 1 і контролером, що забезпечує стабільний канал для обміну даними. Після цього пристрій надсилає контролеру команду, пов'язану з подією, наприклад, сигнал від датчика руху, який виявляє активність у кімнаті, або дані про зміну температури. Контролер обробляє отриману інформацію та, залежно від сценарію, може ініціювати відповідну дію, наприклад, ввімкнення освітлення або надсилання сповіщення.

Після успішного отримання команди контролером з'єднання TCP з пристроєм 1 розривається, і контролер виконує процес для передачі команди пристрою 2.

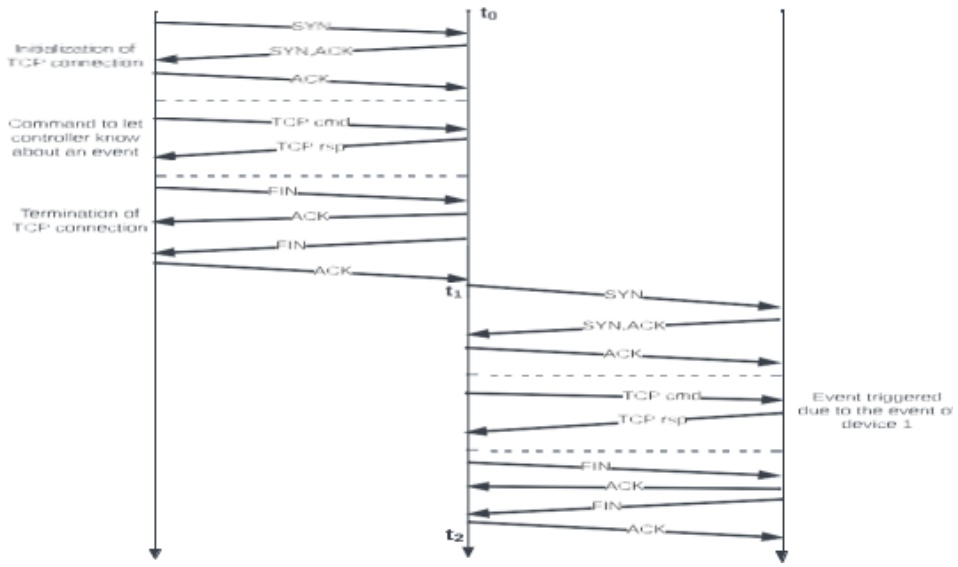

Рисунок 2.3 – Приклад обміну пакетами між двома пристроями IoT через контролер в IoT-AD

У описаному процесі в IoT-AD події, ініційовані пристроєм (наприклад, датчиком руху, що активує світло), викликають обмін пакетами між пристроями в мережі. Кожна подія супроводжується певною послідовністю пакетів, що містять заголовки з інформацією про TCP прапорці, порти призначення і джерела, а також довжину пакетів. Ці характеристики залишаються стабільними для кожної конкретної події, що дозволяє їх використовувати для виявлення події.

Контролер фіксує цю послідовність пакетів, а після виявлення події оновлює журнал пристрою, який її спричинив, додаючи відомості про подію. Після того, як подія та всі пов'язані з нею дії перевірені, журнал події зберігається в хмарі, а на контролері може бути видалений, якщо ресурси обмежені.

Пакетні підписи в IoT-AD формуються за допомогою кортежів, що включають різні поля заголовка пакетів. Це включає:

- номери портів джерела та призначення;
- довжину пакетів;
- типи TCP прапорців;
- часовий проміжок події;
- напрямок пакетів.

– Ці підписи дають можливість ефективно відстежувати і класифікувати події, що відбуваються в мережі IoT, і є основою для виявлення аномалій та моніторингу пристроїв у середовищі IoT.

2.5 Висновки

У цьому розділі представлено дизайн IoT-AD, який включає механізми для виявлення аномалій на рівні пакетів, що виникають унаслідок взаємодії між пристроями IoT. Також розглянуто підходи, спрямовані на підтримку стабільного стану пристроїв IoT протягом тривалого часу. Окрему увагу приділено можливостям відновлення пристроїв після виникнення аномалій, які можуть поширюватися серед них, забезпечуючи безперебійну роботу системи навіть у разі збоїв.

Було впроваджено прототип IoT-AD, який оцінювався як на основі відкритих наборів даних пристроїв IoT, так і через реальне розгортання на невеликому тестовому стенді IoT, створеному в рамках роботи. Прототип також було порівняно з попередніми підходами для виявлення аномалій у середовищах IoT.

Результати оцінки показали, що IoT-AD є легким і ефективним рішенням, здатним виявляти аномалії пристроїв IoT менш ніж за 2,12 мілісекунди з точністю 98%.

У цьому розділі було розглянуто кілька платформ контролерів для пристроїв IoT, таких як IFTTT, Samsung SmartThings і Apple Homekit, які інтегрують різні пристрої IoT від різних виробників. Було виявлено, що, коли пристрої показують нетипову поведінку або повідомляють неточні показання, це визначається як аномалія.

Зокрема, розглянуто IoT Anomaly Detector (IoT-AD), який виявляє аномалії на рівні пакетів та аномалії взаємодії між пристроями IoT. Окрім того, IoT-AD допомагає пом'якшити наслідки поширених аномалій, дозволяючи пристроям відновлюватися після їх поширення. IoT-AD виступає як розширена структура для

контролера пристроїв IoT, здатна виявляти аномалії та допомагати пристроям відновлюватися після них.

Далі було зазначено, що виявлення аномалій полягає у виявленні нетипових закономірностей у поведінці пристроїв порівняно з типовими. У попередніх дослідженнях використовувалися різні підходи, такі як аналіз трафіку, сигнатури на рівні пакетів та семантичні моделі, тоді як у цьому дослідженні було застосовано власні методи виявлення аномалій.

Важливою частиною було симулювання середовища розумного дому, де порівнювалася поведінка реального і симульованого середовища для виявлення поведінкових аномалій.

Підсумовуючи, у роботі зазначено, що несправності пристроїв IoT можуть бути програмними або апаратними. Це можуть бути фантомні команди, збої в командних системах, затримки в оновленні статусу або втрати подій, що виникають через системні збої, проблеми з підключенням до мережі або помилки в операційних системах. Апаратні несправності можуть призводити до помилкових подій або збоїв команд.

Для виявлення цих несправностей у IoT-AD впроваджено пакетні підписи на основі кортежів полів заголовка пакетів. У розробці використовувались характеристики, такі як номери портів джерела та призначення, довжина пакетів, типи прапорців TCP, часові проміжки подій і напрямки пакетів, що дозволяє генерувати підписи для різних подій у мережі.

3 РЕАЛІЗАЦІЯ МЕТОДУ ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ ПРИСТРОЇВ У БЕЗПРОВОДОВИХ МЕРЕЖАХ IOT

У цьому контексті аномалія на рівні пакетів виникає, коли набір обміняних пакетів, що стосуються певної події, не збігається з раніше згенерованими підписами подій, або не має подібного шаблону. Це може бути ознакою аномальної поведінки, яка може бути викликана несправними пристроями, датчиками чи скомпрометованими пристроями в результаті зловмисних атак.

Для вирішення цієї проблеми у середовищі IoT-AD використовується легка модель машинного навчання, яка працює на контролері і відповідає за виявлення аномалій на рівні пакетів. Модель навчена на основі раніше зібраних сигнатур подій, що дозволяє їй розпізнавати типову поведінку пристроїв IoT.

Кожен пристрій IoT зазвичай виконує певний набір операцій протягом певного часу, тому особливості потенційних подій для кожного пристрою можуть бути заздалегідь зібрані і використані для створення навчального набору даних. Це дозволяє моделі виявляти аномалії, порівнюючи нові вхідні події з наявними шаблонами.

Після навчання, контролер використовує цю модель для перевірки вхідних подій. Якщо подія є "дозволеною" або "нормальною" згідно з передбаченням моделі, контролер дозволяє події продовжуватися. У випадку, якщо подія виявляється аномалією (тобто, не відповідає жодному з відомих шаблонів), контролер припиняє подію, що дозволяє запобігти потенційним проблемам через несправні або скомпрометовані пристрої.

3.1 Оцінки

Процес оцінювання IoT-AD складається з трьох ключових етапів. На першому етапі використовуються відкриті набори даних пристроїв IoT, зібрані через платформи контролерів IoT, такі як IFTTT та SmartThings. Ці дані

застосовуються для створення сигнатур на рівні пакетів, а також для відтворення сценаріїв у контролері IoT-AD з метою виявлення аномалій і перевірки взаємодії між пристроями. Наступним етапом є створення тестового стенду, який включає реальні пристрої IoT, щоб оцінити ефективність IoT-AD у реальних умовах, доповнюючи результати аналізу синтетичних даних. Завершальним етапом є порівняння IoT-AD з іншими підходами, запропонованими в попередніх дослідженнях, що дозволяє оцінити його здатність виявляти аномалії у порівнянні з існуючими методами. У процесі оцінювання використовувалися три загальнодоступні набори даних для пристроїв IoT, зібрані через платформи контролерів, такі як IFTTT і SmartThings. Один з них — це набір даних Manufacturer Usage Description (MUD), що містить реальні траси трафіку для 10 різних типів інтелектуальних пристроїв, зібрані протягом 21 дня. Цей набір включає два типи слідів: об'ємні сліди атак (наприклад, спуфінг ARP, флуд TCP/UDP) та доброякісні сліди. Відповідно, цей набір даних надає інформацію про кількість потоків MUD за хвилину, час початку та завершення атаки,

Таблиця 3.1 – Наведені набори даних, що використовуються для оцінки IoT-AD

Dataset	Setup	No. of devices	Duration	Content Type	Data Type
MUD	Smart Home	10	21 days	Packet Lavel Data + Device Iteraction Data	pcap
Mon(IoT)r	Smart Home	45	3 days per device	Packet Lavel Data + Device Iteraction Data	pcap
PingPong	Smart Home	16	15 days	Packet Lavel Data + Device Iteraction Data	pcap
Testbed data	Smart Home	12	10 days	Packet Lavel Data + Device Iteraction Data	pcap

Опис кожного з наборів даних та тестового стенду для розумного дому розкриває їхню роль у дослідженні. Набір даних Mon(IoT)r зібрано протягом 85 днів у США та Великій Британії, включаючи треки з кількох пристроїв. Кожен файл PCAP відповідає певній події пристрою, містить кілька екземплярів подій, позначки часу та дозволяє генерувати підписи для кожної події. Набір даних PingPong включає PCAP-файли мережевого трафіку для 22 популярних пристроїв IoT, де зафіксовано різні функції та події з позначками часу, що дає змогу аналізувати початок і завершення подій. Для оцінки IoT-AD використовувався тестовий стенд, створений шляхом переобладнання однокімнатної квартири в типове середовище розумного дому. У ньому проводилася реальна перевірка ефективності IoT-AD у виявленні аномалій і взаємодій пристроїв, а також тестування можливостей відновлення пристроїв після аномалій.

Ці набори даних і тестовий стенд стали основою для оцінки і тестування IoT-AD, надаючи реальні умови для перевірки роботи системи виявлення аномалій у середовищі IoT.

На рисунку 3.1 показана схема розташування тестового стенду і місця розташування використовуваних пристроїв IoT. У таблиці 3.2 наведено детальну інформацію про пристрої, які були використані. Розроблений тестовий стенд містить загалом 12 позицій.

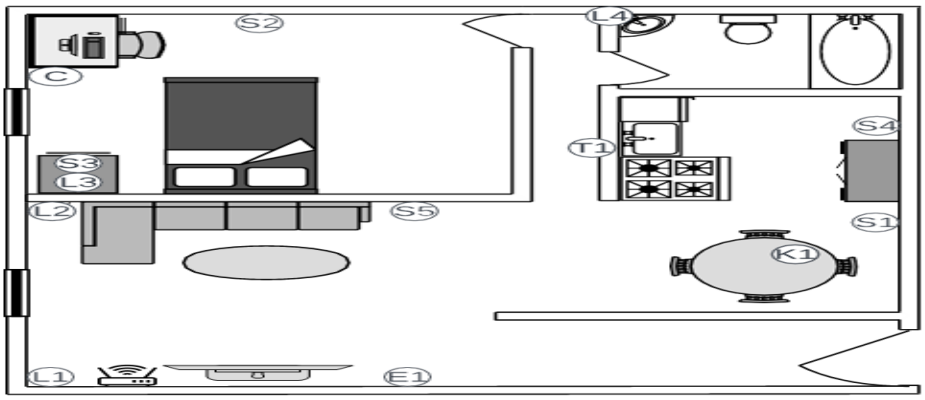

Рисунок 3.1 – План поверху тестового стенду IoT та макет розгортання пристрою

Пристрої IoT можуть обмінюватися даними через контролер IoT-AD, який керує їх взаємодією та активує події згідно з налаштованими умовами. Всі пристрої

підключаються до цього контролера через бездротову мережу в межах локальної мережі.

У тестовому стенді для контролера IoT-AD використовувався міні-комплект Intel Next Unit Computing (NUC). Контролер працював з програмою-демоном, яка здійснювала моніторинг всіх пакетів, що обмінюються пристрої IoT. Для збору мережевого трафіку та відстеження взаємодій між пристроями протягом 10 днів була застосована бібліотека PyShark на Python.

Таблиця 3.2 – Список пристроїв IoT, що використовуються на моєму тестовому стенді, та їх скорочені етикетки

Абревіатура	Ім’я пристрою
C	Міні-комплект Intel NUC як контролер
L1	Розумне сітло Govee
L2	Розумна лампочка Sengled
L3	Розумна лампа Tp-link
L4	Розумне світло Rasa
S1	Розумна розетка TP-link
S2	Розумна розетка Teckin
S3	Розумна розетка WeMo
S4	Розумна розетка KMC з 4 розеткми WiFi
S5	Розумна розетка Amazon
T1	Термостат Ecobee
E1	Echo Dot 4-го покоління з годинником
K1	Розумний чайник Korex

Для взаємодії з пристроями та збору часових позначок функцій пристроїв також використовувалися різні API, надані постачальниками. Детальні відомості про набір даних тестового стенду були представлені в таблиці 3.1.

3.2 Порівняння з раніше запропонованими підходами.

Було проведено порівняння IoT-AD з іншими фреймворками, зокрема з фреймворком на основі штучної нейронної мережі (ANN) для виявлення аномалій

і вторгнень, а також з фреймворком на основі згорткових нейронних мереж (CNN) для виявлення аномалій IoT і вторгнень. Для цього порівняння використовувалися чотири набори даних (MUD, Mon(IoT)r, PingPong та набір даних із тестового стенду).

Для виявлення аномалій на рівні пакетів було застосовано чотири алгоритми машинного навчання: випадковий ліс, k-Nearest Neighbors (KHH), дерево рішень та автокодер.

