НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇН
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

В.о. завідувача кафедри

_____ Лариса ГЛОБА

«___»_____2021 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Метод виявлення вторгнень в мережу Інтернету речей за допомогою нейромережі»

Виконав:
студент IV курсу, групи ТІ-72
Гіззатуллін Данило Денисович _____

Керівник:
асистент кафедри ІТМ ІТС,
Курдеча Василь Васильович _____

Рецензент:
Зав. кафедри промислової електроніки ФЕЛ проф., д.т.н.,
Ямненко Юлія Сергіївна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ

В.о.завідувача кафедри

_____ Лариса ГЛОБА

«___»_____2021 р.

ЗАВДАННЯ

на дипломну роботу студенту

Гіззатуллін Данило Денисович

1. Тема роботи «**Метод виявлення вторгнень в мережу Інтернету речей за допомогою нейромережі**», керівник роботи асистент кафедри інформаційно-телекомунікаційних мереж ІТС Курдеча Василь Васильович, затверджені наказом по університету від «14» квітня 2021 р. № 1007-с

2. Термін подання студентом роботи 7 червня 2021 р.

3. Вихідні дані до роботи наукові статті про технології Інтернету Речей.

4. Зміст роботи

1. Провести аналіз проблем безпеки мереж Інтернету речей.
2. Проаналізувати існуючі методи виявлення вторгнень в мережу Інтернету речей та вибрати прототип
3. Вдосконалити метод за рахунок впровадження процесу донавчання.
4. Провести натурне моделювання та аналітичну оцінку запропонованого рішення

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

1. Титульний слайд
2. Актуальність
3. Мета
4. Задачі
5. Аналіз методів виявлення вторгнень
6. Вибір методу за прототип
7. Недоліки прототипу
8. Запропонований метод
9. Результати натурного моделювання
10. Результати натурного моделювання
11. Результат аналітичної оцінки
12. Загальні висновки
13. Публікації на тему

6. Дата видачі завдання 24 жовтня 2020 року_____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз проблеми безпеки мереж Інтернету речей	06.10.2020 – 16. 11. 2020	Виконано
2	Аналіз сучасних рішень виявлення вторгнень в мережі	17.11.2020 – 27.12.2020	Виконано
2	Порівняння методів виявлення вторгнень в мережу	27.12.2020 - 06.02.2021	Виконано
4	Проведення моделювання запропонованого методу	07.02.2021 – 05.03.2021	Виконано
5	Написання наукової статті (ПРІТС-2021) та виступ	06.03.2021 – 14.04.2021	Виконано
6	Аналіз результатів запропонованого методу	15.04.2021 – 11.05.2021	Виконано
7	Оформлення дипломної роботи	13.05.2021 – 07.06.20201	Виконано

Студент Данило ГІЗЗАТУЛЛІН

Керівник Василь КУРДЕЧА

РЕФЕРАТ

Робота містить 63 сторінки, 14 рисунків, 4 таблиці. Було використано 40 джерел.

Актуальність: актуальність дослідження полягає в тому, що кількість пристроїв в мережі IoT постійно збільшується. Разом з цим збільшується кількість рішень на ринку IoT технологій, що в купі призводить до росту потенційних вразливостей цих мереж. Тим самим збільшується кількість ресурсів, що витрачається на забезпечення безпеки.

Чим більше інтернет речей впроваджується в обіг у різних галузях людського життя, тим більш привабливою для зловмисників стає ідея атак цих мереж, що призводить до збільшення і ускладнення атак. Такий стан речей призводить до ускладнення засобів забезпечення безпеки, що в свою чергу призводить до збільшеня витратів ресурсів на забезпечення безпеки IoT систем.

Мета роботи: зменшити кількість ресурсів, що витрачаються на забезпечення захисту інформації в мережі інтернету речей за рахунок удосконалення нейромережевого імунного методу виявлення вторгнень за допомогою введення процесу донавчання.

Запропонований метод дозволить зменшити кількість обчислень, потрібних для забезпечення задовільного рівня безпеки.

Ключові слова: інтернет речей, мережева безпека, нейронна мережа, uplearning, штучна імунна система, виявлення вторгнень

ABSTRACT

The work contains 63 pages, 14 figures, and 4 tables. 40 sources were used.

Topicality: The relevance of the research is in the fact that the number of devices in the Internet network is constantly increasing. At the same time, the number of solutions in the market of IT technologies is increasing, which in turn leads to an increase in the potential variability of these networks. This increases the amount of resources spent on security.

The more Internet solutions are introduced into circulation in different areas of human life, the more attractive the idea of attacking these networks becomes for the perpetrators, leading to an increase and complication of attacks. This state of affairs leads to the deterioration of security equipment, which in turn leads to increased costs of resources for security of IT systems.

The goal of the work: to reduce the amount of resources spent on information security in the Internet of Things through the improvement of the neuromereger immune method of intrusion detection through the introduction of a donation process.

The proposed method will reduce the number of calculations required to ensure the required safety level.

Keywords: Internet of Things, network security, neural network, uplearning, artificial immune system, intrusion detection

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	Internet of Things
DDoS	Distributed Denial of System
IDS	Intrusion Detection System
IPS	Intrusion PreventingSystem
СВВ	Система Виявлення Вторгнень
СВА	Система Виявлення Аномалій
ШНМ	Штучна Нейронна Мережа
RNN	Recurrent Neural Networks
TCP	Transmission Control Protocol
IP	Internet Protocol
QoS	Quality of service

BPNN	Backpropagation Neuralnetwork
LSTM	Long short-term memory
GRU	Gated Recurrent Units

ВСТУП

Актуальність. актуальність дослідження полягає в тому, що кількість пристроїв в мережі IoT постійно збільшується. Разом з цим збільшується кількість рішень на ринку IoT технологій, що в купі призводить до росту потенційних вразливостей цих мереж. Тим самим збільшується кількість ресурсів, що витрачається на забезпечення безпеки.

Мета й завдання дослідження:

Метою роботи є зменшення кількості ресурсів, що витрачаються на забезпечення захисту інформації в мережі інтернету речей за рахунок удосконалення нейромережевого імунного методу виявлення вторгнень за допомогою введення процесу донавчання.

Для досягнення мети дослідження було поставлено та вирішено такі основні задачі:

1. Провести аналіз проблем безпеки мереж Інтернету речей.
2. Проаналізувати існуючі методи виявлення вторгнень в мережу Інтернету речей та вибрати прототип
3. Удосконалити метод за рахунок впровадження процесу донавчання.
4. Провести натурне моделювання та аналітичну оцінку запропонованого рішення

Об’єкт роботи: процес захисту інформації в мережі Інтернету речей

Предмет дослідження: нейромережевий імунний метод виявлення вторгнення

Теоретичний результат дослідження: Запропонований модифікований нейромережевий імунний метод виявлення вторгнення.

Практичний результат роботи: Розроблене програмне забезпечення, яке може використовуватися в комплексі технологій мережі інтернету речей, для підвищення ресурсоефективності захисту інформації.

Публікації

1. Гіззатуллін Д. Д. Аналіз вразливостей мережі IoT // XV Міжнародна Науково-технічна Конференція "Проблеми телекомунікацій 2021"
2. Гіззатуллін Д. Д. Метод виявлення вторгнень в мережі IoT. // XV Міжнародна Науково-технічна Конференція студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем-2021"

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ МЕРЕЖ IOT. АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ

1.1 Огляд проблеми безпеки мереж інтернету речей

Технологія інтернету речей уже давно увійшла у фазу активного впровадження у використання, наслідком чого є стрімке зростання IoT пристроїв, яких станом на 2021 рік нараховується уже близько 35 мільйонів, присутніх майже у всіх сферах людської діяльності.

Безпека систем IoT є серйозною проблемою через зростаючого числа сервісів і користувачів в мережах IoT. Інтеграція систем Інтернету речей та інтелектуальних середовищ робить інтелектуальні об'єкти більш ефективними. Однак вплив вразливостей безпеки Інтернету речей дуже небезпечний в критично важливих інтелектуальних середовищах, що використовуються в таких областях, як медицина і промисловість. В інтелектуальних середовищах на основі Інтернету речей без надійних систем безпеки додатки і сервіси будуть схильні до ризику. Приватна власність, цілісність і доступність - три важливих концепції безпеки додатків і сервісів в інтелектуальних середовищах на основі Інтернету речей; таким чином, щоб вирішити ці проблеми, інформаційна безпека в системах IoT вимагає досліджень [27].

Проблеми безпеки в системах IoT виникають на різних рівнях IoT. Фізичні пошкодження, відмова обладнання і обмеження потужності - це проблеми, з якими стикаються на фізичному рівні. DoS-атаки, сніффінг, міжмережеві атаки і несанкціонований доступ - це проблеми, пов'язані з мережевого рівня. Атаки шкідливого коду, вразливості додатків і програмні помилки - це проблеми, з якими стикаються на рівні додатків [28].

Згідно [29], пов'язані з безпекою проблеми будь-якої системи IoT можна розділити на чотири типи: аутентифікація і фізичні погрози, ризики конфіденційності, проблеми цілісності даних і проблеми конфіденційності.

Проблема, пов'язана з аутентифікацією, і фізичні погрози - це перші проблеми, які впливають на систему IoT. Рівень сприйняття включає в себе безліч пристроїв IoT, таких як датчики, які залежать від своїх власних систем безпеки; таким чином, вони уразливі для фізичних атак.

Пов'язані з конфіденційністю ризики виникають між пристроями IoT і шлюзами на мережевому рівні. Обмеженість ресурсів низькорівневими пристроями в системах IoT створює непряму проблему щодо конфіденційності передачі даних в мережах IoT [30].

Третій клас проблем безпеки стосується цілісності даних між сервісами та додатками. Проблеми цілісності даних виникають, коли атаки підробки або шум впливають на систему IoT. DoS, DDoS і пробні атаки - це довільні атаки, які можуть завдати шкоди додатків і службам Інтернету речей.

Проблеми четвертого типу пов'язані з конфіденційністю. Конфіденційність інформації - важливий аспект безпеки в системах Інтернету речей [31]. У різних компонентах Інтернету речей використовуються різні типи технологій ідентифікації об'єктів; таким чином, кожен об'єкт має свій власний ідентифікаційний тег, який несе особисту інформацію, інформацію про місцезнаходження і переміщення. Управління та моніторинг програм і сервісів в системі IoT означає створення ризику для конфіденційності інформації; наприклад, використання системи, заснованої на методі глибокої перевірки пакетів для довірених операцій в системі IoT, вважається порушенням конфіденційності інформації [32]. Будь який несанкціонований доступ до

системи управління загрожує конфіденційності інформації користувачів Інтернету речей [29].

Наслідком великого розповсюдження IoT систем являється велика різноманітність пристроїв, операційних систем, протоколів, систем авторизації, аутентифікації, програм і сервісів, які реалізують певні технології IoT у вирішенні тієї чи іншої проблеми.

Кожна нова технологія являє собою потенційне джерело вразливостей, які можуть виникати внаслідок недоліків технології або помилок розробників. Деякі такі вразливості можуть існувати десятиріччями перед тим як їх буде виявлено.

Наприклад в 2020 році було виявлено набір вразливостей, названий Ripple20 [1], який існував з 1997 року в популярній бібліотеці TCP / IP стеку фірми Treck. Ці вразливості дозволяли виконувати злонамірений код на цільовому пристрою. Після виявлення було скомпрометовано велику кількість пристроїв, так як стек Treck поставлявся на ринок більше 20 років. Хоча в наступному оновлені ці вразливості були усунені але, так як підготовка оновлень прошивок для конкретних пристроїв може затягнутися або неможлива, багато пристроїв залишилися без супроводу так як їх проблематично оновити.

Інтелектуальне середовище, що об'єднує технологію IoT, вважається складною системою, тому що вона складається з різних продуктів від різних компаній, заснованих на різних технологіях, які не мають універсальної мови. Отже, стандартизація - ще один важливий аспект безпеки в системах Інтернету речей. Створення стандартної архітектури IoT, заснованої на одній стандартній технології для всіх постачальників і виробників, підвищить функціональну сумісність функцій безпеки всіх об'єктів і датчиків в системі IoT. Успіх цієї інтеграції залежатиме від співпраці між компаніями для створення універсального стандарту. Така стандартизація значно спростить безпеку мережі IoT

Найнебезпечнішими вразливостями IoT систем являються вразливості нульового дня. Це така вразливість яка уже виявлена, але ще немає вирішення для її ліквідації, або оновлення ще не готове або не встановлене на пристрої. Кіберзлочинці можуть скористатись цим розривом між виявленням і ліквідацією вразливості, наприклад для передачі на пристрій викупного вірусу [17], який блокує пристрій за допомогою шифрування, доступ до якого можна відновити лише після оплати викупу. Частіше усього IoT мережі розглядаються злочинцями як джерело DDoS атак. І на відміну від вхідної DDoS атаки, вихідну замасковану атаку визначити не так просто.

Одиничне успішне проникнення в один або кілька кінцевих пристроїв може поставити під загрозу безпеку всієї системи IoT і завдати шкоди її додатків і службам, особливо з промислової точки зору [33]. Таким чином, реалізація надійного механізму безпеки в системі IoT залежить від рівня безпеки окремих пристроїв IoT, який, в свою чергу, залежить від чинників потужності та пам'яті. Отже, вважається, що обмеження потужності і пам'яті створюють непрямі проблеми безпеки в системах Інтернету речей. Для вирішення цих проблем потрібні полегшені рішення безпеки і полегшені методи шифрування і дешифрування. Ці рішення і методи повинні бути застосовані в різних доменах IoT і повинні задовольняти вимогам безпеки, не впливаючи на QoS.

У той же час IoT-пристрої можуть не тільки зберігати у себе дані в незашифрованому вигляді, але також передавати їх по мережі. Якщо передачу даних у відкритому вигляді по локальній мережі можна хоч якось пояснити, то в разі бездротової мережі або передачі через інтернет вони можуть стати надбанням кого завгодно.

