ДОДАТОК А ПРИЗЕНТАЦІЯ

Інформаційна система виявлення шкідливого трафіку в мережах 5G

з використанням методів штучного інтелекту

Магістрант: Коржов Марко Сергійович
Науковий керівник: Поплавський О.А.

КНУБА, група ІСТм-24

Київ, 2025

1

Актуальність дослідження

- Мережі 5G розвиваються стрімкими темпами, але водночас створюють розширену поверхню атак
- Традиційні методи виявлення загроз недостатньо ефективні для захисту мереж п'ятого покоління
- Штучний інтелект дозволяє виявляти як відомі, так і нові форми атак у режимі реального часу
- Комплексна система захисту є критично важливою для операторів мобільного зв'язку та критичної інфраструктури

2

Мета та завдання

Мета:

Розробка архітектури та реалізація інформаційної системи виявлення шкідливого трафіку в мережах 5G з використанням методів ШІ

Ключові завдання:

- Аналіз архітектури мереж 5G та векторів атак
- Вибір оптимальних алгоритмів машинного навчання (RF, ANN, KNN)
- Розробка та тестування інформаційної системи
- Оцінка ефективності та порівняння з існуючими рішеннями

3

Архітектура мереж 5G

Ключові компоненти:

- RAN (мережа радіодоступу)
- Core Network (базова мережа)
- Data Networks
- UE (обладнання користувача)

Характеристики:

- Швидкість: до 10 Гбіт/с
- Затримка: 1-2 мс
- Частоти: 1 ГГц - 100 ГГц
- Три діапазони: низький, середній, високий

4

Основні типи атак на мережи 5G

MITM атаки
Перехоплення комунікації між сторонами через експлуатацію протокольних вразливостей

DDoS атаки
Перевантаження мережі масивним потоком запитів з множинних джерел

Сигнальні шторми
Перевантаження мережі надмірною кількістю сигнальних повідомлень

Фішинг
Соціальна інженерія для отримання конфіденційної інформації

Вимоги до доступу
Несанкціоновані спроби доступу через компрометацію облікових записів

Шкідлив ПО
Вірусні програми, тройани, програми-здирники

5

Використані методи ШІ

Random Forest
- Ансамбль дерев рішень
- Обробка складних даних
- Висока точність
- Стійкість до шуму

Нейронні мережі (ANN)
- Багатошарова архітектура
- Розпізнавання складних залежностей
- Адаптивність
- Висока гнучкість

k-Nearest Neighbors
- Простий та ефективний
- Класифікація за схожістю
- Немає навчання
- Швидка класифікація

6

Архітектура інформаційної системи

Компонент	Функція	Технологія
Data Collector	Захоплення трафіку	Python, libpcap
Preprocessing Engine	Нормалізація даних	Pandas, NumPy
RF Classifier	Класифікація (RF)	scikit-learn
ANN Classifier	Класифікація (ANN)	TensorFlow/Keras
Ensemble Engine	Комбінація результатів	Python
Alert Generator	Формування оповіщень	SMTP, SMS API
Web Dashboard	Візуалізація даних	Flask, React.js
Event Logger	Зберігання подій	PostgreSQL, MongoDB

7

Датасет 5G-NIDD

Загальні характеристики:

- Реальні дані мережи 5G
- Нормальний та аномальний трафік
- Багатокласова класифікація
- Дотримує NIDD формат

Класи атак:

- Benign (нормальний трафік)
- DDoS/DoS атаки
- Port Scans
- Інші типи атак

Ознаки (features): IP адреси, портові номери, протоколи, розміри пакетів, часові інтервали, BPS, PPS та інші статистичні параметри мережевих потоків

8

Результати: Random Forest

Метрика	Значення	Опис
Accuracy	**96.2%**	Загальна точність класифікації
Precision	**94.8%**	Точність позитивних прогнозів
Recall	**95.1%**	Повнота виявлення атак
F1-Score	**94.9%**	Гармонійна середина точності та повноти
ROC-AUC	**0.982**	Площа під кривою ROC