Для перевірки взаємодії між пристроями було реалізовано контролер IoT-AD на основі описаного раніше дизайну. Оцінка ефективності контролера проводилася за кількома показниками. Час висновків вимірює, скільки часу контролер IoT-AD потребує для визначення події або взаємодії, яка може містити аномалію на рівні пакета або бути нелегітимною. Використання пам'яті визначає кількість пам'яті, необхідної для виявлення аномалій на рівні пакетів та перевірки взаємодій. Використання ЦП оцінює завантаження центрального процесора під час перевірки взаємодій та виявлення аномалій.

Ці показники допомогли визначити ефективність і продуктивність IoT-AD у порівнянні з іншими підходами, зокрема щодо точності виявлення аномалій та швидкості обробки даних. Завдяки детальному аналізу було продемонстровано, що IoT-AD перевершує традиційні методи в умовах реального часу, забезпечуючи своєчасне реагування на потенційні загрози.

3.3 Оцінка виявлення аномалій на рівні пакетів

На рисунку 3.1 представлені результати оцінки точності ідентифікації аномалій на рівні пакетів для різних наборів даних та алгоритмів навчання. Результати свідчать, що використання ознак, отриманих на рівні пакетів, спеціально розроблених для пристроїв IoT, дозволяє суттєво підвищити ефективність виявлення аномалій навіть у гетерогенних середовищах із високим рівнем шуму.

Це забезпечує більш точну і своєчасну реакцію на загрози, що є критично важливим для забезпечення безпеки та стабільності систем IoT.

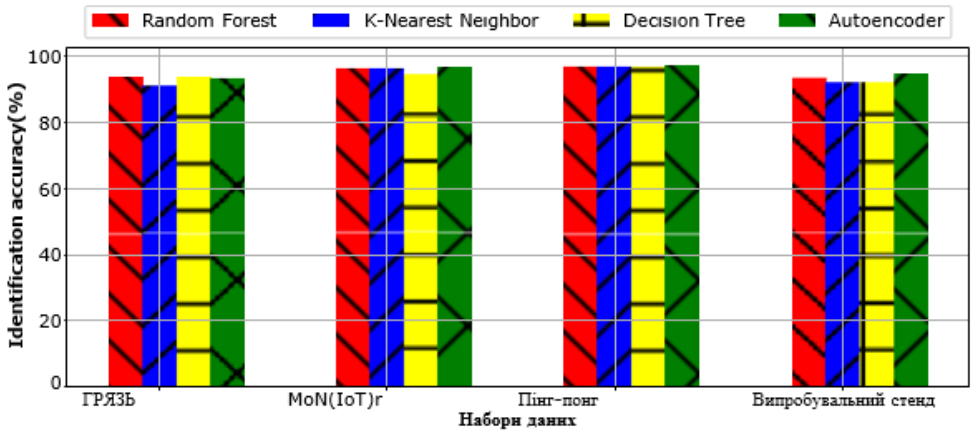

Рисунок 3.2 – Точність виявлення аномалій на рівні пакетів за допомогою IoT-AD для різних наборів даних

Точність виявлення аномалій на рівні пакетів, яка показана на рисунку 3.3, демонструє високі результати ідентифікації аномалій для різних моделей і наборів даних. IoT-AD продовжує показувати чудову ефективність, досягаючи точності понад 90% у всіх випадках. У деяких ситуаціях точність навіть досягає 98%, що свідчить про високу ефективність IoT-AD у виявленні аномалій на рівні пакетів, навіть з різними наборами даних.

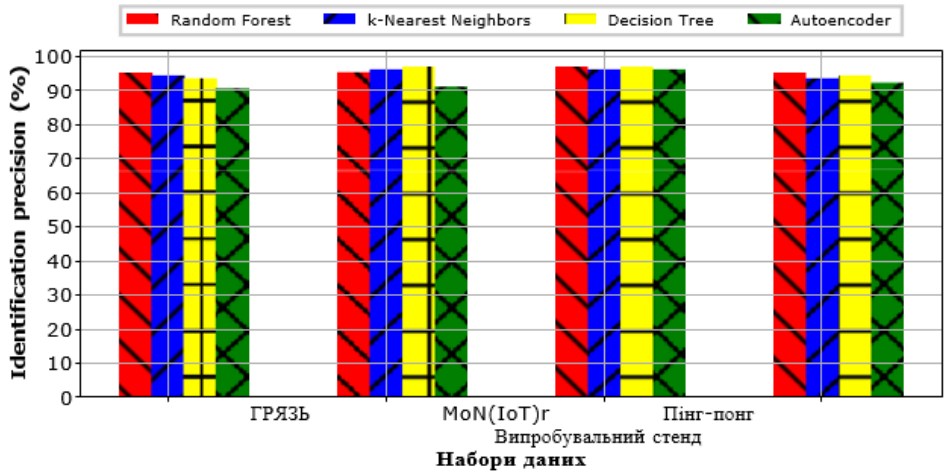

Рисунок 3.3 – Оцінка точності виявлення аномалій на рівні пакетів за допомогою IoT-AD для різних наборів даних

Оцінка F1 для виявлення аномалій на рівні пакетів, представлена на рисунку 3.4, показує результати для різних моделей ідентифікації аномалій та наборів даних. Бали F1 демонструють, наскільки ефективно кожна модель балансує точність і відгук при виявленні аномалій. Вищі значення F1 свідчать про кращу здатність моделі правильно виявляти аномалії, мінімізуючи як хибні спрацьовування, так і пропуски.

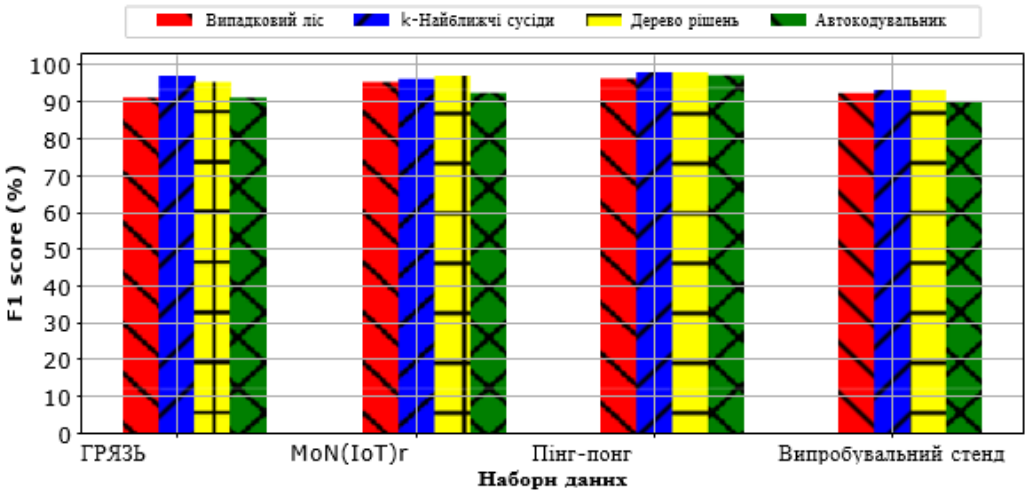

Рисунок 3.4 – Оцінка F1 виявлення аномалій на рівні пакетів за допомогою IoT-AD для різних наборів даних

Результати, представлені на рисунку 3.6, демонструють, що точність і оцінка F1 є основними показниками ефективності моделі для виявлення аномалій на рівні пакетів. Точність відображає частку справжніх позитивних прогнозів серед усіх позитивних, що дозволяє оцінити здатність моделі правильно ідентифікувати аномалії. Оцінка F1 характеризує баланс між точністю та відкликом, забезпечуючи комплексне уявлення про здатність моделі знаходити аномалії з мінімальним рівнем хибнопозитивних і хибнонегативних результатів. Досягнуті результати, де F1 перевищує 90% (а в деяких випадках сягає 98%), свідчать про високу ефективність моделей у вирішенні завдання виявлення аномалій. На рисунку 3.5 показано, що для визначення аномалії на рівні пакета IoT-AD потребує в середньому менше 2,12 мілісекунди. Однак час висновку може змінюватися в залежності від складності

пристроїв і набору даних. Наприклад, набір даних MoN(IoT)r показав більший час висновку через наявність складніших пристроїв, таких як smart TV або розумні холодильники, які використовують більш складні протоколи зв'язку і більше пакетних обмінів порівняно з простішими пристроями (наприклад, розумними лампочками або перемикачами).

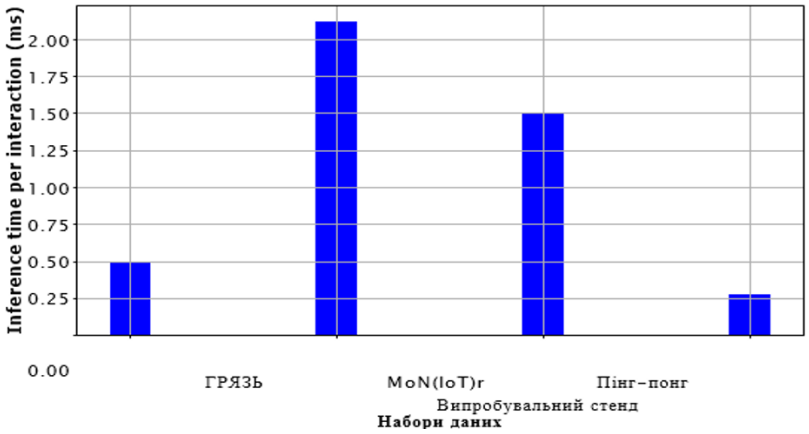

Рисунок 3.5 – Час виведення для аномалій на рівні пакетів пристрою

Результати на рисунку 3.6 демонструють використання пам'яті контролером IoT-AD під час виявлення аномалій на рівні пакетів. Вказано, що для виявлення аномалій контролеру потрібно кілька сотень мегабайт пам'яті (максимум до 227 МБ). Це підтверджує, що навіть при обмежених ресурсах пам'яті на контролерних пристроях, IoT-AD може ефективно здійснювати виявлення аномалій на рівні пакетів.

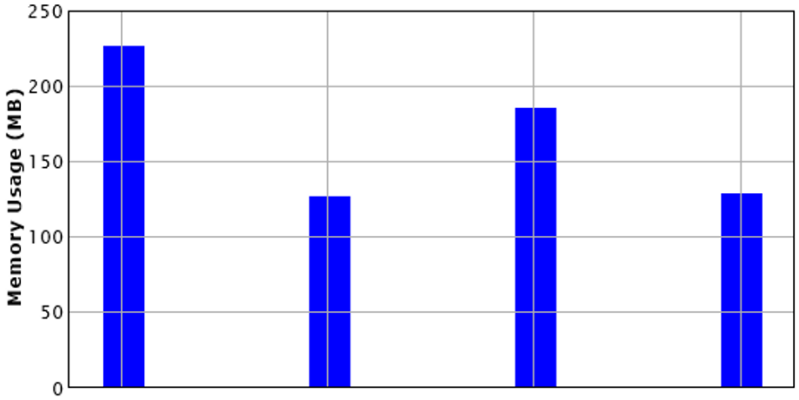

Рисунок 3.6 – Використання пам'яті під час виявлення аномалій на рівні пакетів

На рисунку 3.7 показано навантаження на процесор контролера IoT-AD під час виявлення аномалій на рівні пакетів. Результати вказують, що контролер використовує менше ніж 10% доступних потужностей процесора для виявлення аномалій у трафіку, що обмінюється між пристроями IoT. Це свідчить про те, що IoT-AD здатний ефективно виявляти аномалії без значного навантаження на апаратні ресурси.

Цей показник підтверджує, що система IoT-AD може бути розгорнута навіть на пристроях з обмеженими ресурсами процесора, що є важливим для використання в масштабних або енергоефективних мережах IoT. Такий підхід дозволяє інтегрувати IoT-AD в різноманітні контролери, навіть у пристрої з малопотужними процесорами, гарантуючи стабільну роботу в складних умовах IoT-мереж.

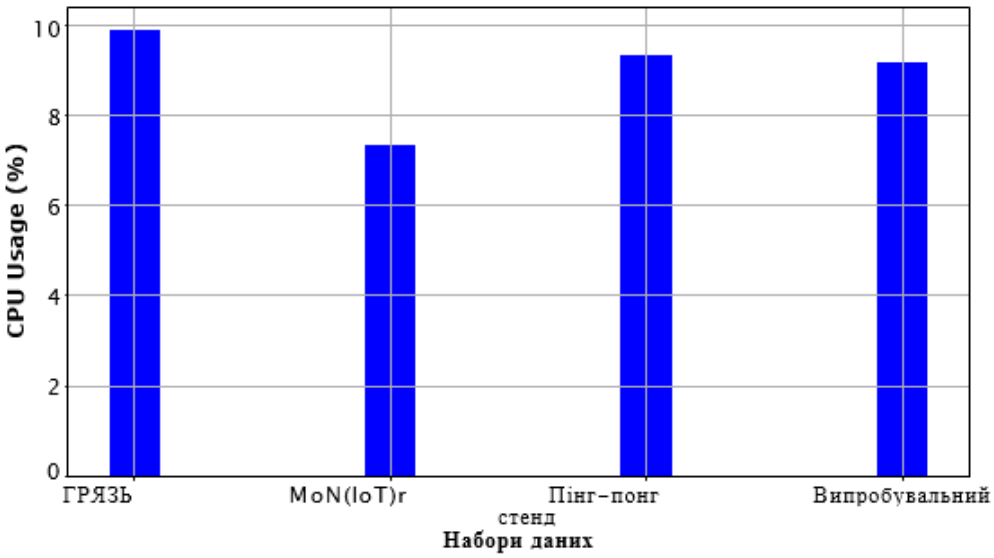

Рисунок 3.7 – Використання ЦП під час виявлення аномалій на рівні пакетів

На рисунку 3.8 показано час висновків для перевірки кожної взаємодії пристрою на основі різних наборів даних. Результати оцінки демонструють, що контролеру IoT-AD необхідно всього 1,74–1,83 мс для перевірки взаємодії між пристроями та відкату до останнього відомого стабільного стану в разі виявлення аномалії. Ці результати підтверджують високу швидкість роботи системи

виявлення аномалій, що дозволяє підтримувати стабільність IoT-мережі навіть за умов виявлення потенційних загроз або аномалій.