Сам користувач може використовувати безпечні канали зв'язку для передачі даних, але шифруванням збережених паролів, біометричних та інших важливих даних повинен потурбуватися виробник пристроїв.

Ще однією вагомою проблемою є проблема використання небезпечних або застралих, програмних компонентів або бібліотек, які можуть дозволити скомпрометувати пристрій. Це включає небезпечне налаштування платформ операційної системи і використання сторонніх програмних або апаратних компонентів з скомпрометованого ланцюжка поставок.

Відсутність безпечних механізмів оновлення пристрою. Це включає в себе відсутність валідації прошивки на пристрої, відсутність безпечної доставки (без шифрування при передачі), відсутність механізмів запобігання відкату і відсутність повідомлень про зміни безпеки через оновлень. Відсутність можливості оновлення пристрою саме по собі є слабким місцем безпеки. Неможливість встановити оновлення означає, що пристрої протягом невизначеного часу залишаються уразливими.

Але крім того, саме оновлення і прошивка також можуть бути небезпечними. Наприклад, якщо для отримання ПЗ не використовуються зашифровані канали, файл оновлення не зашифрований або не підтверджена на цілісність перед установкою, відсутня антіоткатная захист (захист від повернення до попередньої, більш вразливою версії) або відсутні повідомлення про зміни безпеки через оновлень.

Також все більше ресурсів виділяється на забезпечення безпеки IoT мереж. Наймається багато спеціалізованого персоналу, купуються ліцензії на програмне і апаратне забезпечення, використовується певна кількість електроенергії.

Попри те що концепція IoT затверджується як сформована, активно впроваджується у використання і стає все більш популярною серед споживачів, розвиток в області стандартизації протоколів, архітектури та додатків продовжується, що призводить до створення великої кількості пропрієтарних рішень і реалізацій певних компонентів.

Присутність такої великої кількості існуючих, і потенційних вразливостей в мережах IoT, призводить до того що просто неможливо попередити і закрити всі ці вразливості. Таким чином постала потреба в засобах виявлення злонаміреного втручання в систему IoT. Такі засоби допоможуть виявити як і втручання зловмисника в роботу системи так і місце і спосіб цього втручання, для подальшої ліквідації цієї вразливості. Таким чином безпека систем IoT повинна забезпечуватися на кожному рівні технології IoT, починаючі від антивірусних програм закінчуючи системами мережевого моніторингу.

Одним із рівнів забезпечення безпеки є мережевий рівень. Засоби безпеки мережевого рівня мають відслідковувати функціонування мережі, і забезпечувати захист її ресурсів. При вирішенні завдань, пов'язаних з діагностикою та захистом мережевих ресурсів, центральним питанням є оперативне виявлення станів мережі, що призводять до втрати повної або часткової її працездатності, знищення, перекручення чи витоку інформації, що є наслідком відмов, збоїв випадкового характеру або результатом отримання зловмисником несанкціонованого доступу до мережевих ресурсів, проникнення мережевих черв'яків, вірусів і інших погроз інформаційної безпеки. Раннє виявлення таких станів дозволить своєчасно усунути їх причину, а також попередить можливі катастрофічні наслідки.

Для їх виявлення використовується великий спектр спеціалізованих систем. Так, при вирішенні проблем діагностики мереж застосовуються засоби систем управління, аналізатори мережевих протоколів, системи тестування навантаження, системи моніторингу мережі. Проблеми захисту інформаційних ресурсів мереж вирішуються за допомогою міжмережевих екранів (firewall), антивірусів, систем виявлення вторгнень(СВВ) (Intrusion Detection System, IDS), систем контролю цілісності, криптографічних засобів захисту.

Систему виявлення вторгнень можна порівняти з охоронною сигналізацією: якщо хтось намагається незаконно проникнути в будинок, один з датчиків виявить це, що призведе до спрацьовування сигналізації і оповіщення власника будинку і поліції. Аналогічно, якщо хтось спробує порушити конфіденційність, цілісність або доступність комп'ютерної мережі, або спробує зламати засоби захисту, система виявлення вторгнення сповістить власника системи і службу безпеки [23].

Виявлення вторгнень — це процес моніторингу та аналізу подій в комп'ютерній системі або мережі ти пошук вторгнення. Такі події, як спроба проникнення в систему з Інтернету за допомогою програмних експлойтів або спроба отримати більш високі привілеї в системі, є показовими подіями, які будуть розпізнані як вторгнення. Високочутливі системи, які повинні бути захищені від атак "0 дня", або критичні системи з високою доступністю, які не можна часто виправляти, є типовими системами що потребують IDS.

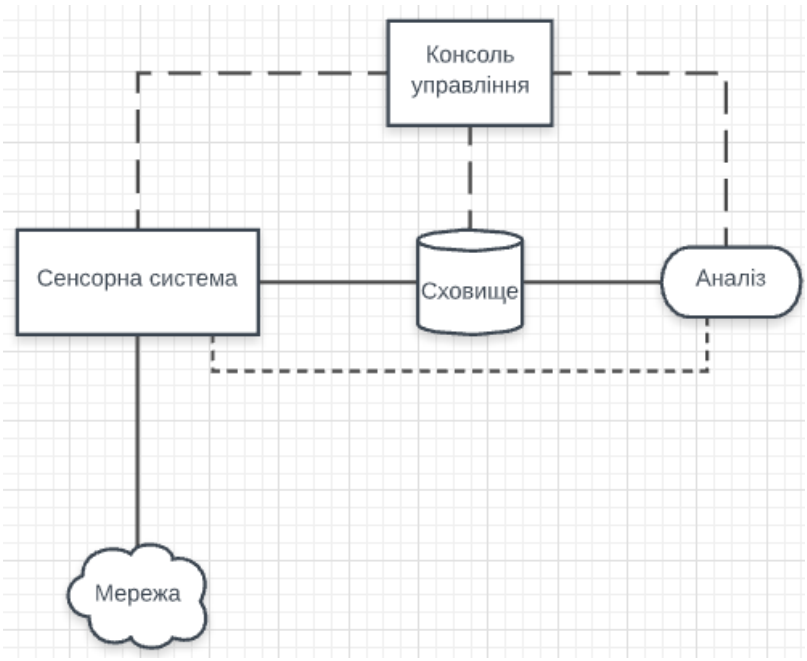

Рис. 1.1 Загальна схема системи виявлення вторгнень

Важливо розуміти, що мета IDS — якомога швидше виявити атаку і попередити потрібних людей, які потім можуть вжити відповідних заходів, якщо система була скомпрометована; іноді IDS може використовувати і автоматичні заходи, для блокування злонаміреної дії. Такі системи називаються IPS (Intrusion Prevention System, IPS).

Системи виявлення вторгнень націлені на виявлення атак на комп'ютерні системи і мережі або на інформаційні системи в цілому, оскільки важко забезпечити доказово захищені інформаційні системи і підтримувати їх в такому безпечному стані протягом всього терміну експлуатації і для кожного використання. Іноді застарілі або операційні обмеження взагалі не дозволяють реалізувати повністю захищену інформаційну систему.

Отже, завдання систем виявлення вторгнень — здійснювати контроль за використанням таких систем і виявляти появу небезпечних станів. Вони виявляють спроби і активне неправомірне використання законними користувачами інформаційних систем або зовнішніми сторонами для зловживання своїми привілеями або використання вразливостей безпеки.

1.2 Аналіз сучасних методів виявлення вторгнень

Сучасні СВВ базуються на двох основних підходах, щодо виявлення вторгнення.

У першому підході виявлення, колекція відомих методів вторгнення зберігається в базі знань, а вторгнення виявляються шляхом пошуку в базі знань тих же методів, або признаків разом з набором вручну встановлених семантичних правил, на базі яких виноситься рішення про наявність втручання.

Інший підхід, а саме виявлення аномалій, заснований на припущенні, що атака на комп'ютерну систему буде помітно відрізнятися

від нормальної діяльності системи, а порушник буде демонструвати поведінку, відмінну від поведінки звичайного користувача або пристрою.

На даний момент дослідження в цій області ведуться великими закордонними комерційними компаніями. Загальний підхід, який лежить в основі цих досліджень, полягає в пошуку методів аналізу, що дозволяють виявляти аномальні стану інформаційних ресурсів у вигляді відхилень від звичайного («нормального») стану.

Ці відхилення можуть бути результатами збоїв в роботі апаратного і програмного забезпечення, а також наслідками мережевих атак хакерів. Такий підхід теоретично дозволить виявляти як відомі, так і нові типи проблем. Від ефективності і точності апарату, що визначає «нормальний» стан і фіксує відхилення, залежить в цілому ефективність вирішення питань діагностики та захисту мережевих ресурсів. Особливу важливість на поточний момент становить проблема виявлення аномальних станів в роботі мережі, що мають розподілений у часі характер. Розподілені в часі аномалії можуть бути наслідками спеціально маскуються мережевих атак зловмисників, прихованих апаратно-програмних збоїв, нових вірусів і т. д.

Якщо зловмисник має можливість фізичного втручання в роботу пристрою N [18, 19] (наприклад вимкненя), то пристроєм M може бути зареєстрована аномалія у вигляді недоступності пристрою N. Основним впливом є інформаційний вплив, який спрямований на інформаційний потік між пристроями N і M. Якщо пристроєм N ведеться моніторинг активності мережі, зокрема, активність мережевого спілкування пристроєм M, то базові атаки типу Man-in-the-middle або replay також приведуть до утворення аномалій, які зловмисник не в змозі приховати [20].

Кожна з наведених вище дій тим чи іншим чином впливає на характеристики мережі системи IoT.

Для вирішення завдання виявлення аномалії в першу чергу необхідно визначити сукупність тих характеристик, які будуть аналізуватися механізмом виявлення аномалій (тобто визначити метрики).

Дані метрики розрізняються залежно від досліджуваної аномалії [21]. Частіше всього виділяють наступні метрики:

--кількість вхідних / вихідних пакетів за одиницю часу;

--кількість втрачених пакетів / помилок за одиницю часу;

--потужність вихідного сигналу;

--споживання електроенергії за одиницю часу.

Таким чином виходячи з визначених метрик можливо класифікувати атаки за характером внесеної аномалії.

Таблиця 1.1

Таблиця опису і характеристик мережевих втручань

Тип аномалії	Опис	Характеристики
Альфа аномалія	Незвично високий рівень трафіку типу точка-точка	Викид в поданні трафіку байти / с, пакети / с по одному домінуючому потоку джерело - призначення. Невелика тривалість(до 10 хвилин)
DDoS атака	Розподілена атака типу відмова в обслуговуванні на одну жертву	Викид в поданні трафіку пакети / с, потоки / с, від множини джерел з одного адресою призначення

Продовження таблиці 1.1

Перегрузка	Незвично високий попит на один мережевий ресурс або сервіс	Стрибок в трафіку по потокам / с з одного домінуючого IP-адресою і домінуючому портом. Зазвичай короткочасна аномалія
Сканування мережі/портів	Сканування мережі за певними відкритим портам або сканування одного хоста по всіх портах з метою пошуку вразливостей	Стрибок в трафіку по потокам / с, з кількома пакетами в потоках від одного домінуючого IP-адреси
Мережеві черви	Шкідлива програма, яка самостійно поширюється по мережі і використовує вразливості операційних систем	Викид в трафіку без домінуючої адреси призначення, але завжди з одним або декількома домінуютьські портами призначення
Точка мультиточка	Поширення контенту від одного сервера багатьом користувачам	Викид в пакетах, байтах від домінуючого джерела до кількох призначень, всі до одного добре відомому порту

Продовження таблиці 1.1

Відключення	Мережеві неполадки, які викликають падіння в трафіку між однією парою джерело-призначення	Падіння в трафіку по пакетам і байтам зазвичай до нуля. Може бути довготривалим і включати всі потоки джерело-призначення від вузла до одного маршрутизатора
Перемикання потоку	Незвичайне перемикання потоків трафіку з одного вхідного маршрутизатора на інший	Падіння в байтах або пакетах в одному потоці трафіку і викид в другому. Може зачепити кілька потоків трафіку

У таблиці 1.1 представлені основні типи мережевих аномалій, їх опис та основні характеристики. Наведена систематизація даних про атаки і етапах їх реалізації дає необхідний базис для розуміння технологій виявлення атак.

Заходи та методи, за допомогою яких в виявляються аномалії, включають в себе наступні атрибути:

порогове значення. Спостереження за об'єктом виражаються у вигляді числових інтервалів. Вихід за межі цих інтервалів вважається аномальним поведінкою. Як можна побачити параметром можуть бути, наприклад, кількість файлів, до яких звертався користувач в даний період часу, число невдалих спроб входу в систему, завантаження центрального процесора і так далі. Порогові значення можуть бути статичними і динамічними (тобто змінюватися, підлаштовуючись під конкретну систему);

статистичні заходи. Рішення про наявність атаки робиться по великій кількості зібраних даних шляхом їх статистичної обробки;

параметричні заходи. Для виявлення атак будується спеціальний профіль нормальної системи на основі шаблонів.;

непараметричні заходи. Тут уже профіль будується на основі спостереження за об'єктом в період навчання; на основі правил (сигнатур). Вони дуже схожі ха непараметричні статистичні заходи. В період навчання складається уявлення про нормальну поведінку об'єкта, яка записується у вигляді спеціальних «правил». Отримуються сигнатури «хорошої» поведінки об'єкта;

інші заходи. Нейронні мережі, генетичні алгоритми, дозволяють класифікувати деякий набір видимих сенсора-датчику ознак.

Базуючись на представлених підходах, створено цілу низку методі виявлення вторгнень, які використовуються в СВВ.

