ДОДАТОК А
ГРАФІЧНИЙ МАТЕРІАЛ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ У ТРАНСПОРТНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

КВАЛІФІКАЦІЙНА РОБОТА
ДРУГИЙ (МАГІСТЕРСЬКИЙ) РІВЕНЬ

Автор:
Волошин І.А.,
студ. гр. КСМм-21-1

Керівник:
Кучук Н.Г.,
проф. каф. ЕОМ

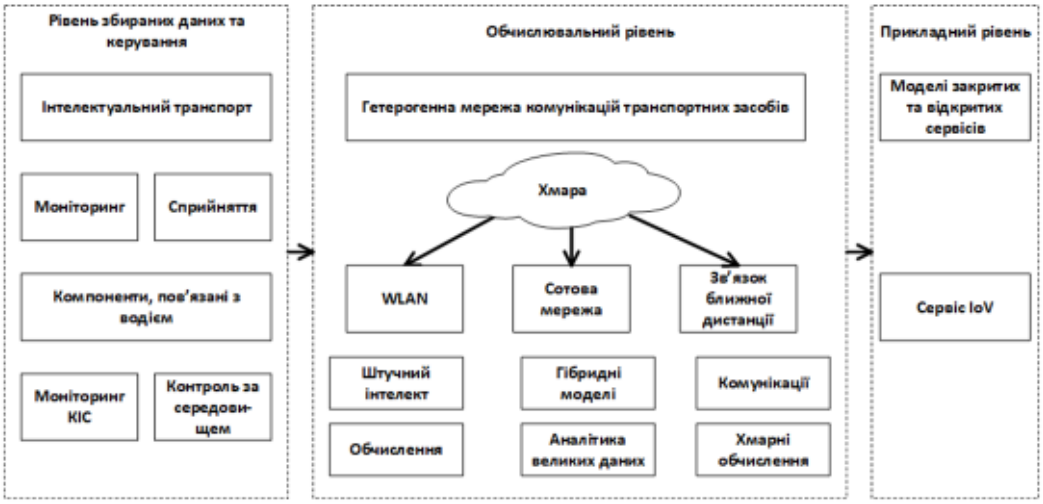
МЕТА І ЗАДАЧІ РОБОТИ

Мета кваліфікаційної роботи: розробка методу для виявлення аномалій транспортній мережі на основі класифікації атак.

Основні проблеми, які потрібно вирішити:

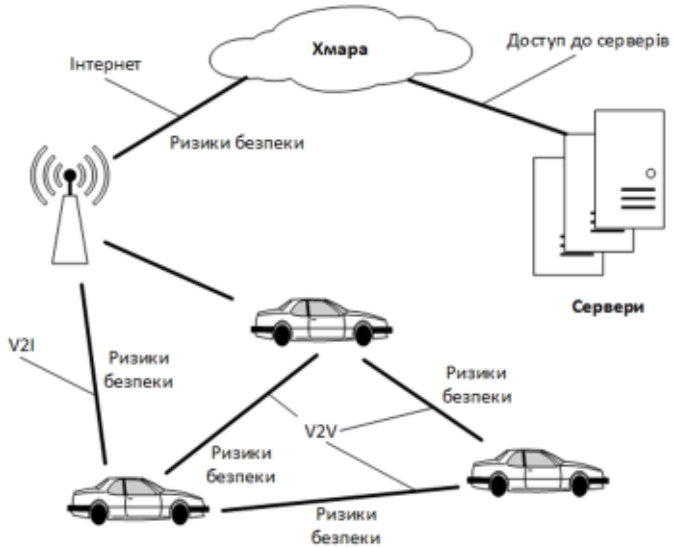
- у випадку класифікації з кількома класами, для точної ідентифікації або виявлення всіх класів даних проблему становить можлива незбалансованість класів;
- іноді матимуть місце великовимірні дані, а функції можуть бути розріджені, тому ефективний вибір функцій є проблемою;
- виявлення та передбачення ефективніше в глибокому навчанні, ніж із застосуванням традиційних методів машинного навчання.