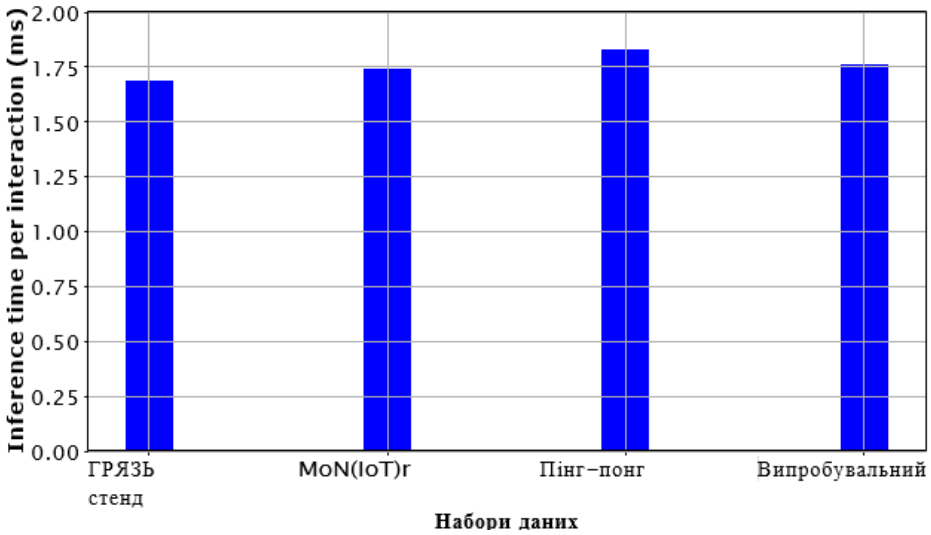

Рисунок 3.8 – Час на висновок і відкат для взаємодії

На рисунку 3.9 показано необхідну пам'ять для перевірки взаємодії між пристроями на основі різних наборів даних. Цей модуль не лише перевіряє взаємодії між пристроями, але й здатний виявляти аномалії в цих взаємодіях і виконувати відкат до останнього стабільного стану, якщо це необхідно

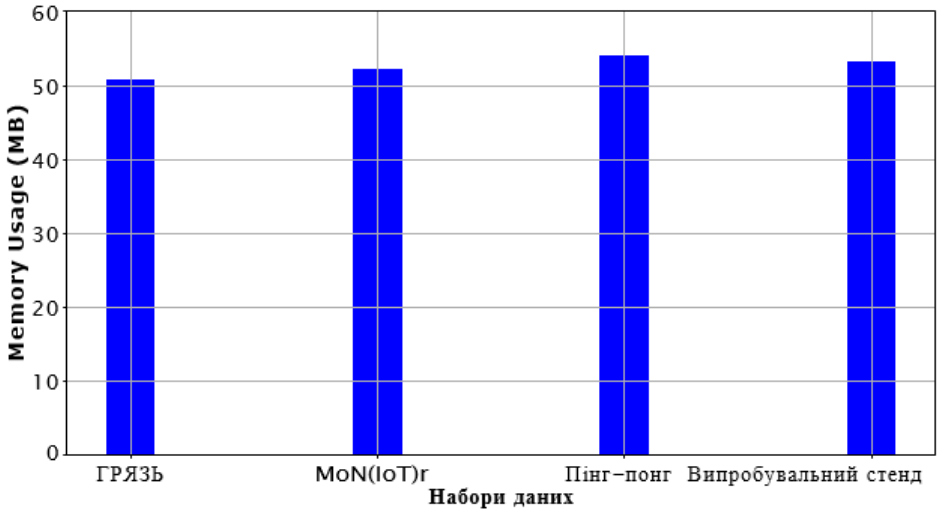

Рисунок 3.9 – Використання пам'яті під час перевірки та відкату взаємодії з пристроєм

На рисунку 3.10 показано результати використання ЦП під час перевірки взаємодії з пристроєм та відкату в разі виявлення аномалії. Використання ЦП у цих процесах коливається від 16,8% до 23,1%, що вказує на невелике навантаження на процесор. Це означає, що ці процеси можуть успішно працювати навіть на контролерах IoT з обмеженими обчислювальними ресурсами.

Хоча IoT-AD показує на 1%-3% нижчу точність виявлення аномалій порівняно з більш складними фреймворками, заснованими на штучних нейронних мережах (АНН) і згорткових нейронних мережах (СНН) (через їх більш складні архітектури), він має значні переваги в інших аспектах. Зокрема:

– зниження використання пам'яті на 22%-63%;

– зниження навантаження на процесор на 39%-62%.

Ці переваги роблять IoT-AD більш придатним для використання в умовах обмежених ресурсів, таких як малопотужні контролери IoT, зберігаючи при цьому ефективність виявлення аномалій і забезпечуючи стабільність роботи мережі.

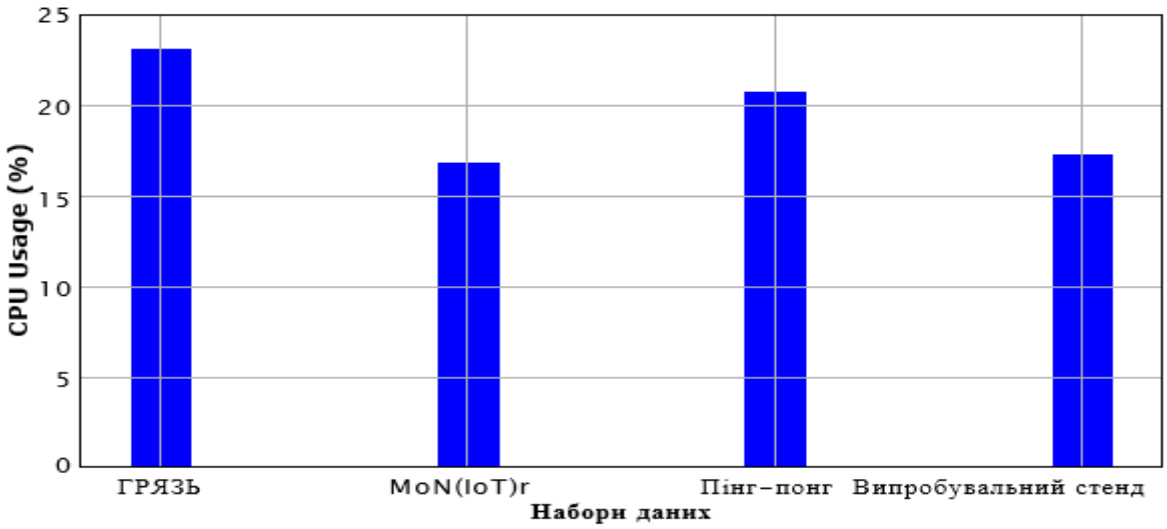

Рисунок 3.10 – Використання ЦП під час перевірки та відкату взаємодії з пристроєм

На відміну від інших фреймворків, IoT-AD має кілька ключових переваг. По-перше, механізм виявлення аномалій на рівні пакетів дозволяє швидко та точно виявляти аномальні події, що виникають у мережевому трафіку між пристроями

IoT. По-друге, IoT-AD здатен перевіряти взаємодії між взаємопов'язаними пристроями, що дає змогу виявляти аномальні або нелегітимні взаємодії в реальному часі. І, по-третє, система має функцію відкату до останнього стабільного стану пристроїв у разі виявлення аномалії, що дозволяє зменшити негативний вплив пошкоджених чи некоректних взаємодій на загальну роботу мережі. Ці функціональні можливості роблять IoT-AD більш універсальним і надійним рішенням для безпеки мереж IoT порівняно з іншими підходами, що не мають таких вбудованих механізмів для відновлення і перевірки взаємодій між пристроями.

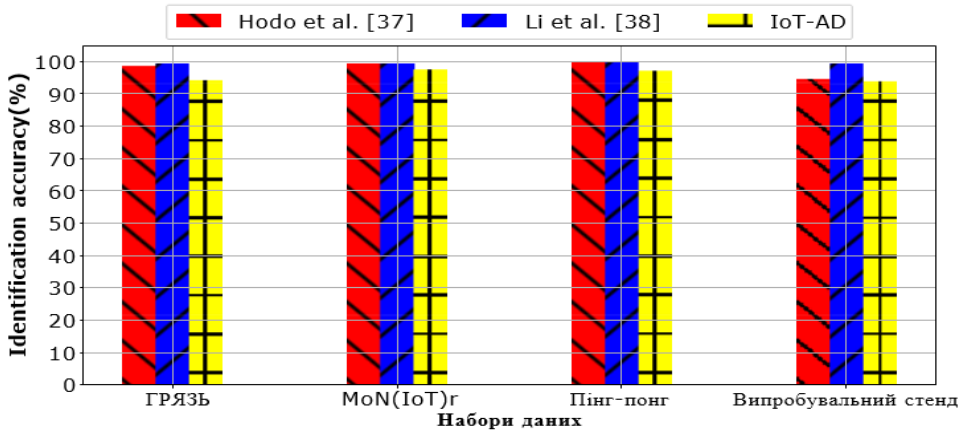

Рисунок 3.11 – Порівняння ефективності виявлення аномалій на рівні пакетів між IoT-AD та іншими фреймворками

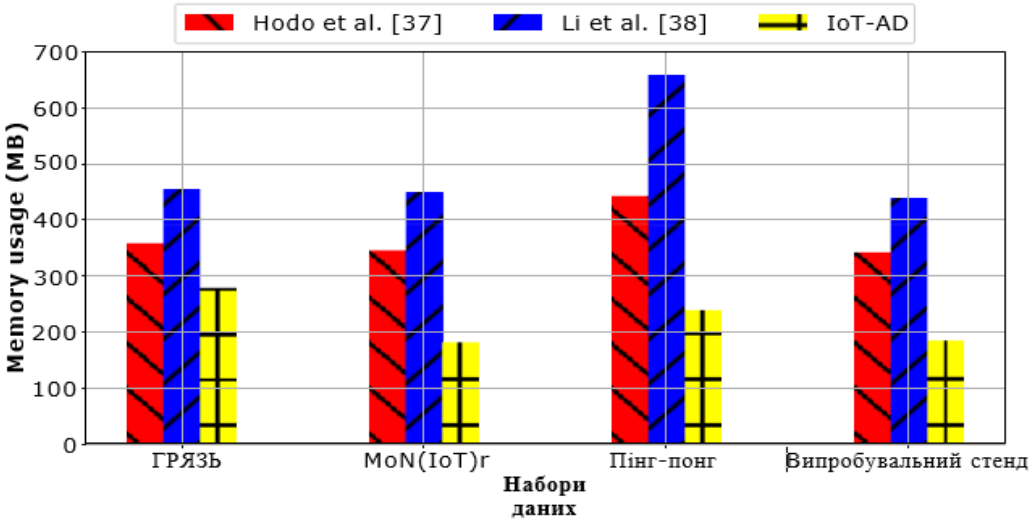

Рисунок 3.12 – Порівняння використання пам'яті між IoT-AD та іншими фреймворками

IoT-AD демонструє легкість і ефективність, працюючи на контролерах з обмеженими ресурсами завдяки мінімальному використанню пам'яті та ЦП, що робить його підходящим для широкого спектра пристроїв IoT. Крім того, швидкість висновків IoT-AD, як показано на рисунку 3.13, на 48% швидша, ніж у інших фреймворків, що є важливою перевагою для виявлення аномалій у реальному часі. Така швидка реакція на аномалії критично важлива для IoT-систем, оскільки вона дозволяє запобігти серйозним збоям або атакам. Отже, IoT-AD забезпечує ефективне та швидке виявлення аномалій, навіть на пристроях з обмеженими ресурсами, що є ключовим для безпеки розумних мереж IoT.

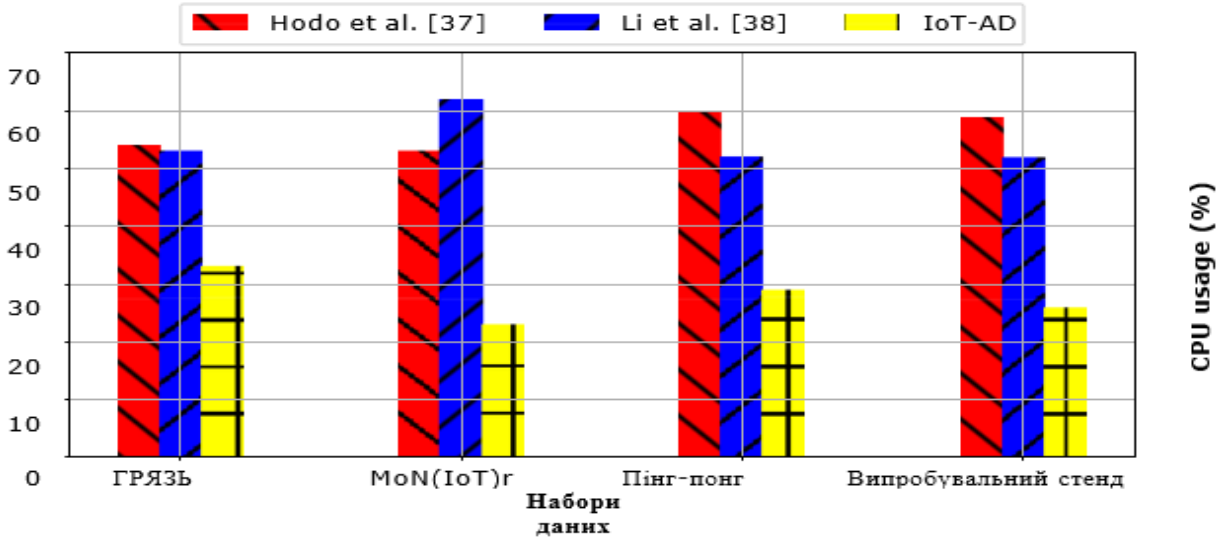

Рисунок 3.13 – Порівняння використання ЦП між IoT-AD та іншими фреймворками

Подальший аналіз результатів показує, що шум у мережі є важливим фактором, який може впливати на час виведення виявлення аномалій у системах IoT. Шум тут включає непов'язаний з подіями трафік, який, хоч і передається між пристроями, не має безпосереднього відношення до фактичних подій або аномалій.

Один з прикладів цього типу шуму включає трафік, який генерується різними мережевими протоколами, такими як ARP або DNS-запити. Інший приклад — трафік, пов'язаний з оновленнями мікропрограм або автоматичними перевірками стану пристроїв, що не є частиною основної події, яку контролер повинен

обробляти. Такий шум може значно збільшити час обробки, оскільки контролер змушений обробляти додаткові дані, що не стосуються основної мети. Однак правильне налаштування системи або фільтрація цього трафіку може значно зменшити вплив цього шуму та покращити ефективність обробки. застосування фільтрації шуму допомагає мінімізувати ці впливи, що дозволяє IoT-AD зберігати свою високу ефективність, навіть за умов присутності зайвого трафіку в мережі.