Сигнатурні методи

Сигнатурні методи дають можливість окреслити атаку набором правил або за допомогою формальної моделі, в якості якої може застосовуватись символьний рядок, семантичний вираз спеціальною мовою і так далі. Суть даного методу полягає у використанні спеціалізованої бази даних шаблонів (сигнатур) атак для пошуку дій, що підпадають під визначення "атака"[7]. Сигнатурний метод може захистити від вірусної або хакерської атаки, коли вже відома сигнатура атаки (наприклад, незмінний фрагмент тіла вірусу) і вона внесена в базу даних СВВ. Тобто, коли мережа переживає перший напад ззовні, перше зараження відбувається ще невідомим вірусом, і в базі просто відсутня сигнатура для його пошуку, СВВ не може сигналізувати про небезпеку, оскільки вважатиме атакуючу діяльність легітимною.

Таким чином, ефективність роботи сигнатурної СВА визначається трьома основними факторами: оперативністю поповнення сигнатурної бази, її повнотою з точки зору визначення сигнатур атак, а також наявністю інтелектуальних алгоритмів відомості дій атакуючих до деяких базовим крокам, в рамках яких відбувається порівняння з сигнатурами.

Ускладнюють вирішення завдання про визначення вторгнення факторами являються:

-важкість обліку послідовності подій, що змушує ввести додаткові перевірки даних, що визначають їх послідовність;

-необхідність хорошого адміністратора системи, який міг би налаштувати її відповідно до своїх знань про безпеку системи;

- можуть бути виявлені тільки повністю відомі вразливості;

Статистичні методи

Недолік сигнатурних методів виявлення мережевих атак, пов'язаний з нездатністю системи виявляти атаки невідомих типів, може бути усунутий застосуванням методів заснованих на виявлення аномалій мережевої активності. Такі методи засновані на припущенні, що для обчислювальної системи існує свій профіль нормального стану і будь-які значні відхилення від нього є ймовірним кандидатом на можливу атаку. Основна перевага такого методу — можливість виявлення нових, невідомих раніше атак.

Для побудови базового профілю системи використовується набір даних, вільний від аномалій, або статистичні методи.

Як клас статистичний аналіз відноситься до поведінкових методів визначення порушень в мережі і заснований на зіставленні поточного стану мережевої інфраструктури з якимись певними заздалегідь ознаками, що характеризують штатний функціонування мережевої інфраструктури.

Статистичні датчики збирають різну інформацію про типову поведінку об'єкта і формують її у вигляді профілю. Профіль в даному випадку — це набір параметрів, що характеризують типову поведінку об'єкта. Існує період початкового формування профілю. Профіль формується на основі статистики об'єкта, і для цього можуть застосовуватися стандартні методи математичної статистики, наприклад метод ковзних вікон і метод зважених сум.

Після того як профіль сформований, дії об'єкта порівнюються з відповідними параметрами і при виявленні істотних відхилень подається сигнал про початку атаки.

У контексті аналізу трафіку передбачається, що причинами аномалій трафіку є суттєва зміна деяких характеристик трафіку. Однак якість результатів виявлення залежить не тільки від обраного методу виявлення змін. Ще більш важливим є вибір показників розглянутого трафіку, які найбільш чутливі до подій, що мають відношення до операції і адміністрування мережі, такі, як мережеві збої, атаки шкідливого трафіку.

Системи, які застосовують статистичні методи, мають цілу низку переваг. Вони не вимагають постійного оновлення бази сигнатур атак, що значно полегшує завдання супроводу даних систем. Можуть виявляти невідомі атаки, сигнатури для яких ще не написані.

Серед недоліків систем виявлення вторгнень можна відзначити труднощі завдання порогового значення (вибір цих значень — нетривіальне завдання, яке вимагає глибоких знань контрольованої системи). Зловмисник може обдурити систему виявлення атак, і вона сприйме діяльність відповідної атаки, в якості нормальної через поступової зміни режиму роботи з плином часу і «приручення» системи до нової поведінки. У статистичних методах ймовірність отримання хибних повідомлень про атаку є набагато вищою, ніж при інших методах.

Data Mining методи

Основна ідея таких методів розпізнавання вторгнень в мережу заснована на припущенні про те, що активність користувачів і програм в системі може бути відстежено і побудована її математична модель, яка враховує весь можливий спектр взаємозв'язків в поведінці мережі.

Традиційні методи аналізу даних (статистичні методи) в основному орієнтовані на перевірку заздалегідь сформульованих гіпотез (verification-driven data mining) і на «грубий» розвідувальний аналіз, що становить основу оперативної аналітичної обробки даних (OnLine Analytical Processing, OLAP), в той час як одне з основних положень Data Mining — пошук неочевидних закономірностей. Інструменти Data Mining можуть знаходити такі закономірності самостійно і також самостійно будувати гіпотези про взаємозв'язки.

Основна ідея цих методів стосовно СВВ заснована на припущенні про те, що активність користувачів і програм в системі може бути відстежено і побудована її математична модель[8]. Для прикладного застосування в СВВ методи виявлення аномалій можна розглянути з двух позицій: методи виявлення порушень (misuse detection), які будують модель атаки, а в процесі виявлення використовують методи класифікації, і методи виявлення аномалій (anomaly detection), які будують модель нормальної активності, а в процесі виявлення використовують методи пошуку винятків.

До основних недоліків цієї групи методів можна віднести наступні:

- більшість підходів для проектування ШНМ є наближеними і часто не призводять до однозначних рішень;

- для побудови моделі об'єкта на основі ШНМ слід дотримуватися багатоциклової настройки внутрішніх елементів і зв'язків між ними;

- проблеми, що виникають при підготовці навчальної вибірки, пов'язані з труднощами знаходження достатньої кількості навчальних прикладів;

- більшість відомих комерційних продуктів схемотехнічної реалізації нейронних мереж, виконуються у вигляді надвеликих інтегральних схем (НВІС), які сьогодні важко назвати широкодоступними.

Нейромережеві методи

Серед Data Mining методів розпізнавання, можна виділити широкий клас методів, що заслуговує окремого розгляду, - нейромережеві методи. В їх основі лежать нейронні мережі - обчислювальні моделі, принцип функціонування яких схожий з мережами біологічних нейронів головного мозку. Завдяки запозиченню принципів організації біологічних структур мозку нейромережі демонструють багато їх властивості, такі, як навчання на основі попереднього досвіду, витяг істотних властивостей з інформації, що надходить, узагальнення наявних прецедентів на нові випадки. Можливості, що надаються нейронними мережами, були використані для вирішення завдань розпізнавання і класифікації образів в безлічі досліджень та прикладних розробок.

Підхід інтелектуального аналізу даних — це засіб здобуття знань з великої кількості даних. Витягнуті знання визначаються як цікаві зразки в даних. Такий шаблон може описувати поведінку даних від користувачів або мереж в обчислювальному середовищі. Можливість автоматичного створення моделей, що залежать від опису трафіку, є одним з переваг підходу інтелектуального аналізу даних. Більш того, цей підхід може застосовуватися в узагальнених IDS і в будь-який обчислювальної середовищі. Підхід інтелектуального аналізу даних ідеально підходить для необмеженого, безперервного і швидко зростаючого в обсязі онлайн-потоку даних . Процедура, що складається з стадії навчання правилам,

стадії кластеризації, стадії класифікації та стадії регресії, застосовується при розробці IDS на основі цього підходу.

Методи, засновані на машинному навчанні, спочатку навчають моделі виявлення на основі зібраних вибірок даних в мережах IoT. Потім навчені моделі використовуються для класифікації нових вхідних вибірок даних IoT на звичайні дані або дані для атаки.

Штучна нейронна мережа є математичною моделлю, побудовану за прикладом біологічних нейронних мереж. За рахунок з'єднання щодо простих алгоритмів разом і побудови оптимальної зв'язку між ними технологія дозволяє виявляти складну залежність між вхідними параметрами, навіть якщо вони спочатку були відсутні в навчальній вибірці. Це дозволяє алгоритму залишатися гнучким при вирішенні різного типу завдань.

Для побудови шаблону поведінки користувача можуть використовуватися такі параметри, як час, коли він зазвичай працює, набір вузлів, з яких він починає робочу сесію, характеристики використання ресурсів системи і так далі[9]. Ці параметри оцифровуються і служать входом в нейронну мережу зворотного поширення помилки (backpropagation neuralnetwork, BPNN), а виходом є коефіцієнт, що дорівнює нулю для користувача з нормальною поведінкою і дорівнює одиниці - з аномальним. Іншими словами, мережа тренується на парах типу («нормальні» параметри, 0) і («аномальні» параметри, 1).

Оскільки для отримання «ненормального» поведінки треба було б змусити користувача поводитися не так, як він звик, то аномальні дані генеруються випадково, що ускладнює інтерпретацію результатів щодо роботи на реальних даних.

Серед Data Mining методів розпізнавання, можна виділити широкий клас методів, що заслуговує окремого розгляду, - нейромережеві методи. В їх основі лежать нейронні мережі - обчислювальні моделі, принцип

функціонування яких схожий з мережами біологічних нейронів головного мозку. Завдяки запозичинню принципів організації біологічних структур мозку нейромережі демонструють багато їх властивості, такі, як навчання на основі попереднього досвіду, витяг істотних властивостей з інформації, що надходить, узагальнення наявних прецедентів на нові випадки. Можливості, що надаються нейронними мережами, були використані для вирішення завдань розпізнавання і класифікації образів в безлічі досліджень та прикладних розробок.

Штучна нейронна мережа є математичною моделлю, побудовану за прикладом біологічних нейронних мереж. За рахунок з'єднання щодо простих алгоритмів разом і побудови оптимальної зв'язку між ними технологія дозволяє виявляти складну залежність між вхідними параметрами, навіть якщо вони спочатку були відсутні в навчальній вибірці. Це дозволяє алгоритму залишатися гнучким при вирішенні різного типу завдань.

Оскільки для отримання «ненормального» поведінки треба було б змусити користувача поводитися не так, як він звик, то аномальні дані генеруються випадково, що ускладнює інтерпретацію результатів щодо роботи на реальних даних.

Із недоліків:

- навчання мережі в ряді випадків призводить до тупикових ситуацій;

- тривалі часові витрати на виконання процедури навчання часто не дозволяють застосовувати ШНМ в системах реального часу;

- поведінка навченої ШНМ не завжди може бути однозначно передбачувано, що збільшує ризик застосування ШНМ для управління дорогими технічними об'єктами;

Нейромережеві імунні методи

Ідея створення штучних імунних систем з'явилася в результаті вивчення процесів біологічного імунітету, який захищає організм від хвороботворних бактерій і вірусів, виявляючи і знищуючи їх ..

Біологічна імунна система являє собою складну адаптивну структуру, що складається з різних органів і компонентів, яка для захисту біологічного організму від зовнішніх бактерій і вірусів використовує різноманітні імунні механізми, такі, як виробництво імунокомпетентних клітин; їх навчання та відбір; виявлення шкідливих бактерій і вірусів; знищення виявлених вірусів; механізми адаптації, механізми імунної пам'яті і так далі. Основною метою імунної системи є розпізнавання чужорідних клітин і бактерій в організмі і знищення їх. Імунна реакція полягає в стимуляції різних механізмів при виявленні шкідливих бактерій, спрямованих на їх знищення. Слід зазначити, що імунна система здатна розпізнавати не тільки вже відомі їй бактерії і віруси, а й також невідомі, які раніше не зустрічаються [22].

В результаті проведеного аналізу біологічної імунної системи був зроблений висновок, що дана система є надійним механізмом виявлення аномалій у вигляді хвороботворних бактерій і вірусів. Така система характеризується здатністю до класифікації об'єктів різного класу, а також наявністю механізмів боротьби з виявленими інфекціями. Завдяки своїм особливостям і характеристикам, імунна система представляє великий інтерес в області обробки масивів даних і захисту інформації.

Перераховані характеристики і можливості доводять перспективність використання основних концепцій імунітету у вирішенні складних комп'ютерних завдань, таких, наприклад, як задач забезпечення інформаційної безпеки.

Слабкою стороною таких методів є значно більше використання обчислювальних ресурсів, відносно інших методів.

Таблиця 1.2

Порівняльна таблиця методів виявлення вторгнень

Метод	Точність	Помилки першого роду	Невідомі атаки	Використання обчислювального ресурсу	Складність розгортання	Складність обслуговування
Сигнатурні	10	ні	ні	Низьке	Низька	Висока
Патерні	10	ні	ні	Низьке	Низька	Висока
Модель орієнтовані	10	ні	ні	Низьке	Висока	Висока
Статистичні	7	так	так	Низьке	Висока	Низька
Data Mining	7-9	так	так	Високе	Низька	Низька
Нейромережеві	7-9	так	так	Дуже високе	Низька	Низька
Нейромережеві імунні	9-10	так	так	Дуже високе	Низька	Низька

1.3 Вибір прототипу на основі існуючих рішень. Огляд застосування нейромережевого імунного методу за основу прототипу

Як можна побачити в таблиці 1.2, методи, засновані на виявленні аномалій, мають ключову перевагу над іншими методами — здатність виявляти невідомі атаки. Така перевага вважається ключовою, так як вона вирішує ряд проблем безпеки в системах IoT, а саме проблему вразливостей нульового дня, і розподілених в часі атак.

Перший підхід потребує оперативного ручного внесення спеціалістами правил і признаків до бази даних, що може виконуватись як оновлення програмного забезпечення, що в свою чергу потребує певного

часу. І це тільки у випадку якщо вразливість була знайдена і описана. Саме тому популярності набули системи що базуються або на методах виявлення аномалій, або на гібридних методах першої і другої груп методів.

Через проблеми безпеки, з якими стикаються системи IoT, методи, які можуть упреждающе виявляти нові атаки, найбільш підходять для захисту мереж IoT. Таким чином, потрібна надійна IDS, яка може виявляти нові атаки в інтелектуальних середовищах на основі Інтернету речей.

Серед цієї групи методів найбільшу точність виявлення досягає група нейромережевих імунних методів [24][25][26], яка сягає 99%. В той же час ці методи пропонують низьку ймовірність хибного спрацювання, близько 2%.