Час класифікації: ~12 мс на один потік трафіку | Час навчання: ~45 хвилин на датасеті 500K зразків

9

Результати: Штучні нейронні мережі

Метрика	Значення	Опис
Accuracy	**97.1%**	Найвища точність серед моделей
Precision	**96.3%**	Мінімум помилкових спрацювань
Recall	**96.8%**	Виявляє більшість атак
F1-Score	**96.5%**	Найкращий збалансований результат
ROC-AUC	**0.991**	Найвища чутливість/специфічність

Час класифікації: ~8 мс на один потік | Час навчання: ~90 хвилин | Архітектура: 3 приховані шари (128, 64, 32 нейрони)

10

Результати: k-Nearest Neighbors

Метрика	Значення	Опис
Accuracy	**94.5%**	Гарна точність, простий алгоритм
Precision	**92.7%**	Помірна точність позитивних
Recall	**93.9%**	Залежить від k та розподілу даних
F1-Score	**93.3%**	Збалансований результат
ROC-AUC	**0.967**	Добрий рівень дискримінації

Час класифікації: ~18 мс на один потік (без предварительного навчання) | Параметр k=5 обраний оптимально | Недолік: повільна класифікація при великому датасеті

11

Порівняння результатів алгоритмів

Метрика	Random Forest	ANN	KNN
Accuracy	96.2%	97.1% ★	94.5%
Precision	94.8%	96.3%	92.7%
Recall	95.1%	96.8%	93.9%
F1-Score	94.9%	96.5%	93.3%
ROC-AUC	0.982	0.991 ★	0.967
Швидкість класиф.	12 мс	8 мс ★	18 мс

★ ANN демонструє найкращі результати за більшістю метрик, особливо за точністю та швидкістю класифікації

12

Ефективність інформаційної системи

Продуктивність:

- Затримка обробки: ~110 мс
- Пропускна здатність: 100K потоків/сек
- Доступність системи: 99.8%
- Час виявлення: середньо 8-12 мс

Точність та надійність:

- Загальна точність: 97.1%
- Помилкові спрацювання: 3.2%
- Пропущені атаки: 2.9%
- ROC-AUC: 0.991 (відмінний)

13

Порівняння з аналогічними рішеннями

Характеристика	Наша система	Snort IDS	Suricata	Zeek
Точність (5G)	**97.1%**	78%	82%	85%
Виявлення аномалій	**Так (ШІ)**	Ні	Обмежено	Залежить від конфіг
Адаптивність	**Висока**	Низька	Помірна	Помірна
Затримка (мс)	**~8-12**	~20-30	~15-25	~50-100
Ліцензування	**Комерційне**	Комерційне	Open Source	Open Source

14

Основні висновки

- Розроблена інформаційна система успішно поєднує три алгоритми машинного навчання для виявлення шкідливого трафіку в мережах 5G
- Штучні нейронні мережи показали найкращу продуктивність (точність 97.1%, ROC-AUC 0.991) серед досліджених алгоритмів
- Система демонструє суттєву перевагу над традиційними інструментами IDS за точністю та адаптивністю до нових типів атак
- Ансамблевий підхід до класифікації підвищує надійність та зменшує помилкові спрацювання
- Середня затримка обробки (110 мс) задовольняє вимоги для мереж 5G

15

Рекомендації та подальшість

Рекомендації для розгортання:

- Впровадження системи в критичних точках мережевої інфраструктури операторів
- Інтеграція з існуючими SIEM та управління безпекою рішеннями
- Регулярне оновлення моделей машинного навчання на основі новітніх даних про атаки

Напрями подальшого розвитку:

- Впровадження глибокого навчання (LSTM, GRU) для аналізу часових послідовностей
- Розвиток federated learning для розподіленого навчання на даних операторів
- Розширення до виявлення невідомих атак через методи transfer learning

16

Дякую за увагу!

Коржов Марко Сергійович

Кваліфікаційна робота на здобуття ступеня магістра

КНУБА, факультет Автоматизації та інформаційних технологій

Київ, 2025

17