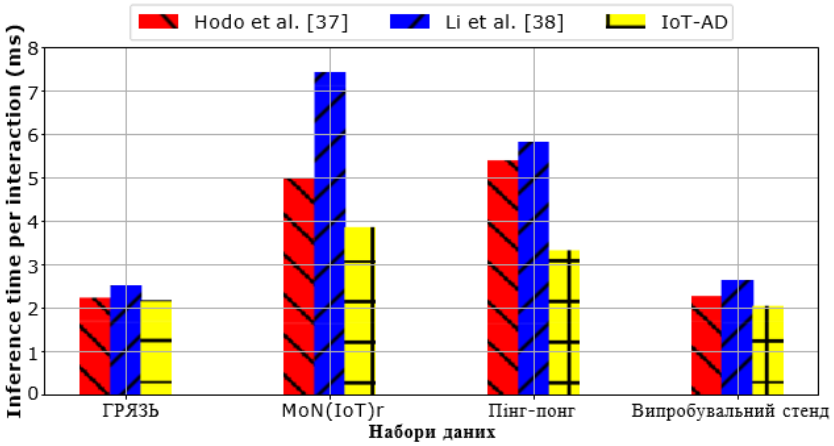

Рисунок 3.14 – Порівняння часу висновків між IoT-AD та іншими фреймворками

Отже, для забезпечення швидкості та точності виявлення аномалій важливо не тільки оптимізувати алгоритми виявлення, але й активно враховувати фактори, що можуть сприяти виникненню мережевого шуму, і впливати на продуктивність системи.

3.4 Висновки

У цьому розділі було проаналізовано процес вибору пристрою, який може виконувати роль контролера для IoT-AD, а також визначено оптимальні умови для його розміщення. Зокрема, було зазначено, що для контролера можна вибрати пристрій IoT, який має достатньо ресурсів для виконання функцій виявлення

аномалій на рівні пакетів і взаємодії. Це можуть бути, наприклад, смарт-телевізор або розумний холодильник, оскільки вони часто мають необхідні обчислювальні потужності. Важливо, що вимоги до ресурсів для виявлення аномалій були чітко визначені в процесі попередніх оцінок.

Контролер IoT-AD може бути розгорнутий як локально в середовищі IoT, так і віддалено в хмарі. Локальний розгортання забезпечує низьку затримку в процесі виявлення аномалій і підтримує взаємодію пристроїв у реальному часі. Крім того, це дозволяє уникнути передачі чутливого трафіку на зовнішні сервіси, що знижує ризик витоку даних. З іншого боку, хмарне розгортання дає більше можливостей для масштабування та забезпечує високу надійність системи за рахунок використання розподілених ресурсів, що також може бути корисно для великих IoT-мереж.

Було також проаналізовано можливі сценарії атак в середовищах IoT, зокрема DDoS-атаки, коли вразливі пристрої IoT можуть бути скомпрометовані і використовуватись у ботнетах для атак на сервери. IoT-AD здатний ефективно протистояти таким атакам, відстежуючи трафік між пристроями і визначаючи аномалії, якщо знайдені невідомі або підозрілі шаблони. У разі виявлення таких аномалій, контролер ізолює скомпрометовані пристрої, що допомагає зупинити оркестрацію DDoS-атак.

Не менш важливими також є спуфінгові атаки, якщо пристрій IoT буде скомпрометовано, зловмисник може підробити його IP-адресу та/або MAC-адресу. У результаті зловмисник може надіслати шкідливу інформацію на інший пристрій IoT у середовищі IoT, щоб маніпулювати його станом, або на мережу за межами середовища IoT.

Контролер IoT-AD має глобальне представлення середовища IoT, що дозволяє йому виявляти та відкидати підроблені пакети, які надходять з порушених пристроїв. Це дає змогу захистити мережу від атак, де зловмисник видає себе за законний пристрій і намагається маніпулювати станами інших пристроїв. Завдяки створенню дерев взаємодії, IoT-AD може ідентифікувати ці пристрої та ізолювати їх від мережі, тим самим запобігаючи шкоді.

У випадку пасивних атак, таких як аналіз трафіку або спіффінг, контролер здатний розпізнавати "шумові" патерни, які включаються в комунікацію між пристроями IoT. Ці патерни можуть бути заздалегідь узгоджені між контролером та пристроєм, що дозволяє контролеру відокремити їх від законного трафіку, знижуючи ризики витоку інформації або несанкціонованого збору даних.

Однак один із головних недоліків IoT-AD — це єдина точка відмови, оскільки якщо контролер вийде з ладу, вся система може припинити свою роботу. Для пом'якшення цього ризику можна застосувати два підходи. Перший — це використання кількох локальних контролерів IoT, що дозволяє забезпечити безперервність роботи в разі відмови одного з них. Потрібні додаткові механізми для синхронізації станів цих контролерів. Другий варіант — це хмарний контроль, при якому хмарні постачальники можуть ефективно управляти резервними контролерами та мінімізувати збої.

Що стосується аномалій, IoT-AD здатний ефективно виявляти та відновлювати аномалії в мережевому трафіку та взаємодії між пристроями. Однак, існують й інші причини аномалій, такі як апаратні збої або проблеми з живленням пристроїв IoT, які IoT-AD наразі не може обробляти. Для розширення можливостей, система може бути доповнена функціями для виявлення аномалій, що виникають на фізичному рівні пристроїв.

Щоб досягти цього, контролер повинен бути оснащений додатковим обладнанням (наприклад, програмно-визначеним радіоприймачем, аналізатором спектру) для збору даних фізичного рівня, а мою модель потрібно буде відповідним чином тренувати, щоб виявляти аномалії на основі даних фізичного рівня.

У цьому розділі представлений фреймворк IoT-AD, який виявляє і зменшує вплив аномалій у трафіку та взаємодіях між пристроями IoT. Оцінки показують, що IoT-AD є ефективною та мало ресурсномісткою системою, здатною виявляти аномалії за час менш ніж 2,12 мс з точністю до 98%.

4 ДОСЛІДЖЕННЯ АНОМАЛІЙ В БЕЗДРОТОВИХ ЛІНІЯХ ЗВ’ЯЗКУ IoT МЕРЕЖАХ

Інтернет речей (IoT) привернув велику увагу як у промисловості, так і серед науковців завдяки постійному виходу на ринок нових розумних пристроїв. Це включає оновлену побутову техніку, носимі пристрої, засоби для охорони здоров'я, транспортні засоби та промислові машини, і це лише деякі з прикладів. Для підтримки цього технологічного прогресу було розпочато значні дослідження та розробки, спрямовані на забезпечення ефективного і автоматизованого функціонування в таких галузях, як виробництво, сільське господарство, транспорт і охорона здоров'я, завдяки їх величезному економічному потенціалу.

Щоб забезпечити ефективне управління великими мережами IoT, необхідні рішення для автоматичного моніторингу та виявлення несправностей, які оперативно сповіщають про проблеми та фільтрують їх без впливу на бізнес-процеси. Збої в роботі мережі або вузла IoT зазвичай вважаються аномаліями мережі або вузла, і вони визначаються різними способами в залежності від аспектів мережі. Наприклад, Sheth та ін. визначають аномалії на фізичному рівні IEEE 802.11, такі як приховані термінали, ефект захоплення, варіації шуму та потужності сигналу. Gupta та ін. описують аномалії в контексті мультихоп мереж, зокрема чорні діри, провали, вибіркові пересилання та затоплення. Аліпур та ін. досліджують аномалії на канальному рівні IEEE 802.11, акцентуючи увагу на атаках, таких як ін'єкційні тести, атаки деаутентифікації, дисоціації, асоціативні та аутентифікаційні флуди.

Виявлення аномалій в мережах IoT зазвичай стосується таких сценаріїв, як вторгнення, шахрайство, несправності, моніторинг стану системи, виявлення подій у мережах датчиків і порушень екосистеми. Більшість досліджень зосереджені на конкретних типах аномалій в рамках певних сценаріїв.

У цьому розділі, з огляду на реальний експериментальний досвід розгортання IoT, будуть розглянуті чотири типи аномалій на канальному рівні, які можна виявити: раптова деградація, раптова деградація з відновленням, миттєва

деградація та повільна деградація. Замість того, щоб фокусуватися на причинах аномалії, увага буде зосереджена на симптомах, що спостерігаються у вимірюваннях зв'язку, зокрема на змінах у прийнятому сигналі. В залежності від типу аномалії, будуть виявлені можливі причини, пов'язані з обладнанням, прошивкою або каналом, і розроблені моделі для автоматичної класифікації цих аномалій.

4.1 Перевірка взаємодії з пристроєм

Якщо на рівні пакетів не виявлено аномалій для події, контролер дозволяє її виконання. Крім того, контролер записує інформацію, пов’язану з подією, таку як пристрій, що ініціював подію, та стан пристрою, який був змінений у результаті цієї події. Журнали цієї інформації використовуватимуться для перевірки подій, що відбуваються протягом певного періоду часу, з урахуванням умов, встановлених користувачем або постачальником кожного пристрою.

Прикладами таких умов можуть бути наступні: взаємодія між пристроями визначається як подія, ініційована одним пристроєм на іншому пристрої в середовищі IoT. Одна і та ж подія може бути викликана кількома різними пристроями. Наприклад, розумна лампочка може бути включена або датчиком руху, або датчиком освітленості.

Взаємодія між пристроями буде вважатися допустимою, якщо вона відповідає умовам, визначеним користувачем або постачальником, що дозволяє системі IoT працювати так, як очікувалося. Наприклад, користувач може встановити умову, за якою, якщо температура в кімнаті, виміряна розумним термометром, перевищить певне порогове значення, монітор надасть команду через контролер для включення кондиціонера та вентилятора. У цьому випадку включення кондиціонера та вентилятора буде вважатися допустимою взаємодією. Однак, якщо монітор температури намагається увімкнути світло, це буде розцінено як неприпустима взаємодія (аномалія).

Контролер створює і підтримує структури даних, відомі як дерева взаємодії, протягом певного часу. Ці дерева відображають послідовності взаємопов'язаних подій, що виникають внаслідок вимірювань або зчитувань з пристроїв. Пристрій, який ініціює взаємодію, є кореневим пристроєм дерева. Наприклад, на рисунку 4.1 (a) пристрій A є коренем дерева взаємодії.

Коли кореневий пристрій генерує нове вимірювання або зчитування, це призводить до створення нового дерева взаємодії. На рисунку 4.1 (a) показано, як утворюються дерева взаємодії в IoT-AD. У дереві взаємодії 1 пристрою A спрацьовують дві події на різних пристроях (пристрій B та пристрій C). Крім того, подія пристрою B додатково викликає події на пристрої D та пристрої E.

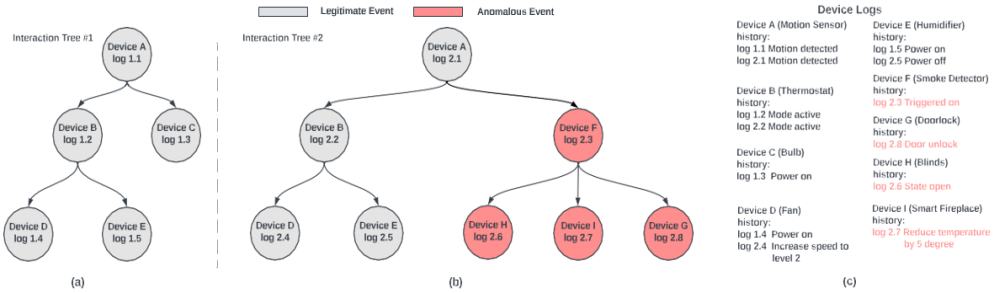

Рисунок 4.1 – Ілюстрація взаємодії між пристроями IoT

Для послідовного запису взаємодій з пристроями та відповідних вимірювань кореневих пристроїв введено формат журналювання на основі пари ключ-значення. Цей формат дозволяє зіставляти кожну подію з унікальним ключем. Унікальний ключ генерується на основі двох різних ідентифікаторів, як показано на рисунку 4.2.

Перша частина ключа, позначена як "X", є порядковим номером вимірювання або зчитування, яке ініціюється кореневим пристроєм. Для кожного нового дерева взаємодії цей порядковий номер збільшується. Друга частина ключа, позначена як "Y", є порядковим номером конкретної події в дереві взаємодії "X". Ми вирішили не використовувати часові мітки як частину генерації ключів, оскільки

синхронізація часу між пристроями IoT є складним завданням, яке потребує додаткових ресурсів і може призвести до неточностей у записах.

Рисунок 4.2 – Генерація журналу пристрою в IoT-AD

У системі IoT кожен пристрій може бути кореневим елементом для кількох дерев взаємодії. Кожне дерево генерується динамічно, коли кореневий пристрій генерує нове вимірювання або зчитування. Наприклад, датчик температури може періодично фіксувати нове зчитування кожні кілька секунд.

IoT-AD використовує правила автоматизації (встановлені користувачами або виробниками пристроїв) для перевірки правильності взаємодій між пристроями. Наприклад, на рисунку 4.1 (b) показано, як вимірювання, зафіксоване пристроєм A, викликає кілька подій на інших пристроях IoT. Якщо, наприклад, на пристрої F виникає аномальна подія, IoT-AD виявляє її, перевіряючи правила автоматизації.

Щоб пом'якшити наслідки таких аномалій і допомогти пристроям повернутися до стабільного стану, IoT-AD пропонує автоматизований механізм відновлення, що називається "відкат". Процес відкату починається, як тільки виявляється аномалія в поведінці пристроїв. Контролер IoT-AD використовує дерево взаємодії для ідентифікації пристроїв, які постраждали від цієї аномалії. Наприклад, аномальна подія на пристрої F може викликати аномальні події на пристроях H, I та G. Тоді IoT-AD створює список постраждалих пристроїв і аналізує їхні журнали, щоб визначити останній стабільний стан кожного з них.

Наприклад, якщо пристрій F був спрацьований через аномальну взаємодію з пристроєм A, його останній стабільний стан буде "спрацьовано". У такому випадку IoT-AD відправить команди для відкату стану цього пристрою до стабільного стану ("спрацьовано"). Крім того, IoT-AD ізолює пристрій, який ініціював аномалію, до моменту, поки власник або адміністратор не виправить проблему.

Цей механізм припускає, що всі взаємодії є допустимими, поки не буде виявлена аномалія. Тобто, пристрої можуть взаємодіяти без попередньої перевірки, і лише у разі виявлення аномалії їхні стани відкочуються назад.

Альтернативою цьому підходу є перевірка кожної взаємодії до її виконання. У такому випадку взаємодія між пристроями була б дозволена лише після перевірки на відповідність правилам автоматизації. Однак такий підхід може значно уповільнити роботу системи, оскільки перевірка взаємодій в реальному часі, особливо за складних правил або великої кількості пристроїв, може заблокувати нормальну роботу середовища IoT, поки не буде проведена перевірка.

4.2 Проведення експериментів

Експерименти, проведені з використанням Google Colaboratory з 32 ГБ оперативної пам'яті та Tensor Processing Unit для прискорення обчислень, оцінювали продуктивність алгоритму за кількома показниками: точність класифікації, точність, запам'ятовування та оцінка F1.

Ці показники виражаються рівняннями нижче,

$$\text{Точність} = \frac{\text{ТП+ТН}}{\text{ТП+ТН+ФП+ФН}} \tag{4.1}$$

$$\text{Точність 2} \ \frac{\text{ТП}}{\text{ТП+ФП}} \tag{4.2}$$

$$\text{Відкликання} = \frac{\text{ТП}}{\text{ТП+ФН}} \tag{4.3}$$

$$F1 - \text{оцінка} = \frac{\text{Точність} \times \text{Точність 2}}{\text{Відкликання}} \tag{4.4}$$

де ТП, ТФ, ТН і ФН означають істинно позитивні, істинно негативні, помилкові спрацьовування і помилкові негативні результати відповідно.