Платою за таку гибкість і ефективність нейромережевих імунних методів є їх значно більше використання обчислювального ресурсу, ніж у всіх інших. Обчислювальна складність методу виявлення аномалії — ключовий аспект. У той час як методи класифікації, кластеризації та статистичні методи володіють великим часом для навчання, тестування, як правило, дешеве. Часто це прийнятно, так як моделі можуть навчатися до реального використання, в той час як функціонування потрібне в режимі реального часу. Навпаки, методи «найближчого сусіда», інформаціоннотеоретіческіе і спектральні методи, у яких немає навчальної фази, мають дорога фаза тестування, яка може бути обмеженням в реальному режимі.

Методи виявлення аномалії зазвичай припускають, що аномалії в даних рідкісні в порівнянні з нормальними екземплярами. Хоча аномалії не завжди рідкісні. Наприклад, при контакті з виявленням хробака в комп'ютерних мережах аномальний (черв'як) трафік фактично частіший, ніж нормальний трафік.

Є кілька перспективних напрямків для подальших досліджень в області виявлення аномалій. Так, наприклад, починають знаходити все більше застосування в ряді областей методи виявлення контекстних і колективних аномалій. Наявність розподілених даних спонукало до розвитку і дослідження методів виявлення розподілених аномалій [6].

Також методи, засновані на машинному навчанні, добре працюють тільки при важливому припущенні, а саме: розподіл навчальних і даних що прогнозуються схожі [10]. Тим не менш, у багатьох практичних додатках це припущення не завжди вірно [11], [12]. Зокрема, в мережевої безпеки щодня виявляються нові типи атак (наприклад, атаки нулевого дня) [10].

Таким чином, практичні дані IoT для моделей машинного навчання (на етапі прогнозування / онлайн) зазвичай сильно відрізняються від даних, які використовуються на етапі навчання / оффлайн.

Щоб вирішити цю проблему, часто потрібен великий обсяг навчальних даних з мітками від безлічі IoT-пристроїв. Однак ручна маркування величезного обсягу даних забирає багато часу і коштує дорого [14], [15]. Таким чином, це обмежує практичне застосування методів машинного навчання для виявлення IoT-атак в різних сценаріях.

Проте, щоб навчити ефективну модель машинного навчання виявлення атак IoT, зазвичай потрібно додати тег величезний обсяг навчальних даних як нормальний або атакуючий [15]. Більш того, загальні моделі машинного навчання часто повинні припускати, що розподіл даних навчальних наборів даних аналогічно розподілу даних прогнозних наборів даних. Це припущення, проте, як правило, не працює [11], [12], [15].

Таким чином існує певний розрив між теоретичною, тестовою і практичною здатністю виявляти аномалію. Це призводить до значно більшої, ніж очікувалось, аномальності трафіку[10-14], що в свою чергу

збільшує кількість обчислень спрямованих на обробку аномалії, і визначення чи є вона злонаміреною.

Розглянемо детальніше нейромережевий імунний метод. IS-IDS імітує імунну систему, імітуючи функціональність KCs, DCs вродженої імунної системи і Т-клітин, В-клітин адаптивної імунної системи.

Штучна нейромережева імунна система складається з двох шарів. Перший рівень IDS імітує вроджену імунну систему і називається "Виявлення аномалій на основі статистичного моделювання" (SMAD). Потім другий рівень, адаптивне виявлення аномалій на основі імунітету (AIAD), імітує адаптивну імунну систему. Перший рівень SMAD складається з двох модулів. Модуль попередньої обробки I працює за аналогією з КС, оскільки він відповідає за виявлення зовнішніх вторгнень. Він намагається перехопити зовнішній трафік, щоб визначити його вразливість з перших рук.

Якщо трафік, який пройшов через модуль попередньої обробки-I, виявляється вразливим, то він потрапляє в модуль попередньої обробки-II, інакше трафік є нормальним і проходить через внутрішню мережу організації. Модуль попередньої обробки-II працює подібно DC-клітинам, які можуть ініціювати імунні реакції, активуючи наївні Т-клітини для подальших адаптивних реакцій. Модуль Preprocessing-II визначає трафік в порядку уразливості для системи, який можна вважати а) нормальним б) найменш підозрілим в) помірно підозрілим і г) сильно підозрілим, і направляє найбільш підозрілий трафік до адаптивної імунної системи.

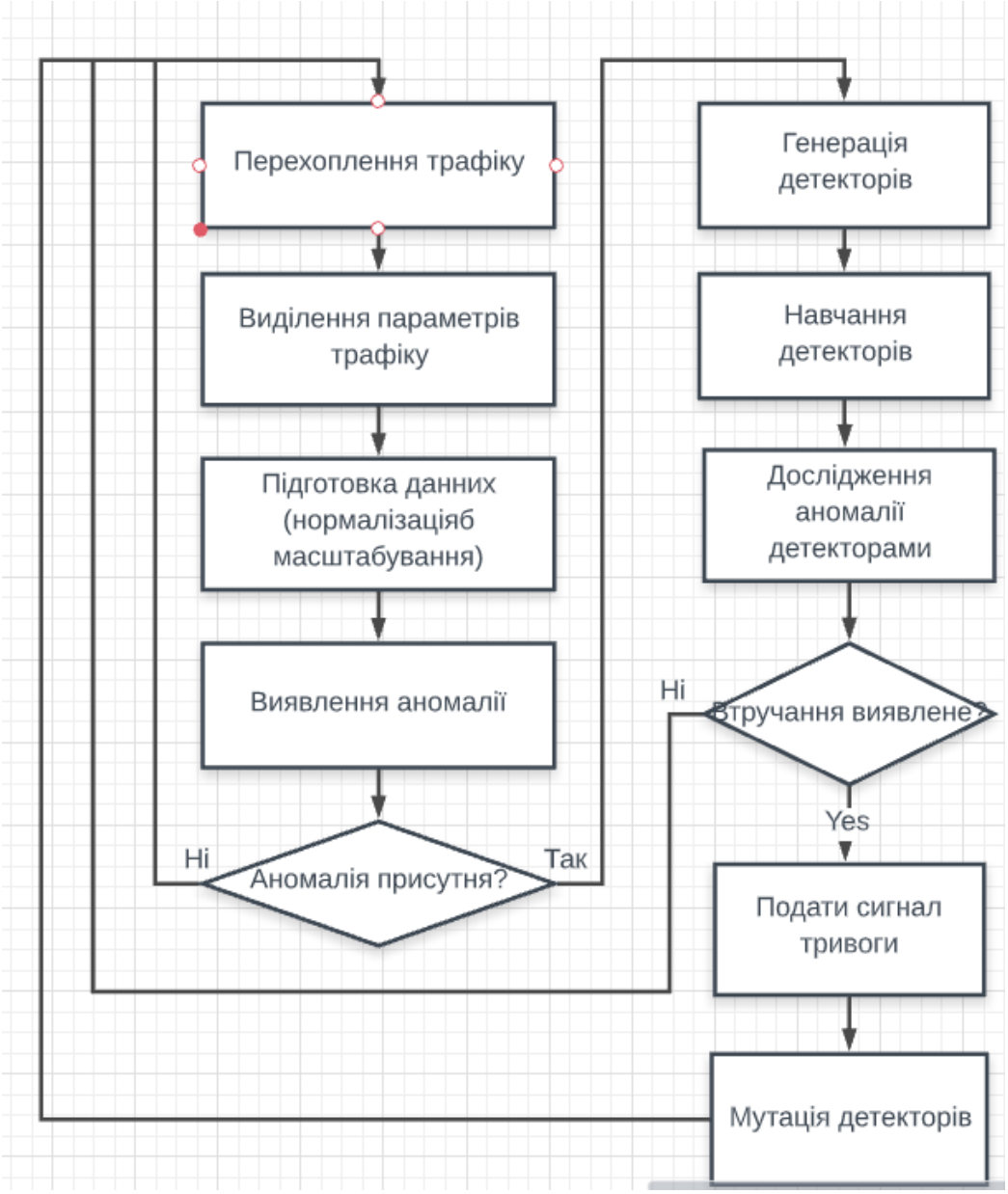

Рис. 1.2 Блоксхема нейромережевого імунного методу виявлення вторгнень в мережу

Таким чином в класичному варіанті метод зводиться до наступних кроків:

Крок 1. Сенсорна система отримує трафік з мережевих сенсорів.

Крок 2. З отриманого трафіку виділяються його параметри.

Крок 3. Отриманий набір даних формується в вектор даних, які нормалізуються, і масштабуються.

Крок 4. Вектор подається на обробку першої нейромережі.

Крок 5. Якщо нейромережа приймає рішення про те, що у вхідному векторі відсутні ознаки аномальності, то система повертається до кроку 1. В іншому випадку перехід на наступний крок.

Крок 6. Генерується набір детекторів з різними параметрами та структурами.

Крок 7. Детектори навчаються на розпізнавання окремих ознак мережевих атак.

Крок 8. Вектор вхідних даних досліджується детекторами.

Крок 9. Якщо признаки втручання не виявлено, система переходе на крок 11.

Крок 12. Подається сигнал тривоги.

Крок 13. Детектори мутують, вбираючи в себе інформацію про виявлене втручання. Перехід на крок 1.

Висновки:

1) Розглянуто проблеми безпеки технології інтернету речей. Проведений огляд допоміг визначати проблеми присутні в мережі Інтернету речей.
2) Проаналізовано сучасні методи виявлення вторгнення в мережу. Даний порівняльний аналіз допоміг виявити слабкі і сильні сторони різних методів, та обрати прототип для запропонованого методу
3) Проведено обґрунтування вибору методу як прототипу. Визначено детально слабкі сторони обраного методу. Детально розглянуто обраний метод.

РОЗДІЛ 2
ВДОСКОНАЛЕНИЙ МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖУ ЗА РАХУНОК ВПРОВАДЖЕННЯ МЕХАНІЗМУ UPLEARNING В НЕЙРОМЕРЕЖУ ВИЯВЛЕННЯ АНОМАЛІЙ

2.1 Метод застосування IS-IDS в мережах IoT

На етапі збору даних і вилучення ознак складається список GFlows, який є входом для модуля IDS. Для ефективного виявлення потоки GFlows обробляються в порядку "останній в першому" (LIFO) (рис. 4.4). Іншими словами, ми починаємо з аналізу останнього захопленого GFlow, щоб швидко виявити загрозу і отримати уявлення про те, що відбувається в реальному часі. В кінцевому підсумку будуть проаналізовані всі GF-потоки, але з поняттям пріоритету для самих останніх повідомлень. Обробка всіх GF-потоків важлива для того, щоб мати повне відстеження стану пристроїв в часі. Після кожного аналізу GFlow стан "NORMAL", "UNKNOWN THREAT" або точний тип загрози відправляється в хмару в форматі Json. Повідомлення містить ідентифікатор пристрою, ідентифікатор повідомлення, тимчасову мітку GFlow, стан, а також опис, якщо необхідно.

Хмара отримує повідомлення про стан від різних пристроїв, як показано на рисунку 2.2, і відображає, завдяки Codex Data Platform IoT, огляд пристроїв в нашій IoT-системі, їх поточний стан, а також історію зміни їх стану. Вся ця інформація зберігається в хмарі з двох основних причин. По-перше, тому що ми знаходимося в умовах обмежених ресурсів пристроїв, тому ми не хочемо їх перевантажувати. По-друге, щоб запобігти їх крадіжку або видалення в разі, якщо пристрій буде заражено або вимкнено.

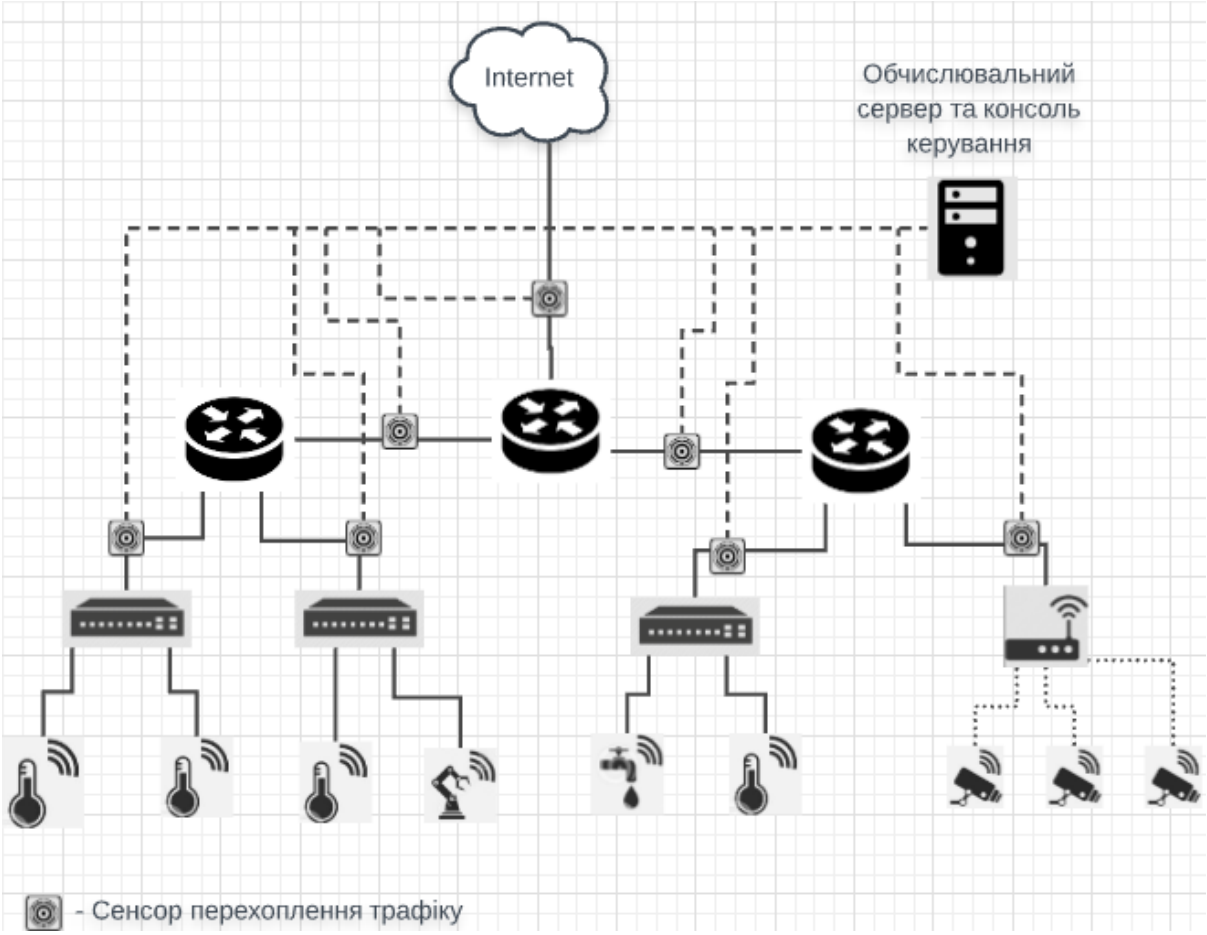

Рис. 2.1 Класична схема побудови СВВ в мережі

Модуль IDS побудований на архітектурі "туман-речі", де ми розміщуємо інтелектуальну і обчислювальну логіку поруч з датчиками даних. Концепція туманних обчислень була вперше представлена компанією Cisco [Cis12] для розширення хмарних обчислень на мережевому рівні.