КЛЮЧОВІ КОМПОНЕНТИ ТА РІВНІ ТРАНСПОРТНОЇ МЕРЕЖІ



3

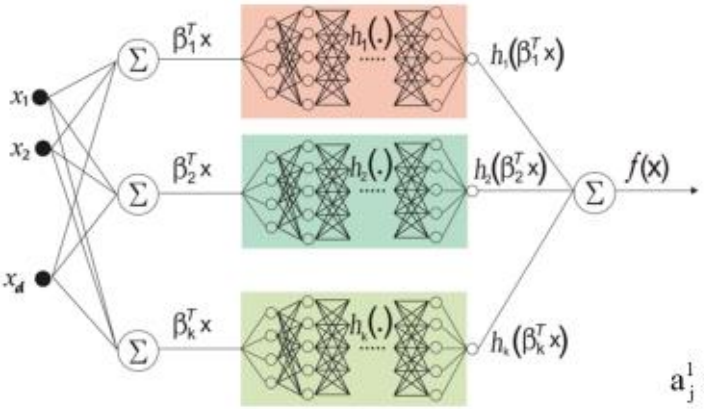
ІНФОРМАЦІЙНІ РИЗИКИ В ТРАНСПОРТНІЙ МЕРЕЖІ



4

ЗАПРОПОНОВАНА АРХІТЕКТУРА XNN

$$f(x) = \sigma + \gamma_1 h_1 \beta_1^T x + \gamma_2 h_2 \beta_2^T x + [...] + \gamma_K h_K \beta_K^T x$$