Було протасовано набір і взято 33% як тестовий набір і 66% як набір поїзда. Потім виконано класифікацію трафіку за допомогою 4 алгоритмів: K-Nearest Neighbors (КНН), Decision Tree (ДТ), Random Forest (РФ) та Neural Network (НН). Я використовував пакет python sklearn для проведення нашого тесту.

Для КНН використовувалось тільки 1 сусіда з функцією рівномірної ваги. Ми отримуємо глобальну точність 99,27%, інші показники наводяться в таблиці 4.2.

Таблиця 4.2 – Результати за алгоритмом K Nearest Neighbor

КНН	Точність	Нагадування	Оцінка Формули F1
Зловмисник	0.9633	0.9972	0.9799
Нормальний	0.9996	0.9916	0.9956
Жертва	0.9573	0.9988	0.9976

Для побудови моделі були обрані параметри за замовчуванням через їх оптимальне поєднання точності та швидкості обчислень. Глобальна точність моделі 99,89% свідчить про її високу здатність до узагальнення, що робить її надійним інструментом для вирішення реальних задач. Аналіз інших метрик, таких як точність, повнота та F1-міра, що представлені в таблиці 4.3, підтверджує ефективність вибраного підходу.

Таблиця 4.3 – Результати за алгоритмом «Дерево рішень»

ДТ	Точність	Нагадування	Оцінка формули F1
Зловмисник	0.9956	0.9982	0.9969
Нормальний	0.9998	0.9990	0.9994
Жертва	0.9946	0.9996	0.9970

Результати підтверджують високу ефективність алгоритму «Дерево рішень». Наприклад, отримуємо щось, як показано на рисунку 4.3 для початку дерева, де вузли відповідають за подальший розподіл.

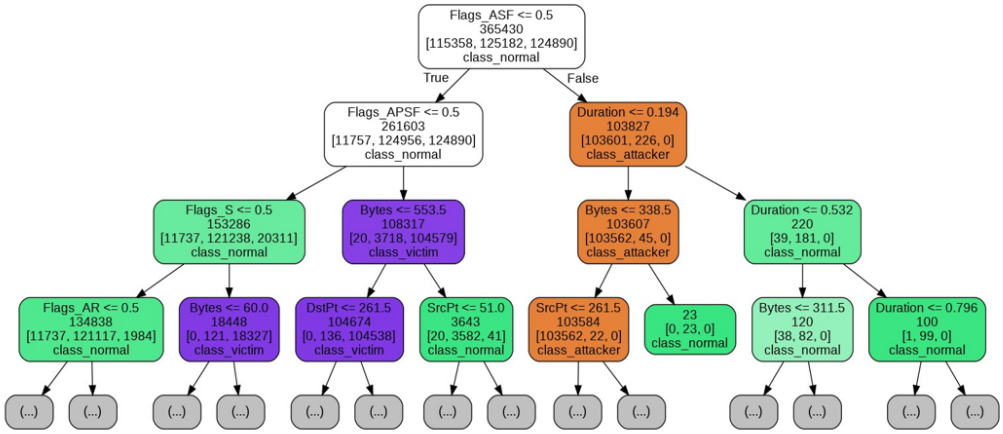

Рисунок 4.3 – Перші вузли дерева рішень

Дерево рішень має глибину 31, 563 вузли та 282 листки, що дає загалом 281 тест. Це дерево можна використати для автоматичної генерації скрипта класифікації (див. вихідний код для прикладу). Запуск цього коду на конкретному екземплярі дасть точність класифікації 99,88%. Для методу випадкового лісу (РФ) були вибрані оптимальні параметри за допомогою стратегії пошуку сітки, яка включала обчислення продуктивності через перехресну валідацію на сітці можливих значень параметрів і вибір найкращого оцінювача.

Як основний показник ефективності була обрана глобальна точність. Зокрема, було використано 800 дерев з максимальною глибиною 20, що дозволило досягти глобальної точності 99,95%, а відповідні показники наведені в таблиці 4.4.

Таблиця 4.4 – Наведені результати за алгоритмом Random Forest

РФ	Тоічність	Нагадування	Оцінка Формули F1
Зловмисник	0.9982	0.9981	0.9982
Нормальний	0.9997	0.9996	0.9997
Жертва	0.9981	0.9993	0.9997

Цікавим результатом випадкового лісу є те, що ми можемо виокремити, які ознаки є найважливішими при обчисленні класифікації. Особливості показані за важливістю на рисунку 4.4.

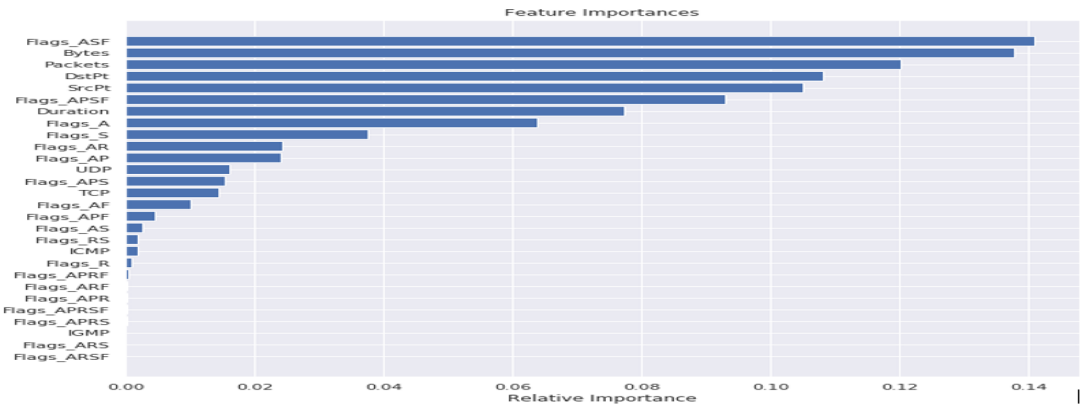

Рисунок 4.4 – Відносна важливість ознак у наборі даних CIDDS-01

Для нейронної мережі був обраний багатошаровий класифікатор персептрона. Ця модель оптимізує функцію втрати за допомогою логарифмічної функції та застосовує методи LBFGS або стохастичного градієнтного спуску. У моделі використовувалося 100 нейронів у прихованому шарі, а функцією активації для прихованого шару була вибрана випрямлена лінійна одиниця (ReLU). Максимальна кількість ітерацій була встановлена на 200. Результатом стала глобальна точність 99,25%. Показники продуктивності для кожного класу наведені в таблиці 4.5.

Таблиця 4.5 – Наведено кінцеві результати за допомогою алгоритму нейронної мережі

НН	Точність	Нагадування	Оцінка Формули F1
Зловмисник	0.9929	0.9938	0.9933
Нормальний	0.9906	0.9962	0.9934
Жертва	0.9914	0.9883	0.9899

Для набору даних CIDDS-01 та алгоритмів машинного навчання ми досягли дуже високої точності. Як було зазначено, для цього конкретного набору даних балансування класів не має значного впливу на точність, яка вже є високою. Завдяки ретельному налаштуванню гіперпараметрів, ми отримали результати, подібні до найкращих алгоритмів, таких як RF-WHICD (де розглядалися лише два класи: нормальні/зловмисники).

Найкращим алгоритмом виявився Random Forest (РЧ) з точністю 99,95%. Однак його вбудовування в IoT-системи може бути складним, і він не забезпечує можливості інтерпретації результатів. Проблема вилучення простих правил із лісу рішень була активно обговорена в спільноті машинного навчання.

Таблиця 4.6 – Наведено порівняння з суміжними роботами

Огляд	Підхід	Точність (%)
Верма і Ранга	2НН	99.60
Верма і Ранга	ДТ	99.90
Тамма і Рі	DNN-10-FCV	99.90
Idhammad	Ентропія+РФ	99.54
Abdulhammed	РФ-УКД	99.99
Запропонований КНН	КНН-1	99.27
Запропонований ДТ	ДТ	99.89
Запропонована РФ	РФ	99.95
Запропонована НН	НН	99.25

Мета полягала в тому, щоб знайти компроміс між силою моделювання випадкових лісів і деякими простими правилами, які можна інтерпретувати як у (маленькому) дереві рішень. Бібліотека Python правил Skope дозволяє нам витягувати такі правила з випадкового лісу.

У експериментах було обрано всі екземпляри, щоб навчити модель і витягти правила.

Для класу потерпілих правила такі:

– Байтів > 100

– Тривалість <= 0,03749999962747097

– Прапорці == АЧС

– А для класу зловмисника визначені правила такі:

– Пт <= 261

– Тривалість <= 0,032500000670552254

– Прапори == APSF

За допомогою цих дуже простих правил ми вже отримуємо глобальну точність 86,88%. Крім того, шляхом простого огляду даних ми виявили, що

додавання екземпляри, позначені прапорцями TCP AR (class victim) або S (class attacker), дозволяють нам підвищити точність до 98,45%, при цьому лише 0,35% є класифікаціями промахів.

Для експериментальної оцінки було використано реальний набір даних вимірювань Рутгерса, що містить інформацію з 29 вузлів при п’яти різних рівнях шуму, причому кожен запис має 300 вимірювань. Хоча кожен канал вимірюється на п'яти рівнях шуму, кожен запис розглядається як окремий зв'язок, і ми припускаємо відсутність кореляції між ними. На цьому реальному наборі даних буде синтетично введено чотири типи аномалій, як було запропоновано в цій роботі.

По-перше, вибирались тільки посилання без втрати пакетів, що зменшує набір даних з 4060 до 2123 (52%) незалежних зв'язків. По-друге, для кожного типу аномалії випадковим чином обирається 33% зв'язків, до яких буде введена аномалія згідно з таблицею 4.7, а решта залишається без змін. Цей підхід дозволяє створити контрольований експериментальний сценарій, де ми можемо чітко оцінити ефективність методів виявлення аномалій.

Розподіл аномалій серед вибраних 33% зв'язків моделює реальні умови мережі, де аномалії виникають нерівномірно, що підвищує практичну релевантність отриманих результатів. Це дозволяє точно імітувати сценарії, коли окремі вузли або сегменти мережі є більш вразливими до атак або збоїв, ніж інші.

Таблиця 4.7 – Показана ін'єкції штучної аномалії для кожного сценарію аномалії

Type	Links	Affected	Appearance	Peristence
SuddenD	2 123	33%(700)	Once, $[200^{th}, 280^{th}]$	For ∞
SuddenR			Once, $[25^{th}, 275^{th}]$	For [5,20]
Instead			On $\approx 1\%$ of a link	For 1 datapoint
SlowD			Once, $[1^{st}, 20^{th}]$	For [150, 180]
$RSSI(x, start) \leftarrow RSSI(x) + \min(0, -rand(0.5,1.5) \cdot (x - start))$				

Раптова аномалія, яка описана в таблиці 4.7, з'являється довільно між 200-м і 280-м пакетом на ураженій ланці і триває без обмежень. У випадку раптового R (який показаний на рисунку 4.2), аномалія з'являється один раз, випадковим чином,

між 25-м і 275-м пакетом, і зберігається протягом випадкової тривалості від 5 до 20 вимірювань.

Для InstaD аномалія може з’явитися в будь-якому місці всього ряду з ймовірністю 0,01, що в середньому означає, що кожна аномалія на ураженій ланці з’являється тричі. Нарешті, повільна аномалія з'являється випадковим чином між 1-м і 20-м вимірюванням і починається з випадкового деградуючого темпу, що триває від 150 до 280 пакетів. Детальну інформацію про ін'єкцію аномалій наведено в таблиці 4.7.

Після введення аномалій відповідно до таблиці 4.7 було створено чотири різні представлення даних. Перше представлення — це значення часу, де кожна ланка перетворюється на єдиний вектор ознак, що містить 300 ознак. Друге представлення включає агреговані ознаки, де кожна ланка узагальнюється до 7 ознак. Третє представлення — це гістограма ознак, де визначено 10 рівних відсіків, і дані представляються вектором ознак, що складається з 10 елементів. Останнє представлення — частотні характеристики, де моделі надається великий вектор ознак у частотній області, що містить майже 150 ознак. Таким чином, для кожного з чотирьох типів аномалій ми генеруємо 16 різних наборів даних кандидатів, що дозволяє створити різноманітні варіанти для подальшого аналізу.

4.3 Основні обмеження

Було визначено три основні обмеження, що стосуються цього дослідження, а також, наскільки я розумію, інших подібних робіт у сфері бездротових мереж і виявлення аномалій IoT, які не орієнтовані на дані додатків, такі як вимірювання.

По-перше, для ефективного використання інструментів машинного навчання необхідно мати достатньо даних для навчання та оцінки. Визначення того, що є «достатнім», є складним, але загалом це означає, що модель повинна отримати достатньо прикладів, щоб точно відображати базовий розподіл. Інтуїтивно можна

сказати, що для вивчення нормального розподілу достатньо менших даних, ніж для експоненціального розподілу.

Хоча синтетичні дані корисні для демонстрації концепції, для більш серйозних завдань потрібні реальні дані. Наскільки я знаю, лише кілька досліджень використовують реальні дані, і жодне з них не займається трасуванням канального шару.

Оскільки набір даних, що використовувався як приклад, включав лише 11 ланок, цього було недостатньо для навчання автоматичних екстракторів ознак і моделей класифікації. Моделі, розроблені для трас IEEE 802.11, не можна безпосередньо застосовувати до трас IEEE 802.15.4, що свідчить про обмеження узагальнення моделей для різних технологій і застосувань.

Модель була протестована на трасах LOG-a-TEC, навчена на синтетичному типі аномалії SuddenD. Вона точно виявила, що дві аномальні ланки не були адекватними. Однак модель помилково класифікувала деякі ланки як аномальні, хоча вони насправді не були такими.

По-друге, архітектура автокодера була обрана для невеликої кількості кандидатів за допомогою методу проб і помилок. Більша кількість даних дозволила б краще тренувати автоенкодер і покращити узагальнення навіть для невідомих прикладів. Оптимізація автокодера та глибоке навчання для запропонованих типів аномалій можуть дати нові ідеї для розробки більш ефективних методів виявлення аномалій. Проте, оскільки пошук гіперпараметрів у глибокому навчанні є складним і потребує великого обсягу даних, цю оптимізацію слід залишити для майбутніх досліджень.

4.4 Висновки

У цьому розділі було розглянуто процес вибору пристрою, здатного виконувати роль контролера IoT-AD, а також визначення його оптимального

розміщення в мережі. Крім того, проведено детальний аналіз безпеки IoT-AD і обговорено обмеження, пов'язані з його дизайном в цілому.