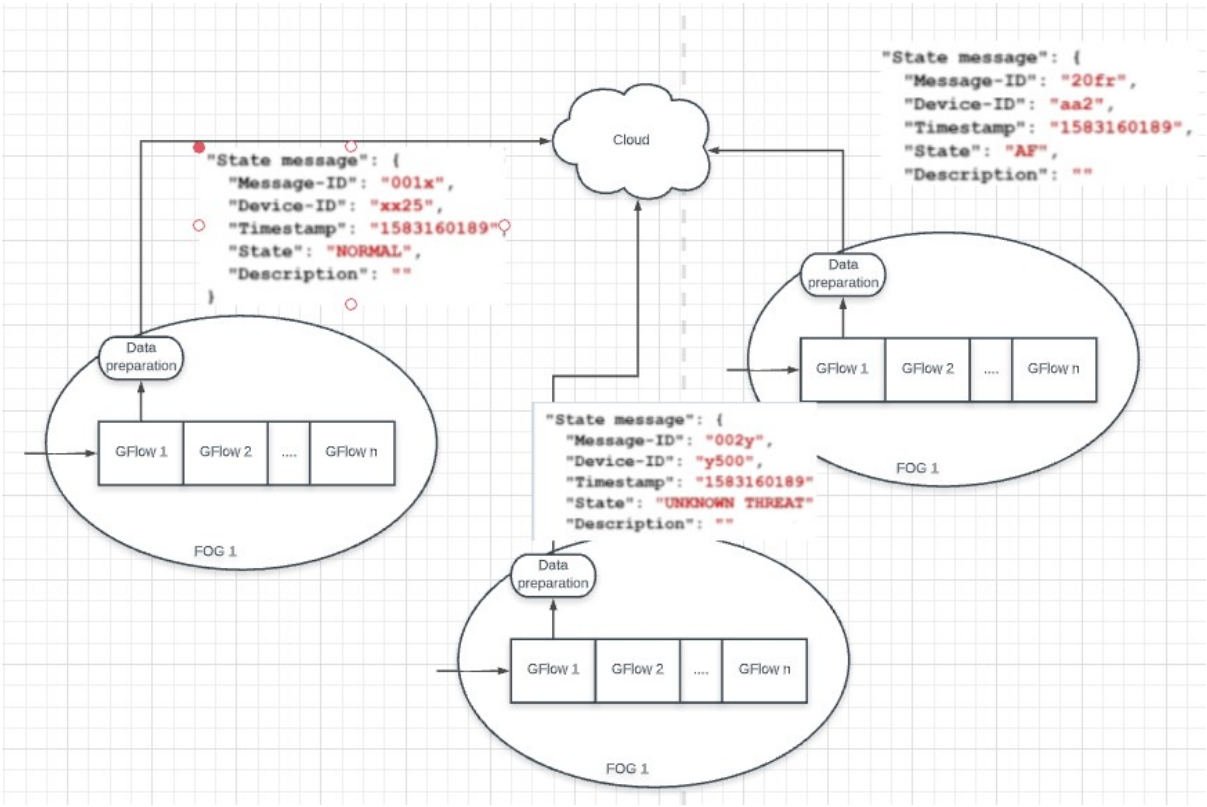

Рис. 2.2 Приклад функціонування передачі повідомлень від туманних вузлів до хмари

Туманний рівень знаходиться між датчиками IoT і хмарою. Туманні обчислення розміщують інтелектуальну обробку і обчислювальну потужність на рівні локальної мережі в мережевій архітектурі, тобто в концентраторах, маршрутизаторах або шлюзах (вузлах туману).

Отже, побудова нашої IDS з використанням туманної стратегії гарантує автономність пристроїв в забезпеченні їх безпеки з низькою затримкою.

Таким чином з отриманого сенсорною системою трафіку на стороні самої локальної мережі проходить процес виділення параметрів та їх підготовка до обробки нейромережею, які потім шифруються і відправляються в потужну обчислювальну хмару, в ролі якої можуть виступати орендовані сервера тої чи іншої компанії, що пропонує послуги хмарного обчислення. На сервері дані обробляються нейромережевою

системою після чого на керуючу підсистему надсилається повідомлення про стан мережі Інтернету речей.

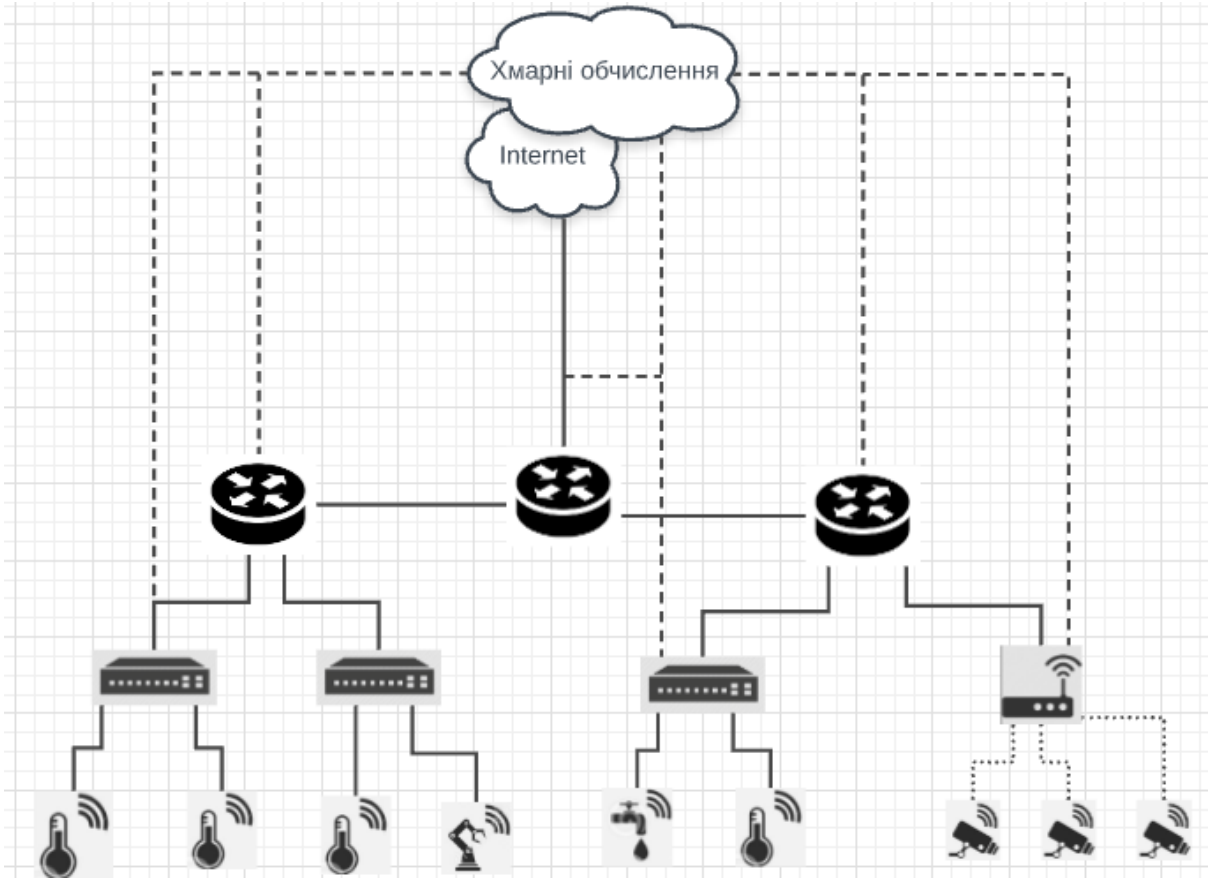

Рис. 2.3 Приклад побудови хмарної СВВ.

На рисунку 2.3 зображено приклад побудови мережі, в якій на рівні вузлів проходить попередня обробка трафіку, що проходе через порти, і відправка в обчислювальну хмару. Таким чином сенсорна частина IDS

знаходиться в локальній мережі, а ядро, що потребує певної кількості обчислювальних ресурсів, в хмарі.

2.2 Модифікований нейромережевий імунний метод

Вирішити проблему високого використання обчислювального ресурсу пропонується завдяки впровадженню процесу донавчаня (Uplearning) в нейромережу виявлення аномалії.

Донавчаня — це процес при якому локальні мінімуми поглиблюються, збільшуючі свою доступність, старі зв'язки послаблюються і посилюються нові, а вся система переоптимізується для нового набору знань.

Система перехода від досвіду загального функціонування мереж до вивчення конкретної мережі. Припускається що при такому підході система адаптується під вирішення конкретної задачі виявлення аномалії цілевої мережі, тим самим зменшуючи кількість виявлених незлонамірених аномалій. Що в свою чергу зменшить кількість активацій наступних шарів системи, тим самим зменшивши кількість обчислень в системі.

За основу модуля виявлення аномалії пропонується обрати рекурентну нейронну мережу (Recurrent neural network; RNN), що представляє собою нейронну мережу, де зв'язки між елементами утворюють спрямовану послідовність. Завдяки цьому з'являється можливість обробляти серії подій у часі або послідовні просторові ланцюжки. На відміну від багатошарових перцептронів, рекурентні мережі можуть використовувати свою внутрішню пам'ять для обробки послідовностей довільної довжини. Тому мережі RNN застосовні в таких завданнях, де щось цілісне розбите на частини, наприклад: розпізнавання рукописного тексту [37], розпізнавання мови [38] [39] або розподілену в часі аномалію[39].

Вибір обумовлено двома причинами. По-перше, рекурентні мережі природним чином підтримують часові ряди. Для того, щоб врахувати залежність від часу в даних, для такої моделі потрібно лише подавати вектори xt в потрібному порядку без застосування складного конструювання ознак (яке зазвичай саме по собі є складним завданням, специфічною для кожного окремого випадку). По-друге, на даний момент нейронні мережі дають найвищу якість регресії в подібних завданнях, коли дані на тестовій вибірці схоже на дані в навчанні, але при цьому сильно помиляються в протилежному випадку. Такий сильний контраст, який є в багатьох випадках недоліком, для детектування рідкісних подій є ключовим фактором успіху.

Для того, щоб детектувати аномалії, необхідно вміти відновлювати нормальний перебіг процесу. Якщо модель отримала досить велику вибірку, в якій міститься більшість сценаріїв нормальної роботи, то можна сподіватися, що після навчання вона зможе успішно вирішити таке завдання регресії.

При цьому, якщо модель є слабким екстраполятор, то вона не зможе давати адекватні оцінки на тих даних, які «не бачила» раніше.

Такими властивостями володіють практично всі алгоритми машинного навчання. Однак ми детальніше зупинимося на використанні рекурентних нейронних мереж.

Це обумовлено двома причинами. По-перше, рекурентні мережі природним чином підтримують тимчасові ряди. Для того, щоб врахувати залежність від часу в даних, для такої моделі потрібно лише подавати вектори xt в потрібному порядку без застосування складного конструювання ознак (яке зазвичай саме по собі є складним завданням, специфічною для кожного окремого випадку). По-друге, на даний момент нейронні мережі дають найвищу якість регресії в подібних завданнях, коли дані на тестовій вибірці схоже на дані в навчанні, але при цьому

сильно помиляються в протилежному випадку. Такий сильний контраст, який є в багатьох випадках недоліком, для детектування рідкісних подій є ключовим фактором успіху.

У глибинному навчанні найкраще себе зарекомендували не звичайні рекурентні нейронні мережі, а їх модифікації, такі як LSTM [34] або GRU [35]. Це більш складні системи, які можуть «запам'ятовувати» дуже довгі послідовності, що недоступно для звичайних нейромереж. Крім того, швидкість збіжності таких архітектур зазвичай вище. Практично всі роботи, пов'язані з аналізом послідовностей, використовують їх в якості основних обчислювальних блоків.