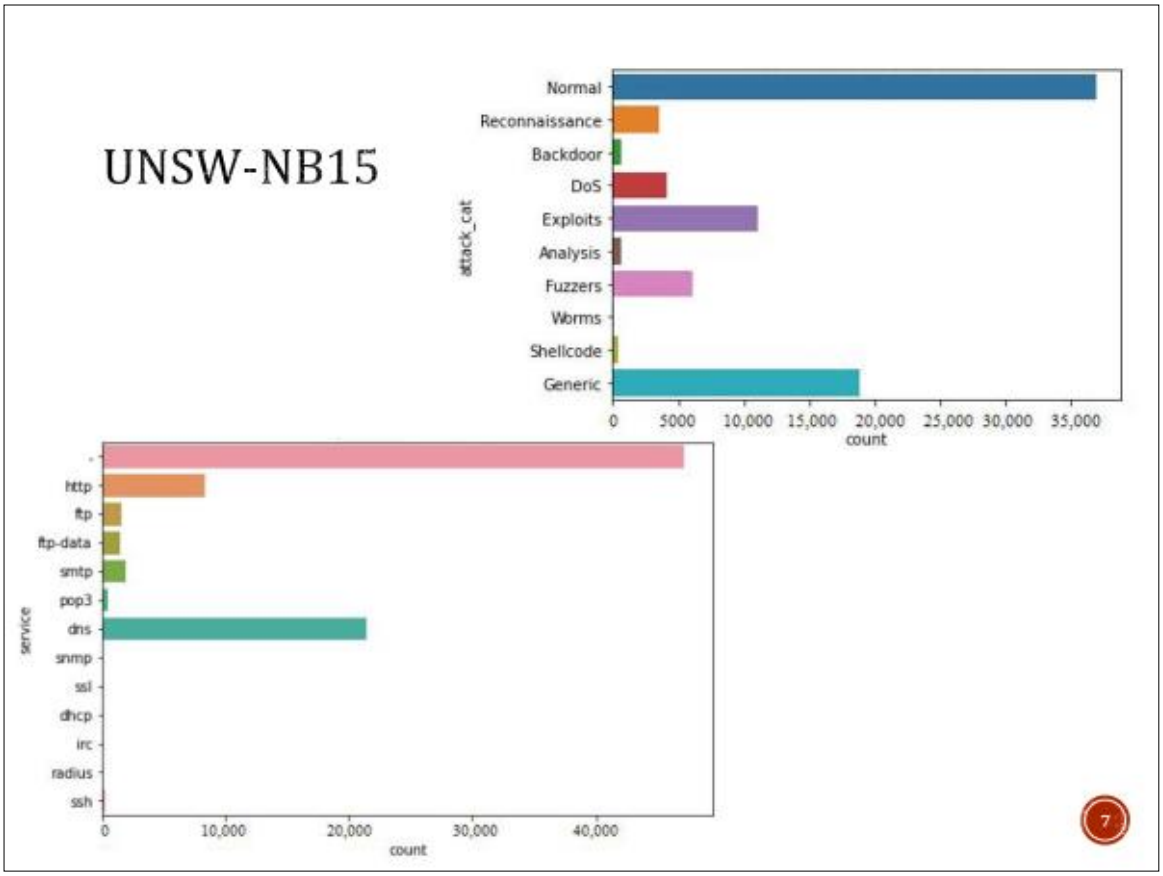


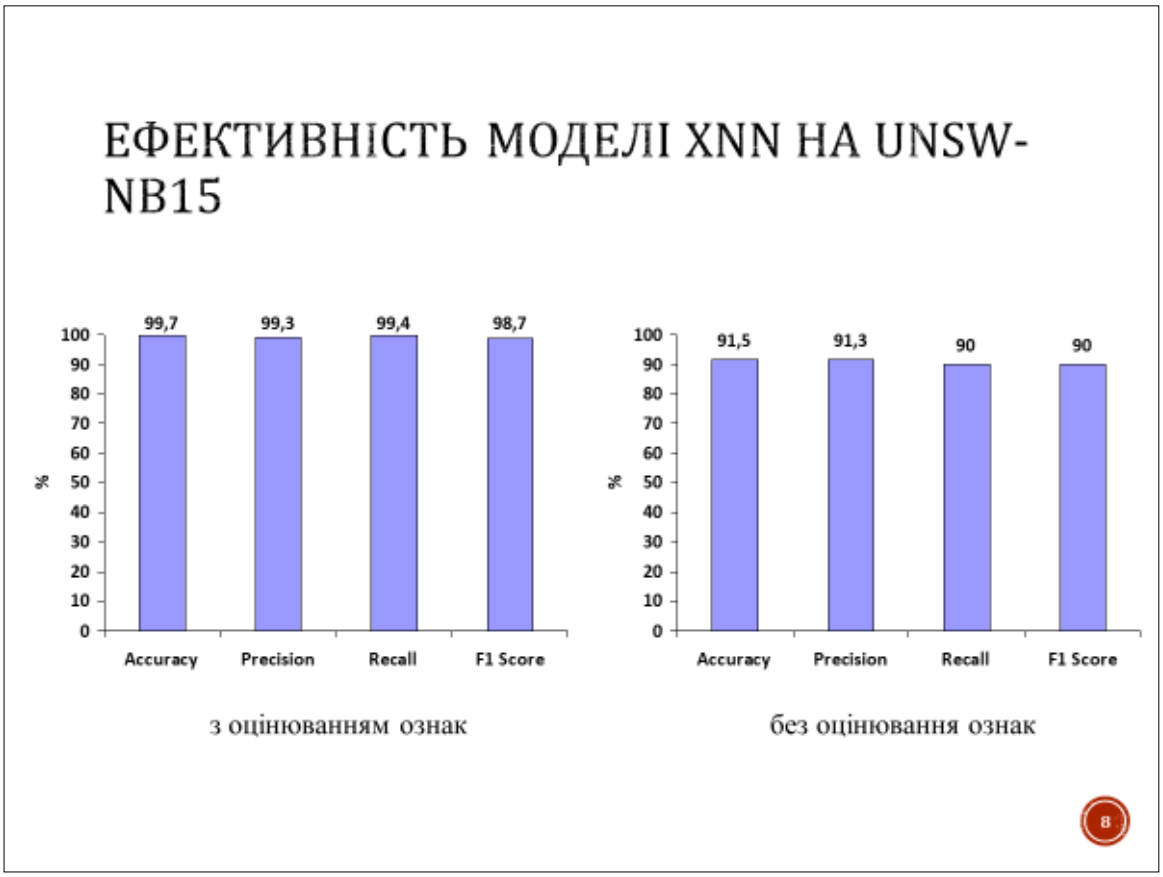
$$a_j^l = \sigma\left(\left[\sum_{k=1}^{a_{l-1}} w_{j,k}^l a_k^{l-1}\right] + b_j^l\right)$$