Було здійснено комплексну оцінку моделей з точки зору представлення даних та застосування моделей машинного навчання, а також розглянуто обмеження кожної з моделей. В результаті було створено набір інструментів для впровадження аномалій, генерації ознак та розробки моделей, який доступний для подальшого відтворення.

Далі було продемонстровано, що автоматично згенеровані функції за допомогою автокодера показують значне покращення, особливо коли кодуються часові значення та представлення FFT. Однак агреговане кодування працює добре тільки для аномалії InstaD, і має слабкі результати при використанні гістограмного представлення. Для конкретної техніки, як локальний фактор викидів (LOF), закодовані ознаки виявились непридатними, значно погіршуючи ефективність класифікації в усіх сценаріях.

Для всіх інших моделей машинного навчання, незалежно від того, контрольовані вони чи неконтрольовані, таких як Logistic Regression (LR), SVM, Random Forest, 1-class SVM і Isolation Forest, закодовані функції показали значне покращення за всіма основними метриками: точністю, відгуком та оцінкою F1.

Також було показано, що за рахунок використання всіх функцій та найкращих моделей на основі оцінки F1, контрольовані моделі значно перевершують свої аналоги без нагляду. Наприклад, на аномаліях SuddenD та SuddenR контрольовані моделі показали в середньому на 18% кращі результати (наприклад, encoder+SVM — 77% проти encoder+OC-SVM — 63% з функціями часового значення). Для аномалії SlowD контрольовані моделі перевершують безнаглядні на 2%, а для InstaD — на 2,6%.

Крім того, аналіз показав, що автоматично згенеровані закодовані функції можуть значно покращити оцінку F1 — до 500%, що було продемонстровано на контрольованому випадковому лісі з аномалією InstaD і неконтрольованому ізоляційному лісі з аномалією SlowD.

ВИСНОВКИ

На сьогодні більшість методів виявлення аномалій у середовищі IoT вимагають значної участі людини та часто орієнтовані на оптимізацію для локальних рішень. Теоретично, аномалії можна виявити відносно легко, і фахівець із відповідної галузі зможе помітити аномальні дані, якщо йому буде надано достатньо часу. Проте існують кілька складнощів при розробці автоматизованих моделей для виявлення аномалій в IoT-системах. Це завдання є складним і не завжди можливо правильно визначити та класифікувати всі типи аномальних даних, особливо коли навчальні дані доступні лише частково або взагалі відсутні.

Виявлення аномалій в Інтернеті речей має широкий спектр застосувань, деякі з яких уже розвинені (наприклад, виявлення вторгнень в мережу), а інші мають значний потенціал для розвитку. Література з цієї теми є досить обширною та різноманітною, проте ця область досліджень все ще знаходиться на етапі активного розвитку, і кількість публікацій на цю тему продовжує зростати.

У першому розділі було розглянуто проблему виявлення аномалій або вторгнень в мережі IoT. Спочатку представлено контекст і розглянуто підходи в літературі. Була зосередженість на методах, заснованих на машинному навчанні, які можуть навчатися безпосередньо на основі даних і знаходити важливі функції, не вдаючись до спеціалізованих моделей мережі або спеціалізованих сигнатур.

Потім було вибрано набір даних про мережеву активність з декількома атаками, який регулярно використовується для розробки NIDS і як орієнтир пропозицій. Використовуючи стандартні бібліотеки з відкритим вихідним кодом, було впроваджено та оцінено кілька алгоритмів на основі машинного навчання, продуктивність яких є найсучаснішою. Джерела доступні, а результати легко відтворюються.

У другому розділі представлено дизайн IoT-AD, який використовує механізми для виявлення аномалій на рівні пакетів, пов'язаних із взаємодією між пристроями IoT, підтримки стану пристроїв IoT протягом тривалого часу і, в

кінцевому підсумку, дозволяє пристроям IoT відновлюватися після аномалій, які могли поширюватися серед них.

Було впроваджено прототип IoT-AD, який було оцінено на основі наборів даних пристроїв IoT з відкритим вихідним кодом, а також за допомогою реального розгортання на невеликому тестовому стенді IoT, який реалізований. Додатково було оцінено цей прототип у порівнянні з попередніми відповідними підходами для виявлення аномалій у середовищах IoT. Результати моєї оцінки демонструють, що IoT-AD — це легка структура, яка може виявляти аномалії пристроїв IoT менш ніж за 2,12 мілісекунди (мс) і з точністю до 98%.

У третьому розділі було розглянуто процес вибору пристрою, який може виступати в якості контролера IoT-AD, і розміщення цього контролера. Також надано аналіз безпеки IoT-AD і обговорено обмеження дизайну IoT-AD в цілому.

Крім того, можна було би вибрати пристрій IoT з достатніми ресурсами, щоб застосувати в якості контролера (наприклад, смарт-телевізор, розумний холодильник). Але як правило, будь-який пристрій, що володіє достатніми ресурсами для виявлення аномалій на рівні пакетів і взаємодії (такі вимоги до ресурсів були кількісно визначені в процесі оцінки в розділі V), повинен мати можливість виступати в ролі контролера.

Було розглянуто також різні потенційні сценарії атак, які можуть мати місце в середовищі IoT, і проаналізували здатність IoT-AD пом'якшувати ці сценарії атак. Розподілені атаки типу «відмова в обслуговуванні» (DDoS): через вразливості (такі як слабка аутентифікація або шифрування) пристрої IoT можуть бути скомпрометовані зловмисником і використовуватися як частина ботнету (наприклад, Mirai) для проведення DDoS-атак.

У четвертому розділі було представлено чотири типи аномалій, які можуть бути присутніми в бездротових лініях зв'язку і корисні для виявлення в реальних операційних розгортаннях IoT.

Продемонстровано, що ці аномалії були виявлені під час розгортання IoT в реальному світі, а саме на випробувальному стенді LOG-a-TEC, і вони суттєво вплинули на очікувану роботу тестового стенду.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Лінь Х.-Х. , Є Е.-Х. , Лін П. Виявлення аномалій для систем IoT Енциклопедія бездротових мереж , Springer International Publishing , Cham (2020) , стор . 18-20 ,10.1007/978-3-319-78262-1_183

2. Фахім М. , Сілітті А. Методи виявлення, аналізу та прогнозування аномалій у середовищі IoT: систематичний огляд літератури IEEE Access , 7 (2019) , стор. 81664-81681 ,10.1109/ACCESS.2019.2921912 Переглянути в ScopusGoogle Scholar

3. Кухар А.А. , Mısırlı G. , Fan Z. Виявлення аномалій для даних часових рядів Інтернету речей: опитування IEEE Internet Things J. , 7 (7) (2020) , стор . 6481-6494 ,10.1109/JIOT.2019.2958185 Переглянути в ScopusGoogle Scholar

4. Сікдер, Л. Бабун, Х. Аксу та А. С. Улуагак, "Aegis: контекстно-залежна структура безпеки для систем розумного дому", *CoRR,* том abs/1910.03750. [Електронний ресурс]. В наявності: http://arxiv.org/abs/1910. 03750

5. Choi, H. Jeoung, J. Kim, Y. Ko, W. Jung, H. Kim, and J. Kim, «Виявлення та ідентифікація несправних пристроїв IoT у розумному домі за допомогою контекстного вилучення», у 2020 році 48-а щорічна міжнародна конференція IEEE/IFIP з надійних систем та мереж (DSN), с. 610–621.

6. А. Б. У. А. Бакар, Х. Гайват, С. Ф. Хасанм і С. К. Мухопад-х'яй, «Виявлення активності та аномалій у розумному будинку: опитування». Ф. Каутеруччо, Л. Чінеллі, Е. Коррадіні, Г. Террачіна, Д. Урсіно,

7. Л. Віргілі, К. Савальо, А. Ліотта та Г. Фортіно, «Основа для виявлення та класифікації аномалій у кількох сценаріях IoT», Комп'ютерні системи майбутнього покоління, том 114, с. 322–335, 2021.

8. В. Чжан, Ю. Менг, Ю. Лю, Х. Чжан, Ю. Чжан і Х. Чжу, "Гомоніт: моніторинг додатків розумного дому з зашифрованого трафіку", в матеріалах конференції ACM SIGSAC з безпеки комп'ютерів і комунікацій,. CCS '18. Нью-

Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, с. 1074–1088. [Електронний ресурс].

9. https://doi.org/10.1145/3243734.3243820 “Моніторинг додатків Smart Home за допомогою зашифрованого трафіку”

10. Д. Брайтенбахер, І. Гомоляк, Ю. Л. Аунг, Ю. Еловічі та Н. О. Тіппенхауер, "Hades-iot: практична та ефективна система виявлення аномалій на основі хоста для пристроїв Iot (розширена версія)", *IEEE Internet of Things Journal*, 2021.

11. J. Wang, S. Hao, R. Wen, B. Zhang, L. Zhang, H. Hu та R. Lu, «Йот-претор: виявлення небажаної поведінки для пристроїв IoT», IEEE Internet of Things Journal, том 8, No 2, с. 927–940, 2021.

12. К. Фу, К. Цзен і Х. Ду, "HAWatcher: Semantics-Aware anomaly detection for appified smart homes" на 30-му симпозіумі з безпеки USENIX (USENIX Security 21). Асоціація USENIX, серпень 2021 р., с. 4223–4240. [Електронний ресурс]. Доступно: https://www.usenix.org/conference/ usenixsecurity21/presentation/fu-chenglong

13. Т. ОКОННОР, Р. Мохамед, М. Мієттінен, В. Енк, Б. Рівз, А.-Р. Садегі, "Homesnitch: прозорість поведінки та контроль для розумних домашніх пристроїв IoT", у матеріалах 12-ї конференції з безпеки та конфіденційності в бездротових та мобільних мережах,. WiSec '19. Нью-Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, с. 128–138. [Електронний ресурс]. В наявності: https://doi.org/10.1145/3317549.3323409

14. Р. Трімананда, Д. Вармаркен, А. Маркопулу та Б. Демський, "Пінгпонг: підписи на рівні пакетів для подій пристроїв розумного дому". [Електронний ресурс]. В наявності: https://arxiv.org/abs/1907.11797

15. Л. Ченг, К. Тіан і Д. Д. Яо, "Орфей: Застосування семантики кіберфізичного виконання для захисту від атак, орієнтованих на дані", ser. ACSAC '17. Нью-Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, с. 315–326. [Електронний ресурс]. В наявності: https://doi.org/10. 1145/3134600.3134640

16. К. Сюй, Ф. Ван і Х. Цзя, «Захистіть Інтернет, один дім за раз», том 9, No 16, с. 3821–3832. [Електронний ресурс]. В наявності: https://doi.org/10.1002/sec.1569

17. Ф. Лі, А. Шінде, Ю. Ши, Ж. Є, Х.-Y. Лі та В. Сонг, «Безпека IoT на основі навчання системної статистики: здійсненність та придатність», IEEE Internet of Things Journal, том 6, No 4, с. 6396–6403.

18. Ф. Лі, Ю. Ши, А. Шінде, Д. Є та В. Сонг, «Посилена кіберфізична безпека в Інтернеті речей за допомогою енергетичного аудиту», IEEE Internet of Things Journal, том 6, No 3, с. 5224–5231.

19. П. Мартінс, А. Б. Рейс, П. Сальвадор і С. Сарджento, "Механізми виявлення аномалій фізичного рівня в мережах IoT", на *симпозіумі NOMS 2020-2020 IEEE/IFIP Network Operations and Management*. IEEE, 2020, с. 1–9.

20. Д. Танг, П. Фан і Х. Танг, "Схема спільного виявлення аномалій на основі rssi для бездротових сенсорних мереж",. *Міжнародна конференція з бездротового зв'язку, мереж і мобільного зв'язку*. IEEE, с. 2783–2786.

21. С. Раджендран, В. Мерт, В. Лендерс та С. Поллін, "Saife: Unsupervised wireless spectrum anomaly with interpretable features," на міжнародному симпозіумі IEEE з динамічних мереж доступу до спектру (DySPAN). IEEE, с. 1–9.

22. J. Yin, Q. Yang and J. J. Pan, "Виявлення аномальної людської активності на основі датчиків," IEEE Transactions on Knowledge and Data Engineering, том 20, No 8, с. 1082–1090. В. Р. Яккула та Д. Д. Кук, "Виявлення аномальних подій датчиків у даних розумного дому для покращення життєвого досвіду", в Artificial Intelligence and Smarter Living.

23. С. Рамапатруні, С. Н. Нараянан, С. Міттал, А. Джоші та К. Джоші, "Моделі виявлення аномалій для безпеки розумного будинку", IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) та IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 19–24.

24. Л. Г. Фахад і М. Раджараджан, "Виявлення аномалій у розумному будинку", IEEE 14th International Conference on Machine Learning and Applications (ICMLA), pp. 419–422.

25. Х. Ву, З. Чу, П. Ян, К. Сян, Х. Чжен і В. Хуанг, «Tw- see: Розпізнавання людської активності через стіну за допомогою товарних пристроїв Wi-Fi», IEEE Transactions on Vehicular Technology, том 68, с. 306–319.

26. J. W. Branch, C. Giannella, B. Szymanski, R. Wolff and H. Kargupta, "Виявлення викидів у мережі в бездротових сенсорних мережах", Knowledge and Information Systems, том 34, No 1, с. 23–54.

27. Ф. А. Нарудін, А. Фейзолла, Н. Б. Ануар і А. Гані, "Оцінка класифікаторів машинного навчання для виявлення шкідливого програмного забезпечення на мобільних пристроях", Soft Comput., том 20, No 1, с. 343–357. [Електронний ресурс]. В наявності: https://doi.org/10.1007/s00500-014-1511-6 Н. Дж. Апторп, Д. Ю. Хуанг, Д. Рейсман, А. Нараянан та

28. Н. Феамстер, "Збереження приватності розумного дому за допомогою розумного формування трафіку IoT", CoRR, vol. abs/1812.00955 [Електронний ресурс]. В наявності: http://arxiv.org/abs/1812.00955

29. Г. Гоял, П. Лю та С. Сурал, «Безпека розумних домашніх систем IoT за допомогою контролю доступу на основі атрибутів», у матеріалах семінару ACM 2022 року з безпечних та надійних кіберфізичних систем,. Sat-CPS '22. Нью-Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, 2022, с. 37–46. [Електронний ресурс]. В наявності: https://doi-org.leo.lib.unomaha.edu/10.1145/3510547.3517920

30. М. Ямауті, Ю. Охсіта, М. Мурата, К. Уеда та Ю. Като, «Виявлення аномалій у роботі розумного дому за поведінкою користувачів і домашніми умовами», IEEE Transactions on Consumer Electronics, том 66, No 2, с. 183–192, 2020.

31. Е. Анті, Л. Вільямс, М. Словінська, Г. Теодоракопулос і П. Бурнап, "Контрольована система виявлення вторгнень для розумних домашніх пристроїв IoT", IEEE Internet of Things Journal, том 6, No 5, с. 9042–9053.