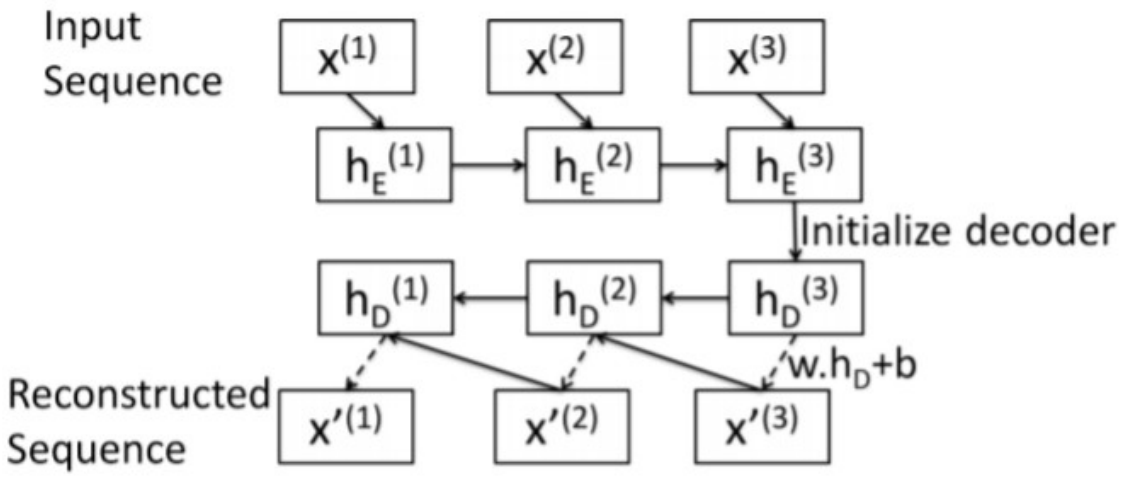

Рис. 2.4 [40] Схема класичної рекурентної нейронної мережі

Проте використання процедури донавчання в ході її функціонування може виникнути явище перенавчання (overfitting)[36], і тим самим втрачання нейромережею здатності вирішувати поставлену задачу.

Для того, щоб уникнути цього небажаного явища, запропоновано використати метод розріджених матриць на основі баєсівської моделі, що дозволить домогтися виключення всіх неінформативних ваг.

Таким чином вирішується відразу кілька завдань: відбувається регуляризація моделі, прискорюється час обробки, а також залишаються тільки набори цінних ознак.

Використання байесовских методів в глибинному навчанні є те, що фактично вчиться не одна мережа, а цілий ансамбль мереж в рамках однієї моделі. Ансамблювання може збільшити точність моделі, збільшити стійкість моделі щодо малих змін в даних. Ціною за таку властивість є дещо складніший і довший процес попереднього навчання нейромережі.

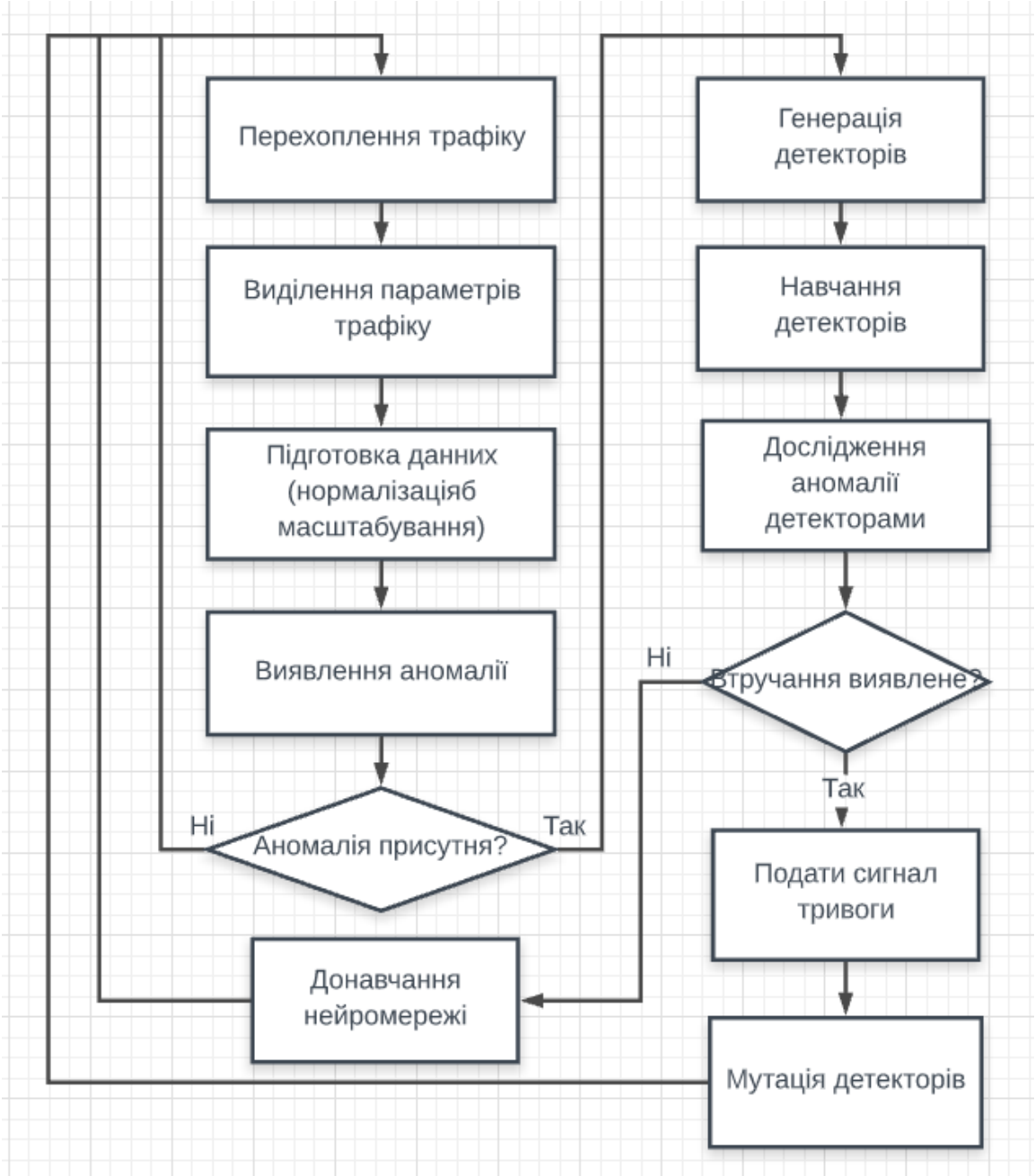

Рис. 2.5 Блоксхема запропонованого методу

Таким чином запропонований метод зводиться до набору наступних кроків:

Крок 1. Сенсорна система отримує трафік з мережевих сенсорів.

Крок 2. З отриманого трафіку виділяються його параметри.

Крок 3. Отриманий набір даних формується в вектор даних, які нормалізуються, і масштабуються.

Крок 4. Вектор подається на обробку першої нейромережі.

Крок 5. Якщо нейромережа приймає рішення про те, що у вхідному векторі відсутні ознаки аномальності, то система повертається до кроку 1. В іншому випадку перехід на наступний крок.

Крок 6. Генерується набір детекторів з різними параметрами та структурами.

Крок 7. Детектори навчаються на розпізнавання окремих ознак мережевих атак.

Крок 8. Вектор вхідних даних досліджується детекторами.

Крок 9. Якщо признаки втручання не виявлено, система переходе на крок 10. Іначе перехід на крок 11.

Крок 10. Перша нейронна мережа донавчається на вхідному векторі і переходе на крок 1.

Крок 11. Подається сигнал тривоги.

Крок 12. Детектори мутують, вбираючи в себе інформацію про виявлене втручання. Перехід на крок 1.

Висновки:

1) Детально розглянуто використання обраного методу виявлення вторгнень в мережах інтернету речей. Приведено схему використання в мережі інтернету речей. Розглянуто переваги та недоліки використання обраного методу. Обрано для якого з недоліків буде проводитись модифікування.

2) Запропоновано модифікований метод виявлення вторгнення в мережу інтернету речей за допомогою нейромережі, з використанням процедури донавчання. Наведено блоксхему запропонованого методу.

РОЗДІЛ 3
ОПИС СТВОРЕНОГО МАКЕТУ ПРОВЕДЕННЯ НАТУРНОГО МОДЕЛЮВАННЯ ТА НАДАННЯ АНАЛІТИЧНОЇ ОЦІНКИ ЗАПРОПОНОВАНОГО МЕТОДУ

3.1 Натурне моделювання

Розроблений макет представляє собою написану програму Python, з використанням бібліотек TensorFlow та numpy, розгорнуту в хмарному середовищі Google Colaboratory.

Для проведення експерименту нейромережа була навчена на датасеті UNSW_NB15_a перевірялась на CICIDS-17. Таким чином ми намагаємось наблизитись до використання нейромережі в реальних умовах, в яких дані, які обробляє нейромережа, відрізняються від даних на яких вона була навчена.

Середовищем виконання експериментів було обрано середовище Google Colaboratory, з викоританням мови програмуванн Python та бібліотеки TensoFflow.

Фізичним середовищем експеременту виступали сервера Google з процессором Intel(R) Xeon(R) CPU @ 2.20GHz, 13GB оперативної памяті, та потужною відеокартою NVIDIA® Tesla® P100

Під кількістю обчислювальних ресурсів вважається кількість обчислювальних операцій, що виконуються в фрагментах коду нейромережі.

Дослідження здатності адаптації до незлонамірених аномалій

В ході експерименту випадковим чином обирається 1000 записів із датасету з набором 0,7 мільйона записів. Вибрані записи обробляються за допомогою методів прототипу і запропонованого. Записуєтсья кількість виявлених в даних аномалій.

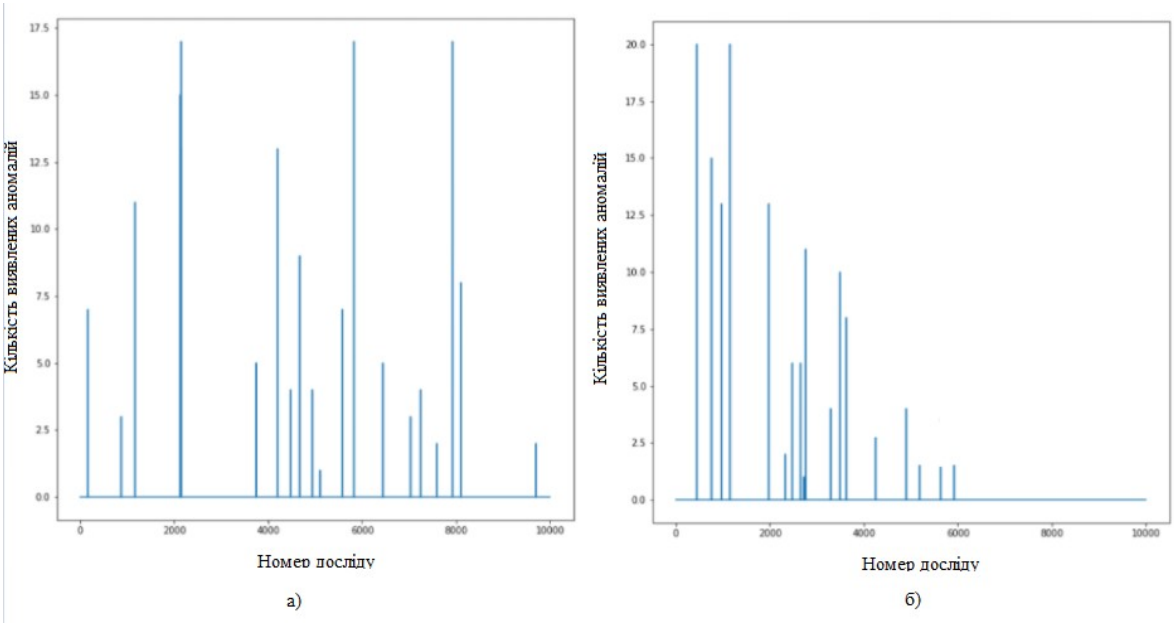

Рис. 3.1 Кількість виявлених аномалій в мережевому трафіку в залежності від кількості проведених експериментів. а) прототип, б) запропонований метод

Як видно на рисунку 3.1, кількість виявлених незлонамірених аномалій в ході експеременту зменшувалась.

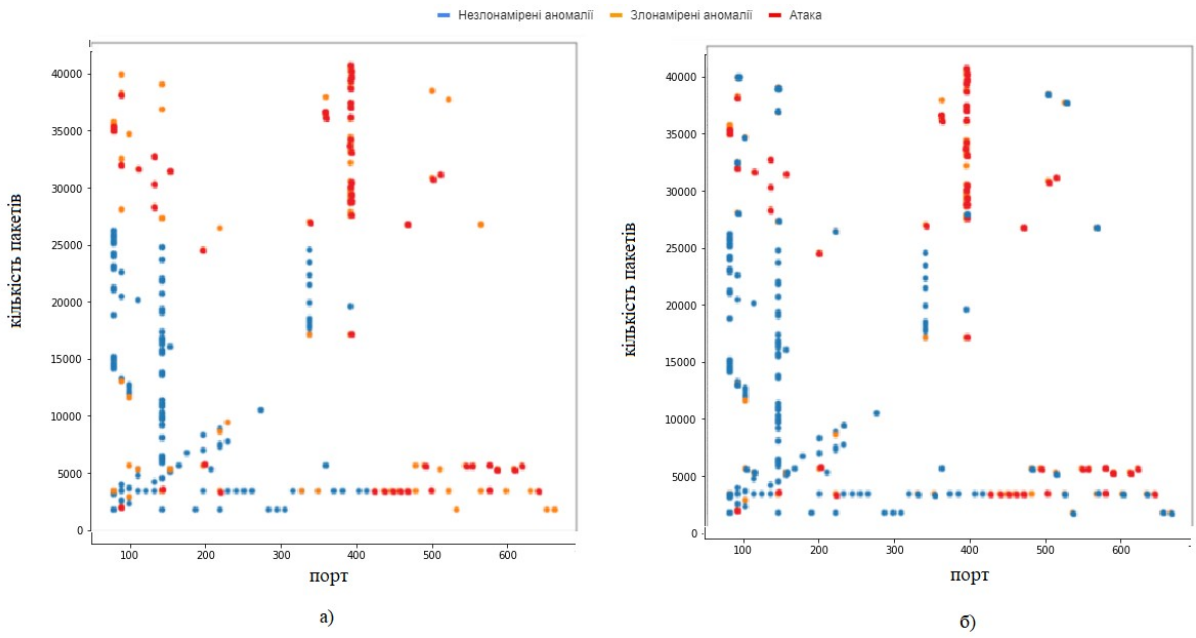

Рис. 3.2. Рішення про аномальність події відносно кількості пакетів що надходить на певний порт. а) До проходження процесу донавчання, б) Після проходження процесу донавчання

На рисунку 3.2 зображено події надходження певної кількості пакетів на певний порт. Синім кольором позначені неаномальні події. Оранжевим незлонамірені аномалії, червоним злонамірені аномалії.