5

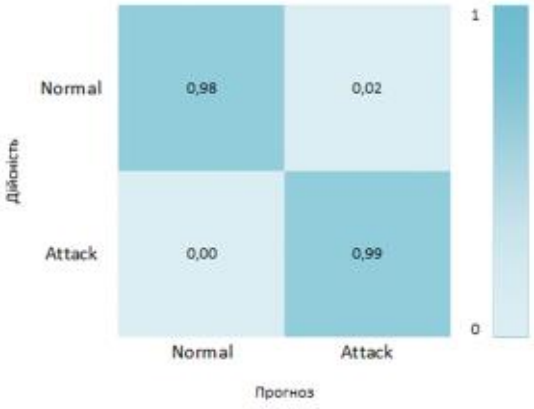
СТРУКТУРА ПОТОКУ ДАНИХ ПРИ РЕАЛІЗАЦІЇ ЗАПРОПОНОВАНОГО МЕТОДУ

6

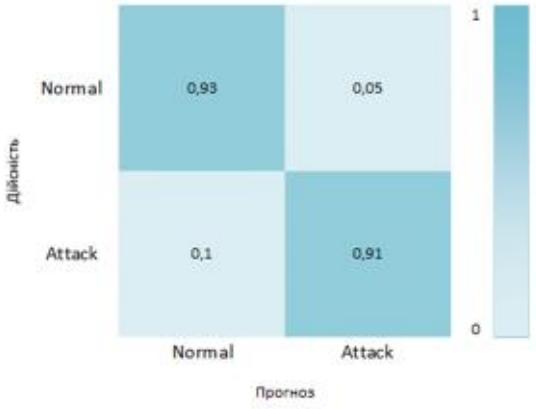

UNSW-NB15
attack_cat
Normal
Reconnaissance
Backdoor
DoS
Exploits
Analysis
Fuzzers
Worms
Shellcode
Generic
0
5000
10,000
15,000
20,000
25,000
30,000
35,000
count
service
-
http
ftp
ftp-data
smtp
pop3
dns
snmp
ssl
dhcp
irc
radius
ssh
0
10,000
20,000
30,000
40,000
count
7


ЕФЕКТИВНІСТЬ МОДЕЛІ XNN НА UNSW-NB15
%
100
90
80
70
60
50
40
30
20
10
0
99,7
99,3
99,4
98,7
Accuracy
Precision
Recall
F1 Score
з оцінюванням ознак
91,5
91,3
90
90
без оцінювання ознак
8