32. І. Андреа, К. Хризостому та Г. К. Хаджихристофі, "Інтернет речей: вразливості та виклики безпеки", IEEE Symposium on Computers and Communication (ISCC), с. 180–187.

33. Х. Чі, К. Цзен, Х. Ду та Д. Ю, "Загрози втручання між додатками в розумних будинках: категоризація, виявлення та обробка", CoRR, том abs/1808.02125. [Електронний ресурс]. В наявності: http://arxiv.org/abs/1808. 02125

34. В. Ікбал, Х. Аббас, М. Данешманд, Б. Рауф і Ю. А. Бангаш, «Глибокий аналіз вимог безпеки IoT, викликів та їх протидії за допомогою програмно-визначеної безпеки», IEEE Internet of Things Journal, том 7, No 10, с. 10 250–10 276, 2020. М. Антонакакіс, Т. Ейпріл, М. Бейлі, М. Бернхард, Е. Бурштейн,

35. Ж. Кокран, З. Дурумерік, Ж. А. Гальдерман, Л. Інверніцці, М. Калліціс та ін., "Розуміння ботнету mirai", в 26-й симпозіум з безпеки USENIX (USENIX Security 17) с. 1093–1110.

36. М. Ф. Б. Аббас і Т. Шрікантан, «Виявлення шкідливого програмного забезпечення на основі підписів низької складності для пристроїв IoT», в Applications and Techniques in Information Security, L. Batten, D. S. Kim, X. Zhang, and G. Li, Eds. Singapore: Springer Singapore, pp. 181–189. В. Яссін, Н. І. Удзір, А. Абдулла, М. Т. Абдулла, Х. Зульзаліл та

37. З. Муда, "Виявлення аномалій на основі сигнатур за допомогою інтегрованих класифікаторів інтелектуального аналізу даних", Міжнародний симпозіум з біометрії та технологій безпеки (ISBAST), 2014, с. 232–237.

38. А. Хамза, Х. Х. Гарахейлі, Т. А. Бенсон і В. Сівараман, "Виявлення об'ємних атак на пристрої лотів за допомогою моніторингу активності грязі на основі sdn", у Матеріалах симпозіуму ACM 2019 року з досліджень SDN, ser. SOSR '19. Нью-Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, 2019, с. 36–48. [Електронний ресурс]. В наявності: https://doi.org/10.1145/3314148.3314352

39. Д. Рен, Д. Ж. Дюбуа, Д. Чоффнес, А. М. Мандаларі, Р. Колкун і Х. Хаддаді, "Інформаційний вплив від споживчих пристроїв IoT: багатовимірний, мережево-інформований підхід до вимірювання", в Proceedings of the Internet Measurement Conference, ser. IMC '19. Нью-Йорк, Нью-Йорк, США: Асоціація

обчислювальної техніки, Симпозіум з мереж, комп'ютерів та комунікацій (ISNCC). IEEE, 2016, с. 1–6.

40. Ю. Лі, Ю. Сюй, З. Лю, Х. Хоу, Ю. Чжен, Ю. Сінь, Ю. Чжао та Л. Цуй, «Робастне виявлення для мережевого вторгнення промислового IoT на основі багатоканального синтезу», Вимірювання, том 154, с. 107450, 2020.

41. Г. Біау та Е. Скорнет, "Випадкова екскурсія лісом", TEST, том 25, No 2, с. 197–227.

42. Н. С. Альтман, "Вступ до непараметричної регресії ядра та найближчого сусіда", Американський статистик, том 46, No 3, с. 175-185.

43. Ю.-Ю. Сонг і Л. Ін, "Методи дерева прийняття рішень: застосування для класифікації та прогнозування", Шанхайський архів психіатрії, том 27, No 2, с. 130.

44. Г. Е. Хінтон і Р. Земель, "Автокодери, мінімальна довжина опису і вільна енергія Гельмгольца", Досягнення в нейронних системах обробки інформації, т. 6. Е. Дейхофф, Архітектури нейронних мереж: вступ. Ван Ностранд Рейнхольд Л.

45. Н. Д. Апторп, Д. Рейсман і Н. Фемстер, "Розумний будинок - це не замок: вразливості конфіденційності зашифрованого трафіку IoT", CoRR, том abs/1705.06805. [Електронний ресурс]. В наявності: http://arxiv.org/abs/1705. 06805 А. Акар, Х. Ферейдуні, Т. Абера, А. К. Сікдер, М. М'єттінен,

46. Х. Аксу, М. Конті, А.-Р. Садегі та С. Улуагак, «Peek-a-boo: Я бачу ваші дії розумного дому, навіть зашифровані!» у Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec '20. Нью-Йорк, Нью-Йорк, США: Асоціація обчислювальної техніки, 2020, с. 207–218. [Електронний ресурс]. В наявності: https://doi.org/10.1145/3395351.3399421

47. Н. Апторп, Д. Рейсман та Н. Фемстер, "Закриття жалюзі: чотири стратегії захисту конфіденційності розумного дому від мережевих спостерігачів", препринт arXiv:1705.06809.

48. «Інтернет речей під обстрілами: Kaspersky виявив понад 100 мільйонів атак на розумні пристрої в першому півріччі 2019 року». В

Інтернеті]_https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-Kaspersky виявляє понад 100 мільйонів атак на розумні пристрої за перше півріччя 2019 року.

49. П. Ньюман, "Звіт про IoT: як зростання технології Інтернету речей досягає основних компаній і споживачів", Business Insider, 28-Jan-2019.

50. І. Бутун, С. Д. Моргера та Р. Санкар, "Огляд систем виявлення вторгнень у бездротових сенсорних мережах", IEEE Communications Surveys & Tutorials, 1 (16), 266–282.

51. Р. Доші, Н. Апторп і Н. Фемстер, "Виявлення DDoS-атак з машинним навчанням для споживчих пристроїв Інтернету речей", в: 2018 IEEE Security and Privacy Workshops (SPW), 29–35

52. Ф. Хуссейн, Р. Хуссейн, С. А. Хассан та Е. Хоссейн, "Машинне навчання в безпеці IoT: поточні рішення та майбутні виклики", arXiv [cs. CR], 14 березня 2019 року.

53. П. Шукла, "ML-IDS: підхід машинного навчання для виявлення атак червоточини в Інтернеті речей», в: Конференція інтелектуальних систем (IntelliSys), 234–240

54. J. Cañedo та A. Skjellum, "Використання машинного навчання для захисту систем IoT", In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 219–222

55. Н. Неса, Т. Гош та І. Банерджі, "Підхід навчання на основі непараметричних послідовностей для виявлення викидів в IoT," Future Gener. Обчислень. Сист. (82), 412–421,

56. Е. Вієгас, А. Сантін, Л. Олівейра, А. Франса, Р. Ясінскі та В. Педроні, "Надійна та енергоефективна комбінаційна схема класифікатора для виявлення вторгнень у вбудованих системах", Comput. Безпека., (78), 16–32,

57. Х. Х. Пажух, Р. Джавідан, Р. Хаямі, Д. Алі та К.-К. Р. Чу, "Дворівневе зменшення розмірів і дворівнева модель класифікації для виявлення вторгнень на основі аномалій у магістральних мережах IoT", IEEE Transactions on Emerging Topics in Computing, 2(7), 314 - 323, (2019).

58. М. Таваллаї, Е. Багері, В. Лу та А. А. Горбані, "Детальний аналіз набору даних KDD CUP 99," In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6.

59. М. Рінг, С. Вундерліх, Д. Шерінг, Д. Ландес і А. Хото, "Огляд наборів даних виявлення вторгнень на основі мережі", Comput. Безпека., (86), 147–167.

60. М. Рінг, С. Вундерліх, Д. Грюдль, Д. Ландес та А. Хото, "Набір даних технічного звіту CIDDS-001".

61. Р. Абдулхаммед, М. Фаезіпур, А. Абузнейд та А. АбуМаллух, "Підходи глибокого та машинного навчання для виявлення незбалансованого мережевого трафіку на основі аномалій", IEEE Sensors Letters, 1(3), 1–4, (2019).

62. А. Верма та В. Ранга, "Про оцінку систем виявлення мережевих вторгнень: статистичний аналіз набору даних CIDDS-001 з використанням методів машинного навчання", Pertanika J. Sci. Technol., 3(26), 1307-1322.

63. У. Ветцкер, І. Сплітт, М. Циммерлінг, К. А. Боано та К. Ремер, "Вирішення проблем бездротового співіснування в промисловому Інтернеті речей", IEEE Intl Conference on Computational Science and Engineering (CSE), Париж, Франція.

64. Д. Д. К. Сільва, Дж. Дж. П. Родрігес, К. Салім, С. А. Козлов і Р. А. Рабело, «M4DN. Платформа керування мережами та пристроями IoT-A для Інтернету речей», IEEE Access, том 7, с. 53 305–53 313, квітень 2019 р.

65. А. Шет, К. Дорр, Д. Грюнвальд, Р. Хан і Д. Сікер, "Mojo: Розподілена система виявлення аномалій фізичного рівня для 802.11 wlan", в Матеріалах 4-ї міжнародної конференції з мобільних систем, додатків і послуг. ACM, с. 191–204.

66. С. Гупта, Р. Чжен і А. М. Ченг, "Анди: система виявлення аномалій для бездротових сенсорних мереж", 2007 р. IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 1-9.

67. Х. Аліпур, Ю. Б. Аль-Нашіф, П. Сатам і С. Харіпі, "Виявлення бездротових аномалій на основі аналізу поведінки ieee 802.11", IEEE Transactions on Information Forensics and Security, том 10, No 10, с. 2158–2170.

68. В. Чандола, А. Банерджі та В. Кумар, «Виявлення аномалій: огляд», Обчислювальні опитування ACM (CSUR), том 41, No 3. М. Вучник, Т. Сольц, У. Грегорк, А. Гроват, К. Брегар, М. Смольнікар,

69. М. Мохорчич і К. Фортуна, "Безперервна інтеграція в розвитку бездротових технологій", IEEE Communications Magazine, том 56, No 12, с. 74–81.

70. А. Зимек, Е. Шуберт, Г.-П. Крігель, "Дослідження щодо виявлення неконтрольованих викидів у числових даних високої розмірності", Статистичний аналіз та інтелектуальний аналіз даних: Журнал ASA Data Science, том 5, No 5, с. 363–387.

71. К. К. Аггарвал, "Ансамблі аутсайдерів: позиційний документ", Бюлетень ACM SIGKDD Explorations, том 14, No 2, с. 49–58.

72. М. Гупта, Д. Гао, К. С. Аггарвал і Д. Хан, "Виявлення викидів для тимчасових даних: опитування", IEEE Transactions on Knowledge and Data Engineering, том 26, No 9, с. 2250–2267.

73. Х. Сюй, Х. Лю і М. Яо, «Недавній прогрес у виявленні аномалій», Hindawi Complexity, том 2019, січень 2019.

74. А. Кук, Г. Мисірлі та З. Фан, «Виявлення аномалій для даних часових рядів IoT: опитування», IEEE Internet of Things Journal, том 7, No 7, с. 6481–6494, липень 2020 р.

75. А. Лавін та С. Ахмад, "Оцінка альго- рифм виявлення аномалій у реальному часі – еталон аномалії numenta", 2015 IEEE 14th Міжнародна конференція з машинного навчання та додатків (ICMLA)., с. 38–44.

76. Р. Юрдак, Х. Р. Ван, О. Обст і П. Валенсія, Аномалії мережі бездротових датчиків: діагностика та стратегії виявлення. Берлін, Гейдельберг: Шпрінгер Берлін Гейдельберг, с. 309–325. [Електронний ресурс]. В наявності: https://doi.org/10.1007/978-3-642-17931-0_12

77. Т. Кіеу, Б. Янг, К. Го та К. С. Дженсен, «Виявлення викидів для часових рядів з рекурентними ансамблями автоенкодерів». у матеріалах Двадцять восьмої Міжнародної спільної конференції зі штучного інтелекту (IJCAI-19), Макао, П.Р. Китай, с. 2725–2732.

78. Т. Д. О'Ші, Д. Корган і Т. К. Кленсі, "Навчання без учителя представлення структурованих сигналів радіозв'язку", у 2016 році Перший міжнародний семінар з зондування, обробки та навчання для інтелектуальних машин (SPLINE). IEEE, с. 1–5.

79. Т. Джей О'Ші, Т. Ерпек і Т. К. Кленсі, "Комунікації на основі глибокого навчання mimo", препринт arXiv arXiv:1707.07980.

80. Х. Чжан, К. Лю, К. Шанг, Л. Фенг, К. Чен, З. Ву та С. Го, "Дводіапазонна локалізація в приміщенні на основі Wi-Fi за допомогою стекового деносуючого аутоенкодера", на IEEE Global Communications Conference (GLOBE-COM), Вайколоа, HI, США, США, грудень 2019 р.

81. Б. Ван, Ф. Ху, Ю. Чжао та Т. Н. Го, "Виявлення аномалій та діагностика масивів у бездротових мережах з кількома антенами: рамки, виклики та інструменти," IEEE Network, том 32, No 1, с. 152–159.

82. М. Р. Шахід, Г. Бланк, З. Чжан і Х. Дебар, "Виявлення аномальних комунікацій у мережах IoT за допомогою розріджених автокодерів", на IEEE 18-му Міжнародному симпозіумі з мережевих обчислень і додатків (NCA), Кембридж, США, вересень 2019 р.

83. З. Чен, К. К. Єо, Б. С. Лі та К. Т. Лау, "Виявлення аномалій мережі на основі автоенкодера", на симпозіумі з бездротових телекомунікацій (WTS), Фенікс, Аризона, США.

84. К. Інь, С. Чжан, Д. Ван і Н. Н. Сюн, "Виявлення аномалій на основі згорткового рекурентного автокодера для часових рядів IoT", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020.

85. В. Л. Тінг, "IEEE 802.11 виявлення мережевих аномалій та класифікація атак: підхід глибокого навчання", на конференції IEEE Wireless Communications and Networking Conference (WCNC), Сан-Франциско, Каліфорнія, США.

86. J. Ran, Y. Ji та B. Tang, "Підхід до напівконтрольованого навчання для виявлення мережевих аномалій ieee 802.11", у 2019 році IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, 2019, с. 1–5.

87. О. Салем, А. Герассімов, А. Мехауа, А. Маркус та Б. Фурхт, "Виявлення аномалій у медичних бездротових сенсорних мережах за допомогою svm та лінійних регресійних моделей," Міжнародний журнал електронної охорони здоров'я та медичних комунікацій (IJEHMC), том 5, No 1, с. 20–45.

88. "Виявлення та класифікація несправностей датчиків і аномалій пацієнта в медичних бездротових сенсорних мережах", на міжнародній конференції IEEE зі зв'язку (ICC), Будапешт, Угорщина, червень 2013 р., с. 4373–4378.