Видно що в ході процесу донавчання, кількість незлонамірених аномальних подій зменшилась, перейшовши в клас нормальних подій.

Висновок:

Запропонований метод дозволяє системі адаптуватись до незлонамірених аномалій. Кількість виявлених аномалій з часом зменшується.

Дослідження здатності зменшувати кількість обчислень

В ході експерименту випадковим чином обирається 1000 записів із датасету з набором 0,7 мільйона записів. Вибрані записи обробляються за допомогою методів прототипу і запропонованого. В середовищі виконання був запущений профайлер, що відстежує кількість виконаних обчислювальних операцій.

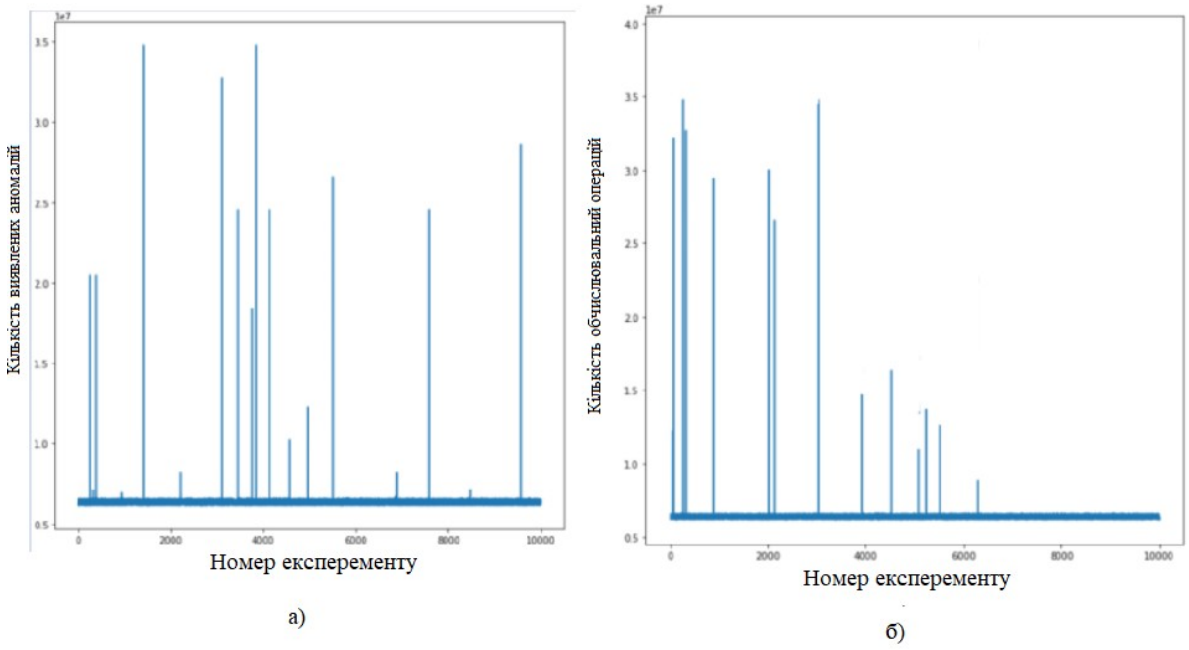

Рис. 3.3. Кількість виконаних обчислювальних операцій в залежності від кількості проведених експериментів. а) прототип, б) запропонований метод

Як видно на рисунку, кількість обчислень зменшується пропорційно до зменшення виявлених незлонамірених аномалій.

Висновок:

Запропонований метод дозволяє з часом зменшити кількість обчислень, потрібних для функціонування системи.

Дослідження здатності виявляти злонамірені аномалії

В ході експерименту випадковим чином обирається 1000 записів із датасету з набором 0,7 мільйона записів.Випадковим чином деякі з цих записів заміняються на записи із датасету мережевих атак. Вибрані записи обробляються за допомогою методів прототипу і запропонованого. Кількість виявлених злонамірених і незлонамірених аномалій запиисується.

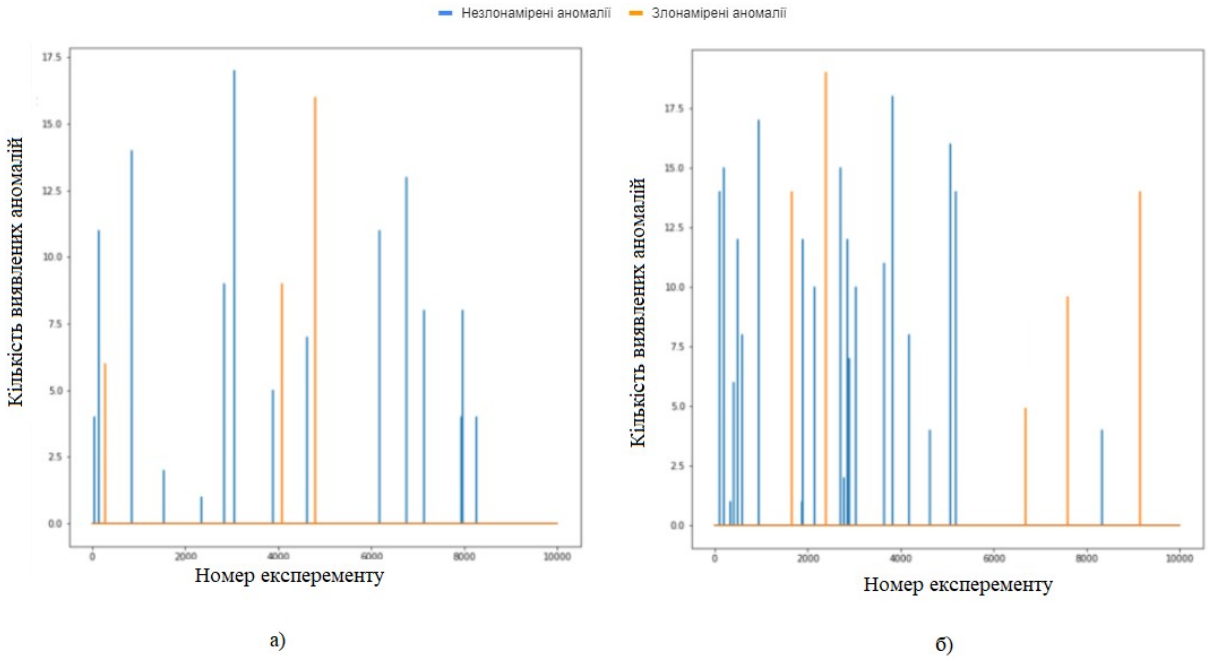

Рис. 3.4 Кількість виявлених злонамірених і не злонамірених аномалій в мережевому трафіку в залежності від кількості проведених експериментів. а) прототип, б) запропонований метод

На рисунку 3.4 злонамірені аномалі позначені оранжевим кольором, а незлонамірені синів. Як видно на рисунку, здатність виявляти злонамірені аномалії не зникла. При тому що кількість незлонамірених з часом зменшується.

Висновок:

Запропонований метод адекватно працює, процес адаптації не призводить до втрати здатності виявляти злонамірені аномалії.

Дослідження точності виявлення втручання

В ході експерименту випадковим чином обирається 3000 записів із датасету атак на мережі з набором 200 тисяч записів. Нейромережа для запропонованого методу попередньо донавчена виявляти тільки

злонамірені аномалії. Вибрані записи обробляються за допомогою методів прототипу і запропонованого. Точність вираховується як відношення кількості виявлених втручань до загальної їх кількості. Замір проводиться 15 разів. Кожного разу точність записується.

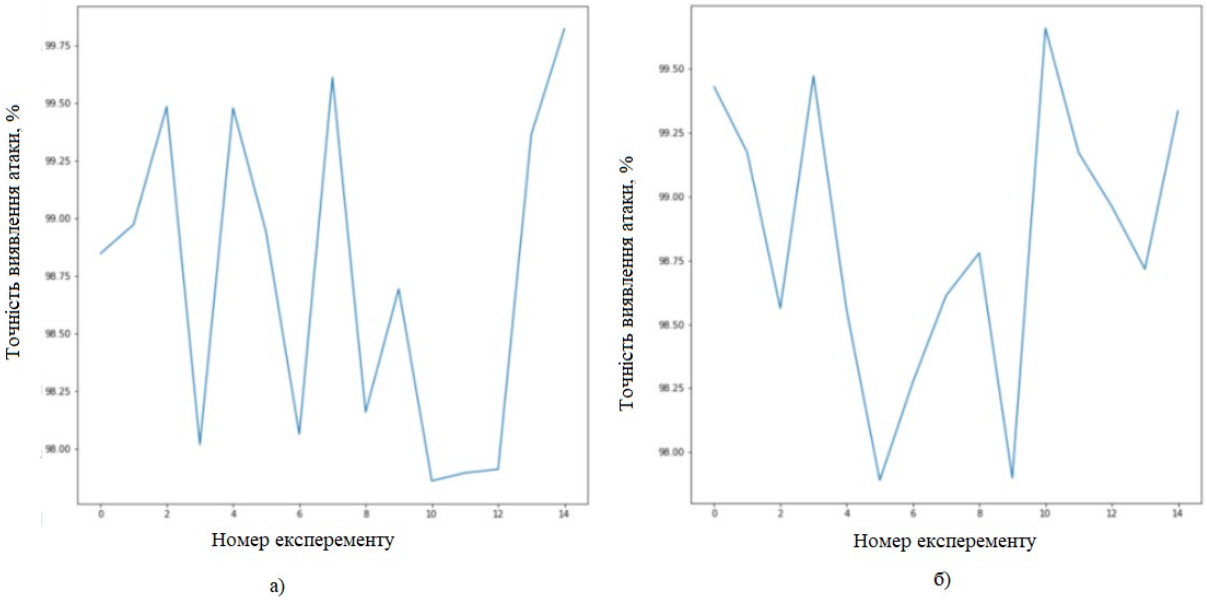

Рис. 3.5 Ефективність виявлення аномалій в різних дослідах. а) прототип, б) запропонований метод

Як видно на рисунку 3.5, точність запропонованого методу знаходиться в томуж діапазоні що і в прототипі.

Висновок:

Запропонований метод не втрачає точності виявлення втручання в мережу.

Дослідження збереження здатності запропонованого методу виявляти різні за масштабом аномалії

В ході експерименту випадковим чином обирається 3000 записів із датасету атак на мережі з набором 200 тисяч записів. Нейромережа для

запропонованого методу попередньо донавчена виявляти тільки злонамірені аномалії. Вибрані записи обробляються за допомогою методів прототипу і запропонованого.

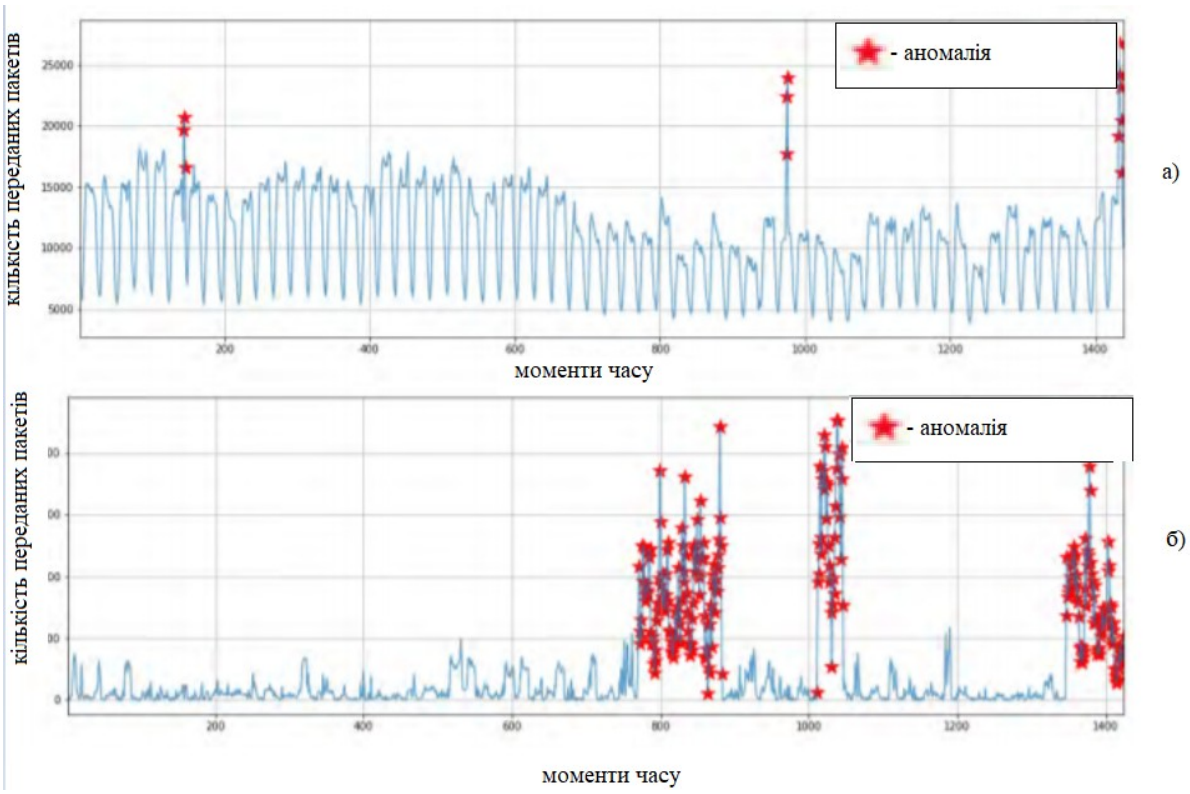

Рис. 3.6. Виявлені аномалії у відношенні мережевого трафіку до часу. а) незначні аномалії, б) значні аномалії

Як видно на рисунку 3.6, запропонований метод дозволяє виявляти як і стрімке збільшення трафіку, так і короткочасні невеликі стрибки.