МАТРИЦІ ПОМИЛОК XNN ДЛЯ UNSW-NB15



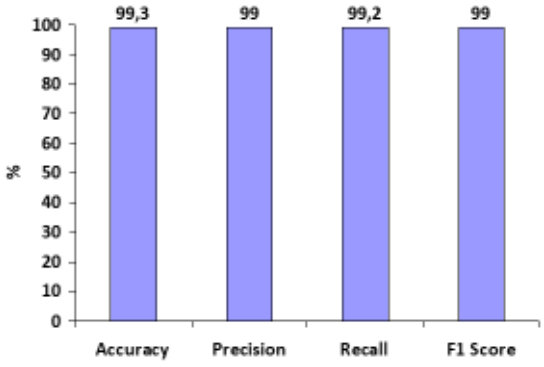
з оцінюванням ознак



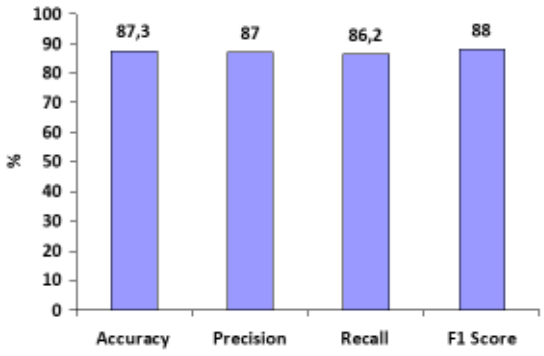
без оцінювання ознак

9

ЕФЕКТИВНІСТЬ МОДЕЛІ XNN НА CICIDS2019



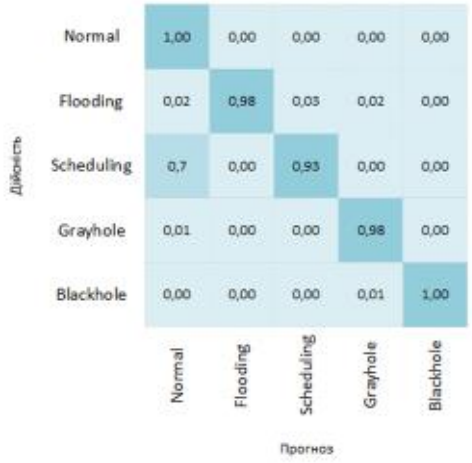
з оцінюванням ознак



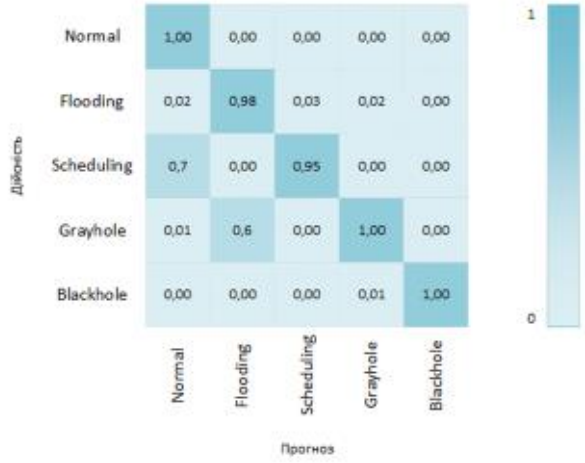
без оцінювання ознак

10

МАТРИЦІ ПОМИЛОК XNN ДЛЯ CICIDS2019



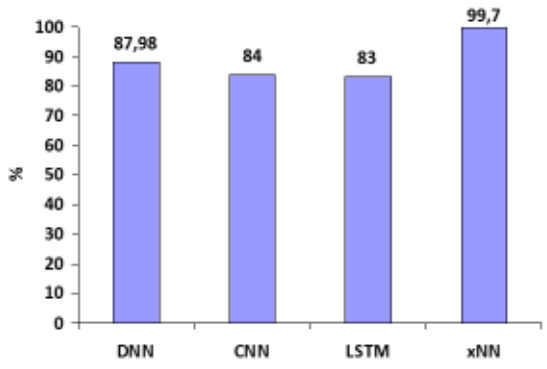
з оцінюванням ознак



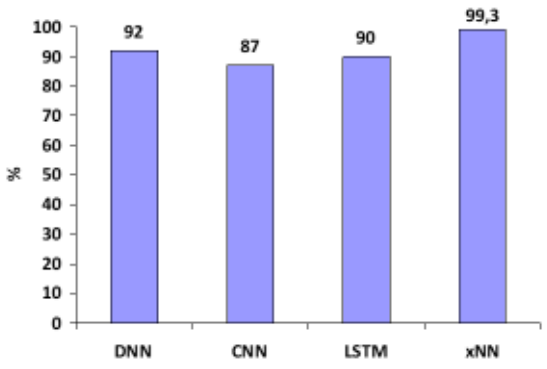
без оцінювання ознак

11

ПОРІВНЯННЯ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ



набір даних UNSW-NB15



набір даних CICIDS2019

12

АПРОБАЦІЯ РЕЗУЛЬТАТІВ

Черкаський державний
технологічний університет

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

**ПРОБЛЕМИ
ІНФОРМАТИЗАЦІЇ**

ТЕЗИ ДОПОВІДЕЙ ДЕСЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

24 – 25 листопада 2022 року

Том 1

Черкаси – Баку – Бельсько-Бяла – Харків – 2022

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖІ IOV

Російський Д.М., Волошин І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Ідентифікувати різноманітні складні кібератаки в широкому діапазоні галузей, таких як Internet of Vehicles (IoV), зараз є дуже складним завданням. IoV – це комп'ютерна мережа транспортних засобів, яка складається з датчиків, приводів, мережевих засобів і систем та з'єднує між транспортними засобами. Важливу роль в IoV відіграє комунікація. Транспортні засоби в мережі обмінюються та передають інформацію на основі кількох протоколів. Через бездротовий зв'язок між транспортними засобами вся мережа може бути чутливою до кібератак. Під час цих атак конфіденційна інформація може бути передана зловмисній мережі або фактичному користувачу, що призведе до зловмисних атак на IoV. Традиційно системам виявлення вторгнень (IDS) стає дедалі