89. М. А. Альшейх, С. Лін, Д. Ніято, Х.-П. Тан, "Машинне навчання в бездротових сенсорних мережах: алгоритми, стратегії та програми", IEEE Communications Surveys & Tutorials, том 16, No 4, с.

90. T. Šolc, C. Fortuna та M. Mohorcˇic, "Недорога розробка тестового стенду та її застосування в когнітивному радіопрототипуванні," в Когнітивне радіо та мережі для гетерогенних бездротових мереж. Springer.

ДОДАТОК А

ПЕРЕЛІК НАУКОВИХ ПРАЦЬ

Сертифікат № 2024-110-1

Міністерство освіти і науки України
Хмельницький національний університет

СЕРТИФІКАТ

Войченко Роман Олександрович

учасник XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2024»
24 години участі (0,8 ECTS credits)

Голова оргкомітету АПКН-2024

Олег СИНЮК
проректор Хмельницького національного
університету з наукової роботи,
доктор технічних наук, професор

м. Хмельницький
15-16 листопада 2024

E-mail: apkt.khnu@gmail.com

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2024»

15-16 листопада 2024

Войченко Р.О., Стецюк М.В.

Хмельницький національний університет

ВИЯВЛЕННЯ АНОМАЛІЙ В ІНТЕРНЕТ-ПРИСТРОЯХ

Запропоновано використовувати аналіз часових рядів та статистичні методи для виявлення аномалій у трафіку пристроїв Інтернету речей (IoT). Метою є поєднання різних статистичних підходів для виявлення аномалій на основі нерозмічених даних, а також створення профілів, які відображають ключові характеристики пристроїв. У межах цього підходу розроблено методи виділення ознак нормальної поведінки пристроїв та визначення меж, за які виходять аномальні події, шляхом аналізу трафіку.

It is proposed to use time series analysis and statistical methods to detect anomalies in the traffic of Internet of Things (IoT) devices. The goal is to combine different statistical approaches to detect anomalies based on unlabeled data and create profiles that reflect key device characteristics. Within this approach, methods for identifying signs of normal device behavior and determining the limits beyond which abnormal events occur, by means of traffic analysis, have been developed.

Технології Інтернету речей обмінюються даними без участі людини. IoT стає все більш популярним у сфері оптимізації операцій, і до 2030 року кількість таких пристроїв досягне 50 мільярдів. Інновації в IoT покращують інтелектуальні додатки, зокрема в інфраструктурі міст, охороні здоров'я, транспорті та освіті.

Розширене впровадження IoT створило нові виклики для безпеки [1, 2]. Пристрої IoT, зазвичай підключені через бездротові мережі, вразливі до атак, що може призвести до серйозних наслідків [6]. Захист IoT є складним завданням через різнорідність архітектур, численні вразливості та інтеграцію нестандартних рішень.

Запропонований підхід до виявлення аномалій у трафіку IoT складається з трьох етапів: вилучення ознак, оцінка нормальної поведінки та виявлення аномалій. На етапі вилучення ознак формується вектор характеристик для кожного пристрою чи користувача шляхом агрегації часових рядів. Ці ознаки включають такі параметри, як частота повідомлень, кількість входів, повторювані повідомлення, інтервали між ними та кількість помилок. Наступний етап – оцінка нормальної поведінки, де розраховується нормальний діапазон значень для кожної ознаки, щоб створити межі нормальної поведінки пристроїв.

Для визначення нормальних діапазонів використовуються статистичні методи: інтерквантильний розмах, критерій Граббса, GESD-тест і експоненціальне згладжування. Межі нормальної поведінки для кожної ознаки обчислюються за формулою (1):

$$ND(f) = [Q1(f) - scale * iqr, Q3(f) + scale * iqr] \quad (1)$$

де *scale*=1,5 використовується для визначення незначних відхилень, а scale=3— для значних викидів. GESD-тест застосовується для ідентифікації одного або кількох викидів у наборі даних, що дозволяє виявити аномальні значення, які не відповідають звичайній активності.

На заключному етапі методика виявлення аномалій перевіряє активність кожного пристрою на наявність значних відхилень від визначених нормальних діапазонів. Для цього етапу використовуються розраховані раніше межі нормальної поведінки ознак та особливості пристроїв. Процес виявлення аномалій включає кілька кроків: порівняння значень ознак із нормальними діапазонами, визначення атрибутів аномалій, таких як час і інтенсивність, фільтрацію незначних відхилень і розрахунок підсумкових значень, що дає змогу оцінити кількість аномалій для кожного пристрою [3].

Для оцінки запропонованого підходу до виявлення аномалій у трафіку пристроїв було використано механізм генерації журналів, заснований на розподілах вихідних атрибутів пристрою, таких як часові мітки, підключення пристрою, мережеві адреси, помилки тощо [4]. Під час генерації до журналу додавалися аномалії для кожної з ознак для випадково вибраних пристроїв із заданою ймовірністю, після чого отримана розмітка порівнювалася з результатами виявлення аномалій у згенерованому журналі.

На основі вхідних даних визначалося частотне розподілення повідомлень з пристроїв, і на його основі генерувалися ідентифікатор пристрою та його профіль, що містив усі можливі значення атрибутів для даного пристрою. Згодом, у процесі генерації аномальної активності, певні атрибути пристрою змінювалися з заданою ймовірністю та додавалися до згенерованого журналу. Для формування залежних та незалежних атрибутів використовувався коефіцієнт кореляції Спірмена: залежні атрибути (наприклад, версія програмного забезпечення, ідентифікатор користувача) генерувалися на основі їхніх розподілів щодо поточного пристрою, а незалежні (наприклад, адреси мережевих шлюзів, IP-адреси) — на основі загального розподілу атрибута або інших атрибутів журналу. Загальна схема підходу до генерації журналу активності пристроїв представлена на рисунку 1.

Загальна схема підходу до генерації журналу активності пристроїв представлена на рисунку 1. Спершу обирається пристрій з загального переліку відповідно до початкового розподілу частоти входів. Далі визначається час підключення пристрою в обраному часовому інтервалі з невеликим випадковим відхиленням. Потім для пристрою встановлюється набір атрибутів, таких як спроби входу, мережеві адреси, помилки тощо, з урахуванням того, чи є ці атрибути специфічними для даного пристрою [5]. На завершення генеруються необхідні атрибути для кожного пристрою, що додаються до журналу активності.

Для генерації журналу активності пристроїв виконуються такі кроки: обирається пристрій відповідно до частоти його підключень, визначається час підключення з невеликим випадковим відхиленням, встановлюється набір атрибутів (спроби входу, мережеві адреси, помилки) з урахуванням їх специфічності для

пристрою, і генеруються потрібні атрибути. Ці дії повторюються до досягнення потрібної кількості записів, а в кінці дані сортуються за часом.

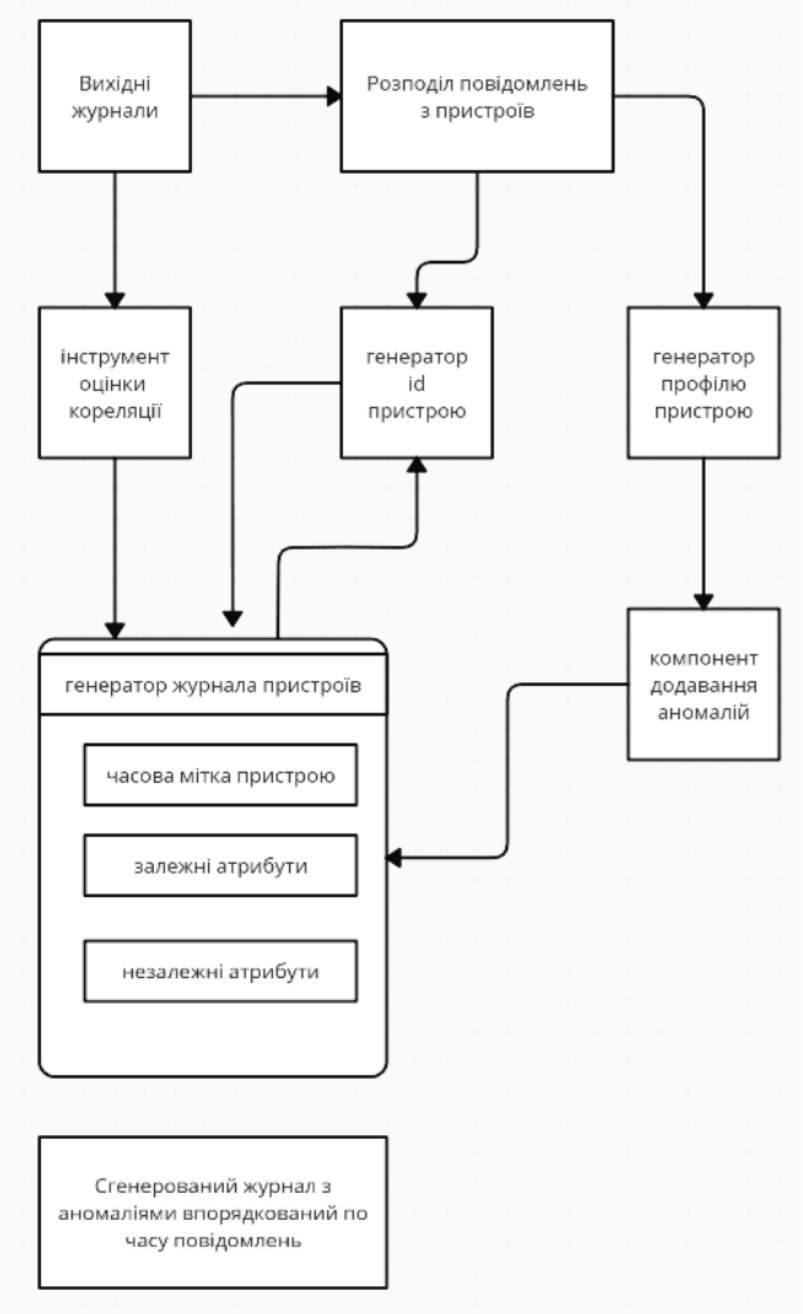

Рисунок 1 – Загальна схема генерації журналу активності пристроїв

Генерований журнал використовується для створення ознак пристроїв, визначення значень, які відповідають нормальній поведінці, та виявлення різних

аномалій., де точність виявлення визначається як відношення кількості знайдених аномалій до загальної кількості аномалій для кожної ознаки.

Найкраще визначаються аномалії, пов'язані зі зміною часових інтервалів між повідомленнями, тоді як найменш помітними були аномалії, пов'язані з кількістю повторюваних повідомлень. Це, ймовірно, пов'язано з незначними змінами частоти повідомлень під час генерації, які могли вписатися в межі нормальних значень. Для цієї ознаки може знадобитися більш чутливе налаштування методів визначення меж нормальної поведінки.

. Описано методики аналізу трафіку IoT-пристроїв, ознаки для виявлення аномалій, механізм генерації журналів подій, а також числову оцінку виявлених аномалій у згенерованому журналі з використанням запропонованого підходу.

У дослідженні використовувалися різні статистичні методи для виявлення аномалій у трафіку IoT-пристроїв, які відзначаються гнучкістю, універсальністю, швидкістю обчислень та здатністю працювати з нерозміченими даними. До недоліків підходу можна віднести відсутність оцінки запропонованих методик на основі розмічених даних з аномаліями.

Подальше вдосконалення підходу передбачає аналіз більшої кількості ознак і порівняння ефективності запропонованих методів з методами, що базуються на машинному навчанні.

Перелік посилань

1. Іваненко, П.В. Виявлення аномалій у системах Інтернету речей: Навчальний посібник. / П.В. Іваненко. — Київ: Державний університет телекомунікацій, 2021. — 312 с.
2. Сидоренко, О.М. Безпека Інтернету речей. / О.М. Сидоренко. — Харків: ХНУРЕ, 2020. — 278 с.
3. Петренко, Л.О. Вступ до IoT та аналіз аномалій: Підхід на основі статистичних методів. / Л.О. Петренко. — Львів: Видавництво Львівської політехніки, 2019. — 345 с.
4. Мартинюк, Д.В. Статистичні методи виявлення аномалій у IoT: Практичний посібник. / Д.В. Мартинюк. — Одеса: ОНПУ, 2022. — 256 с.
5. Корнійчук, І.С. Введення до машинного навчання для IoT: Навчальний посібник. / І.С. Корнійчук. — Суми: Сумський державний університет, 2021. — 204 с.
6. Павленко, Т.М. Основи обробки даних для виявлення аномалій в IoT. / Т.М. Павленко. — Київ: Університет ім. Т. Шевченка, 2018. — 189 с.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Войченка Романа Олександровича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а) та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11.12.24
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT

Автор: Войченко Роман Олександрович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма:Кібербезпека та захист інформації

Науковий керівник: кандт. техн. наук, доцент Кльоц Юрій Павлович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 80.5%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені модифікації стосуються математичних формул і не є порушенням академічної доброчесності.

Керівник роботи _____ Юрій КЛЬОЦ

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Роман Войченко

Співавтор:

Назва: Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT

Експерт: Микола Стецюк

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:19.5%

Коефіцієнт подібності 2:5%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-19 09:47:08.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2024-12-19 Старший викладач Сергій Мостовий

Дата експерт

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 157198 Назва: Метод виявлення аномальної поведінки пристроїв у безпровідних мережах IoT Додано в БД: 2024-12-10 Автора: Войченко Роман Керівники: Стецюк М.В. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	96496	699	600 (1%)	7 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Войченко Роман Олександрович

Тема Метод виявлення аномальної поведінки пристроїв у безпроводових мережах IoT

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Обсяг кваліфікаційної роботи освітнього ступеня «магістр»:

кількість листів креслень - ; кількість сторінок записки 75

1. Кваліфікаційна робота присвячена спрямована на виявлення аномалій поведінки пристроїв у безпроводових мережах IoT. Здійснено глибокий аналіз існуючих методів і моделей, запропоновано новий підхід до виявлення аномалій в безпроводних мережах.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У роботі використано сучасні методи та досягнення в області безпроводових мереж IoT. У першому розділі проведено аналіз фону алгоритму виявлення аномалій. Другий розділ присвячено розробці фреймворку IOT-AD для виявлення аномалій серед взаємопов'язаних пристроїв IOT. У наступних розділах реалізовано метод виявлення аномальної поведінки. Проведено дослідження аномалій у безпроводових лінія зв'язку.

4. Позитивні сторони роботи Позитивні сторони проекту Робота добре структурована, чітко висвітлені всі етапи дослідження. Використані сучасні інструменти та підходи, що свідчить про якість проведеного дослідження..

5. Негативні сторони роботи Негативним аспектом цієї роботи є те, що не до кінця розкрито питання ефективності та масштабованості запропонованих методів виявлення аномальної поведінки в реальних умовах IoT-мереж

6. Оцінка графічного оформлення та пояснювальної записки роботи В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно»
.

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович
завідувач кафедри АКІТР, доктор технічних наук, професор

« 17 » грудня 2024. (підпис)