Висновок:

Запропонований метод дозволяє виявляти аномалії різних масштабів.

Таблиця 3.1

Таблиця порівняння середньої кількості обчислень для обробки одного вхідного вектору даних мережі

Номер експерименту	Прототип	Запропонований
1	294728	235770
2	303438	243959
3	291343	241253
4	291730	247422
5	292043	241596
6	280723	242307
7	295552	244119
8	288489	244189
9	281353	254877
10	288683	247606
11	276852	250886
12	284231	253888
13	301622	247559
14	273317	240542
15	274615	249370
16	272640	241620
17	284618	244716
18	287279	249945
19	281472	239234
20	286262	243224

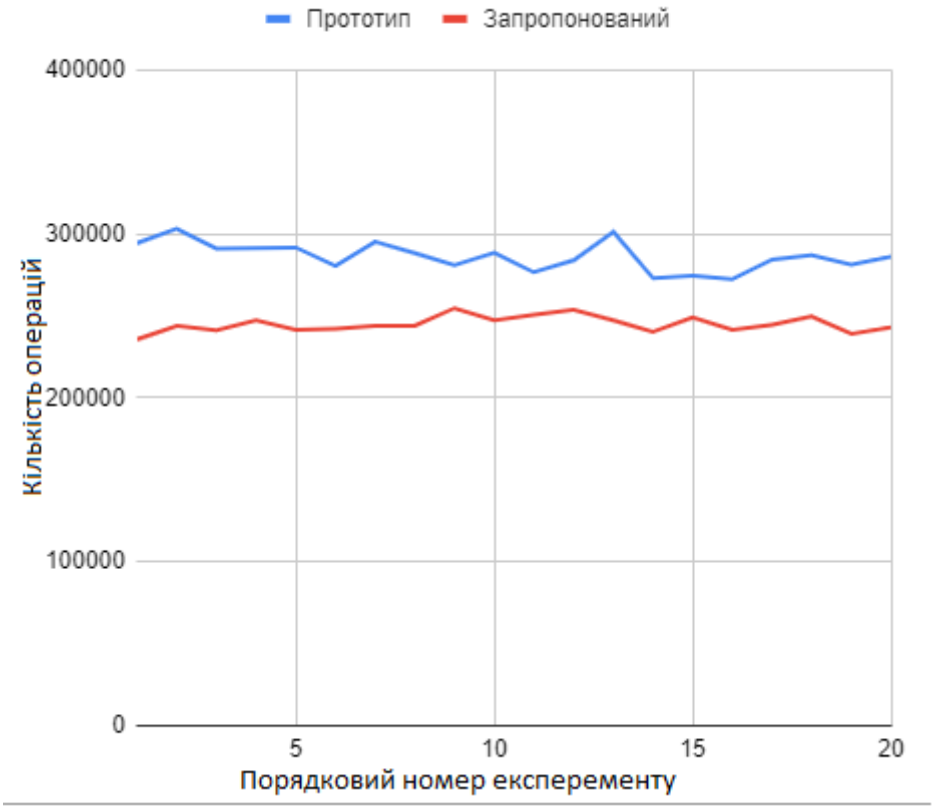

Рис. 3.7. Порівняння середньої кількості операцій потрібних для обробки одного вхідного вектору мережевого трафіку.

3.2 Аналітична оцінка запропонованого рішення

В даному розділі проаналізовано розглянуті методи натурного моделювання з попереднього розділу.

Аналіз буде проводитись за критеріями ресурсозатратності, де під кількістю витрачених ресурсів мається на увазі середня кількість виконаних обчислювальних операцій для обробки одного вхідного вектору мережевих даних.

Виходячи з вище представлених експериментів можна сказати що запропонований метод не втратив переваг прототипу, таких як здатність виявляти різні за масштабом атаки, а також відношення виявлених атак до загальної кількості атак залишилось на одному рівні.

В той самий час експерименти показують що середня кількість витрачених обчислювальний ресурсів, що потрібна на обробку одно вхідного вектору даних мережі зменшилась. Отже можна зробити висновок що процес донавчання допоміг досягти поставлену мету.

Приріст ресурсоекономії можна оцінити як:

$$K = \frac{\sum_{0}^{N} \alpha_n * N}{\sum_{0}^{N} \beta_n * N} = \frac{\sum_{0}^{N} \alpha_n}{\sum_{0}^{N} \beta_n} \quad (3.1)$$

де K – коефіцієнт приросту ресурсоекономності, α_n – *середня кількість обчислювальних операцій в реалізації* прототипу, β_n – *середня кількість обчислювальних операцій* в реалізації запропонованому методу, n – *порядковий номер експерименту*.

Таблиця 3.2

Порівняння середньої кількості виконаних обчислювальних операцій в реалізаціях прототипу і запропонованого методу

	Прототип	Запропонований
Середній показник кількості виконаних операцій на обробку одно вхідного вектору даних мережі	286549,5	245204,1

Таким чином розрахуємо $K = \frac{286549,5}{245204,1} =$ 1.1686. Приріст обчислювальної ефективності запропонованого методу становить 16.8 %.

Висновки:

1) Проведено натурне моделювання запропонованого методу та прототипу. Проведено експеримент порівняння методів за часом виконання алгоритму шифрування, та дешифрування повідомлень.
2) Проведено аналітична оцінка запропонованого методу, та обчислений рівень криптостійкості для запропонованого методу.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1) Проведено огляд проблем безпеки захисту мереж інтернету речей, за рахунок якого було обрано напрямок вирішення проблеми захисту на рівні програмного забезпечення.
2) Проаналізовано сучасні рішення захисту мереж інтернету речей від втручання, на основі чого було обрано прототип методу виявлення втручання на основі нейромережевого імунного методу.
3) Удосконалено нейромережевий імунний метод виявлення вторгнень в мережу за рахунок впровадження процесу донавчання в нейромережу виявлення аномалії.
4) Виконано натурне моделювання модифікованого методу, та поставлено ряд експериментів, що підтверджують працездатність запропонованого методу. За рахунок аналітичної оцінки, проведеної за допомогою експериментальних даних показано що кількість обчислювальних ресурсів, що витрачаються зменшилась, що дозволяє говорити про те що поставлена мета була досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Posetive Technologes [Електронний ресурс] / Актуальные киберугрозы. II квартал 2020 года — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/ (дата публикации: 16.07.2020).
2. Nandi A. An Overview: Security Issue in IoT Network [Електронний ресурс] / A. Nandi, M. Agarwal, D. Samanta // IEEE. – 2018. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8653728.
3. I. Dutt, S. Borah and I. K. Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed", IEEE Access, vol. 8, pp. 34929-34941, 2020.
4. de Castro L and Timmis J (2002) Artificial Immune Systems: A New Computational Intelligence Approach. Springer
5. JernvK (1974) Towards a network theory of the immune system. Annals of Immunology.
6. Zimmermann J., Mohay G. Distributed intrusion detection in clusters based on non-interference // Proceedings of the Australasian Workshops on Grid Computing and E-Research (ACSW Frontiers). Australian Computer Society, Inc. 2006. P. 89–95
7. Ioulianou, Philokypros, Vasilakis, Vasileios, Moscholios, Ioannis et al. (1 more author) (Accepted: 2018) A Signature-based Intrusion Detection System for the Internet of Things. In: Information and Communication Technology Form, 11-13 Jul 2018. (In Press)
8. H. Bahsi, S. Nomm and F. B. La Torre, "Dimensionality reduction for machine learning based IoT botnet detection", Proc. 15th Int. Conf. Control Autom. Robot. Vis. (ICARCV), pp. 1857-1862, Nov. 2018.

9. V. C. Loi, M. Nicolau and J. McDermott, "Learning neural representations for network anomaly detection", IEEE Trans. Cybern., vol. 49, no. 8, pp. 3074-3087, Aug. 2019.
10. L. Wen, L. Gao and X. Li, "A new deep transfer learning based on sparse auto-encoder for fault diagnosis", IEEE Trans. Syst. Man Cybern. Syst., vol. 49, no. 1, pp. 136-144, Jan. 2019.
11. S. Jialin Pan and Q. Yang, "A survey on transfer learning", IEEE Trans. Knowl. Data Eng., vol. 22, no. 10, pp. 1345-1359, Oct. 2010.
12. J. Lu, V. Behbood, P. Hao, H. Zuo, S. Xue and G. Zhang, "Transfer learning using computational intelligence: A survey", Knowl.-Based Syst., vol. 80, pp. 14-23, May 2015.
13. V. C. Loi, M. Nicolau and J. McDermott, "Learning neural representations for network anomaly detection", IEEE Trans. Cybern., vol. 49, no. 8, pp. 3074-3087, Aug. 2019.
14. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153-1176, 2nd Quart. 2016.
15. S. García, A. Zunino and M. Campo, "Botnet behavior detection using network synchronism" in Privacy Intrusion Detection and Response: Technologies for Protecting Networks, Hershey, PA, USA:IGI Global, pp. 122-144, 2012.
16. Бессонова Е.Е., Ефремов А.А., Настека А.В.и др. Анализ защищенности систем «Умный дом» // Материалы конференции Региональная информатика «РИ-2014». СанктПетербург, 2014.
17. Pang Y., Jia S. Wireless smart home system based on Zigbee // International Journal of Smart Home. 2016. V. 10. N 4. P. 209–220. doi: 10.14257/ijsh.2016.10.4.19

18. Belaidouni S., Miraoui M., Tadj C. Towards an efficient smart space architecture // International Journal of Advanced Studies in Computer Science and Engineering. 2016. V. 5. N 1. P. 18–27.
19. Barcena M.B., Wueest C. Insecurity in the Internet of Things. Symantec, Report 21349619. 2015.
20. Стариковский А.В., Жуков И.Ю., Михайлов Д.М. и др. Исследование уязвимостей систем умного дома // Спецтехника и связь. 2012. №2. С. 55–57.
21. Son S.-Y. Home electricity consumption monitoring enhancement using smart device status information // International Journal of Smart Home. 2015. V 9. N 10. P. 189–196. doi: 10.14257/ijsh.2015.9.10.21
22. Проталинский О.М. Применение методов искусственного интеллекта при автоматизации технологических процессов. — Астрахань: Изд-во АГТУ, 2004.
23. R. Bace and P. Mell. “Intrusion Detection Systems”, NIST Special Publication 800-31. 2001.
24. I. Dutt, S. Borah and I. K. Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed", IEEE Access, vol. 8, pp. 34929-34941, 2020.
25. M. Tabatabaefar, M. Miriestahbanati and J.-C. Grégoire, "Network intrusion detection through artificial immune system", Proc. Annu. IEEE Int. Syst. Conf. (SysCon), pp. 1-6, Apr. 2017.
26. M. Pamukov, "Application of artificial immune systems for the creation of IoT intrusion detection systems", 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS, 2017.)
27. Weber M, Boban M (2016) Security challenges of the internet of things In: 2016 39th International Convention on Information and

Communication Technology, Electronics and Microelectronics (MIPRO), 638–643.. IEEE, Opatija.

28. Kumar S, Vealey T, Srivastava H (2016) Security in internet of things: Challenges, solutions and future directions In: 2016 49th Hawaii International Conference on System Sciences (HICSS), 5772–5781, Koloa.
29. Liu X, Zhao M, Li S, Zhang F, Trappe W (2017) A security framework for the internet of things in the future internet architecture. Future Internet 9(3).
30. Trappe W, Howard R, Moore RS (2015) Low-energy security: Limits and opportunities in the internet of things. IEEE Secur Priv 13(1):14–21.
31. Hassan AM, Awad AI (2018) Urban transition in the era of the internet of things: Social implications and privacy challenges. IEEE Access 6:36428–36440
32. Mohan R, Danda J, Hota C (2016) Attack Identification Framework for IoT Devices. Springer, New Delhi.
33. Forsström S, Butun I, Eldefrawy M, Jennehag U, Gidlund M (2018) Challenges of securing the industrial internet of things value chain In: 2018 Workshop on Metrology for Industry 4.0 and IoT, 218–223.. IEEE, Brescia.
34. Sepp Hochreiter and Jurgen Schmidhuber. Long short-term memory. Neural Comput., 9(8):1735– 1780, November 1997. ISSN 0899-7667. doi: 10.1162/neco.1997.9.8.1735. URL http://dx.doi. org/10.1162/neco.1997.9.8.1735.
35. Cho, Kyunghyun; van Merrienboer, Bart; Gulcehre, Caglar; Bahdanau, Dzmitry; Bougares, Fethi; Schwenk, Holger; Bengio, Yoshua. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. arXiv:1406.1078, 2014.

36. S. Wager, S. Wang, and P. Liang. Dropout training as adaptive regularization. In Advances in Neural Information Processing Systems 26, pages 351–359, 2013.
37. E. Hodo, X. Bellekens, A. Hamilton, P. L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Networks, Computers and Communications (ISNCC), 2016 International Symposium on. IEEE, May 2016.
38. F. Hosseinpour, P. V. Amoli, J. Plosila, T. Hmlinen, and H. Tenhunen. An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach. International Journal of Digital Content Technology and its Applications(JDCTA), Volume 10, Issue 5, December 2016.
39. M. Kansra and P. D. Chadha. Cluster Based detection of Attack: IDS using Data Mining
40. Sutskever, Ilya, Vinyals, Oriol, and Le, Quoc V. Sequence to sequence learning with neural networks. In Ghahramani, Z., Welling, M., Cortes, C., Lawrence, N. D., and Weinberger, K. Q. (eds.), Advances in Neural Information Processing Systems 27, pp. 3104–3112. Curran Associates, Inc., 2014.