важче виявляти нові, складніші атаки, які використовують незначні сліди. Щоб уникнути виявлення, зловмисники маскуються під типових користувачів. Ці проблеми можна вирішити за допомогою глибокого навчання. Багато моделей машинного та глибокого навчання (DL) були реалізовані для виявлення зловмисних атак; однак основною проблемою залишається вибір функцій. Завдяки використанню навчальних емпіричних даних DL самостійно визначає ознаки вторгнення.

Метою доповіді є подання моделі вторгнення на основі DL, яка зосереджена на нападах типу «відмова в обслуговуванні» (DoS). Для оцінки та ранжирування ознак пропонується використовувати кластеризацію k-середніх. Після виділення найкращих функцій для виявлення аномалій застосовується нова модель Explainable Neural Network (xNN), що дозволить окремо класифікувати атаки в наборі даних CICIDS2019 і UNSW-NB15. Модель показала хороші результати щодо точності, запам'ятовування, оцінки F1. Для порівняння можна побачити, що запропонована модель xNN показала хороші результати після використання техніки підрахунку характеристик. У наборі даних 1 (UNSW-NB15) xNN показав хороші результати з найвищою точністю 99,3%, тоді як CNN набрав 85%, LSTM – 89%, а Deep Neural Network (DNN) – 91%. xNN досяг найвищої точності 98,7% під час класифікації атак у другому наборі даних (CICIDS2019); згорткова нейронна мережа (CNN) досягла 86%, довготривала короткочасна пам'ять (LSTM) досягла 89,5%, а DNN досягла 83%. Запропоноване рішення перевершило існуючі аналоги за точністю виявлення та класифікації.

Список літератури

1. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. IEEE Internet Things J. 2021, 9, 616–632.
2. Ozcelebi, R.; Tiri, M.; Fedeoglu, F.; Ihan, M. Deep Real-Time Anomaly Detection for Connected Autonomous Vehicles. Procedia Comput. Sci. 2020, 177, 456–461.

13

ВИСНОВКИ

- Мережі транспортних засобів можна захистити від кіберзагроз за допомогою технологій штучного інтелекту. Глибоке навчання захищає автономний транспортний засіб, коли зловмисник намагається проникнути до нього.
- Для оцінки запропонованої системи безпеки використовувалися набори даних безпеки CICIDS2019 і UNSW-NB15.
- Задля визначення того, які характеристики є найважливішими, була використана кластеризація K-means.
- Виявлення типів атак у цьому наборі даних було здійснено за допомогою пояснюваної нейронної мережі xNN.

14

ВИСНОВКИ

- Наскільки відомо, xNN ніколи не застосовувалися в IDS, особливо в транспортних комп'ютерних мережах.
- Що стосується точності виявлення та класифікації, а також безпеки шини CAN у реальному часі, запропонований підхід перевершив існуючі рішення в дослідженні.
- Оцінка та ранжирування ознак на основі K-means також сприяли в цьому дослідженні найкращим методам вибору ознак і ранжирування на основі вагових коефіцієнтів.

ДОДАТОК Б
ПУБЛІКАЦІЇ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Черкаський державний
технологічний університет

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

ТЕЗИ ДОПОВІДЕЙ ДЕСЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

24 – 25 листопада 2022 року

Том 1

Черкаси – Баку – Бельсько-Бяла – Харків – 2022

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖІ IOV

Росінський Д.М., Волошин І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Ідентифікувати різноманітні складні кібератаки в широкому діапазоні галузей, таких як Internet of Vehicles (IoV), зараз є дуже складним завданням. IoV – це комп'ютерна мережа транспортних засобів, яка складається з датчиків, приводів, мережевих засобів і систем зв'язку між транспортними засобами. Важливу роль в IoV відіграє комунікація. Транспортні засоби в мережі обмінюються та передають інформацію на основі кількох протоколів. Через бездротовий зв'язок між транспортними засобами вся мережа може бути чутливою до кібератак. Під час цих атак конфіденційна інформація може бути передана зловмисній мережі або фіктивному користувачу, що призведе до зловмисних атак на IoV. Традиційним системам виявлення вторгнень (IDS) стає дедалі важче виявляти нові, складніші атаки, які використовують незвичайні схеми. Щоб уникнути виявлення, зловмисники маскуються під типових користувачів,. Ці проблеми можна вирішити за допомогою глибокого навчання. Багато моделей машинного та глибокого навчання (DL) були реалізовані для виявлення зловмисних атак; однак основною проблемою залишається вибір функцій. Завдяки використанню навчальних емпіричних даних DL самостійно визначає ознаки вторгнення.

Метою доповіді є подання моделі вторгнення на основі DL, яка зосереджена на нападах типу «відмова в обслуговуванні» (DoS). Для оцінки та ранжирування ознак пропонується використовувати кластеризацію k-середніх. Після виділення найкращих функцій для виявлення аномалій застосовується нова модель Explainable Neural Network (xNN), що дозволить окремо класифікувати атаки в наборі даних CICIDS2019 і UNSW-NB15. Модель показала хороші результати щодо точності, запам'ятовування, оцінки F1. Для порівняння можна побачити, що запропонована модель xNN показала хороші результати після використання техніки підрахунку характеристик. У наборі даних 1 (UNSW-NB15) xNN показав хороші результати з найвищою точністю 99,3%, тоді як CNN набрав 85%, LSTM – 89%, а Deep Neural Network (DNN) – 91%. xNN досяг найвищої точності 98,7% під час класифікації атак у другому наборі даних (CICIDS2019); згорткова нейронна мережа (CNN) досягла 86%, довготривала короткочасна пам'ять (LSTM) досягла 89,5%, а DNN досягла 83%. Запропоноване рішення перевершило існуючі аналоги за точністю виявлення та класифікації.

Список літератури

1. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. IEEE Internet Things J. 2021, 9, 616–632.

2. Oucheikh, R.; Fri, M.; Fedouaki, F.; Hain, M. Deep Real-Time Anomaly Detection for Connected Autonomous Vehicles. Procedia Comput. Sci. 2020, 177, 456–461.