УДК 004.056.5:004.89

МЕХАНІЗМИ ВИЯВЛЕННЯ АНОМАЛІЙ В ТРАФІКУ IOT: ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ЗАПОБІГАННЯ ВТОРГНЕННЯМ

Нежуренко Олександр Григорович,
к.т.н., старший викладач кафедри комп'ютерних наук
та інформаційних технологій,
Житомирський державний університет імені Івана Франка

Анотація: Стаття досліджує виклики кібербезпеки IoT через зростання кількості пристроїв із обмеженими ресурсами та вразливістю до атак, таких як DDoS. Мета – аналіз методів машинного навчання для виявлення аномалій у трафіку IoT, демонстрація їхньої ефективності та практичної реалізації, зокрема через автоенкодер із LSTM і механізмом уваги в Google Colab. Результати показують високу загальну точність 0.953 із recall 1.00 для нормального трафіку та 0.52 для аномального, вказуючи на потребу оптимізації для незбалансованих даних. Висновок: методи машинного навчання ефективні для захисту IoT, але потребують вдосконалення чутливості до аномалій і адаптації до реальних умов.

Ключові слова: IoT-кібербезпека, виявлення аномалій, машинне навчання, автоенкодер, DDoS-атаки.

Стрімкий розвиток інтернету речей (IoT) призводить до експоненціального зростання кількості підключених пристроїв, що створює нові виклики для забезпечення кібербезпеки. Мережі IoT характеризуються високою гетерогенністю пристроїв, обмеженими обчислювальними ресурсами та складністю традиційних методів захисту. Зловмисники активно використовують вразливості IoT-пристроїв для здійснення різноманітних кіберзагроз, включаючи DDoS-атаки, вторгнення в мережу та компрометацію конфіденційних даних. Традиційні системи виявлення вторгнень (IDS)

виявляються неефективними у динамічному середовищі IoT через складність виявлення аномальної поведінки серед великих обсягів гетерогенного трафіку. Особливу складність становить виявлення невідомих атак та адаптація до нових типів загроз у реальному часі. Класичні підходи, що базуються на сигнатурах відомих атак, не здатні ефективно протидіяти новим видам кіберзагроз. Крім того, обмежені обчислювальні ресурси IoT-пристроїв не дозволяють реалізувати складні алгоритми захисту безпосередньо на кінцевих пристроях, що вимагає розробки нових архітектурних рішень та методів розподіленого аналізу.

Метою дослідження є аналіз методів машинного навчання для виявлення аномалій у трафіку IoT, оцінка їх ефективності для запобігання вторгненням та демонстрація практичної реалізації.

Сучасні методи машинного навчання пропонують інноваційні рішення для виявлення аномалій у трафіку IoT. Федеративне навчання представляє особливо перспективний напрямок для забезпечення безпеки IoT-мереж через можливість децентралізованого навчання моделей без компрометації приватності даних. Reis, M. J. C. S. [1] пропонує систему Edge-FLGuard, яка реалізує трирівневу ієрархічну архітектуру для виявлення аномалій у реальному часі в 5G-IoT екосистемах. Система використовує легкі моделі глибокого навчання (автоенкодери та LSTM) на edge-вузлах, які навчаються локально та періодично синхронізуються через захищену федеративну координацію. Федеративний автоенкодер досягає F1-показника 0,89 та AUC-ROC 0,94, тоді як федеративна LSTM-модель демонструє ще кращі результати з F1-показником 0,91 та AUC 0,96, що значно перевершує локальні моделі.

Механізми уваги в глибокому навчанні відкривають нові можливості для аналізу мережевого трафіку IoT через здатність фокусуватися на найбільш релевантних характеристиках даних. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Morales-Reyes, A. [2] представляють attention-driven глибоку нейронну мережу, що використовує Scaled-Dot Product Attention та Word2Vec-подібні ембедінги для покращення якості виявлення аномалій. Цей підхід дозволяє створювати більш точні векторні представлення мережевого

трафіку, адаптуючи принципи обробки природної мови до аналізу кіберзагроз. Використання механізмів уваги забезпечує кращу інтерпретованість результатів та підвищує надійність виявлення складних атак.

Практична реалізація методів виявлення аномалій в IoT-мережах базується на моделі автоенкодера з LSTM і механізмом MultiHeadAttention, реалізованої в Google Colab, яка обробляє послідовності мережевого трафіку розміром (50, 20) із нормалізацією через StandardScaler. Модель навчається на нормальних даних (90% вибірки), використовуючи MSE як функцію втрат, і виявляє аномалії (наприклад, DDoS-атаки) шляхом аналізу помилок реконструкції з порогом на 95-му перцентилі. Механізм уваги з чотирма головами (key_dim=64) підвищує чутливість до складних часових патернів у трафіку, забезпечуючи загальну точність 0.953, recall 1.00 для нормального трафіку та 0.52 для аномального, що вказує на обмеження через незбалансованість даних і потребу в оптимізації порогу чи застосуванні методів балансування, таких як SMOTE (рис. 1):

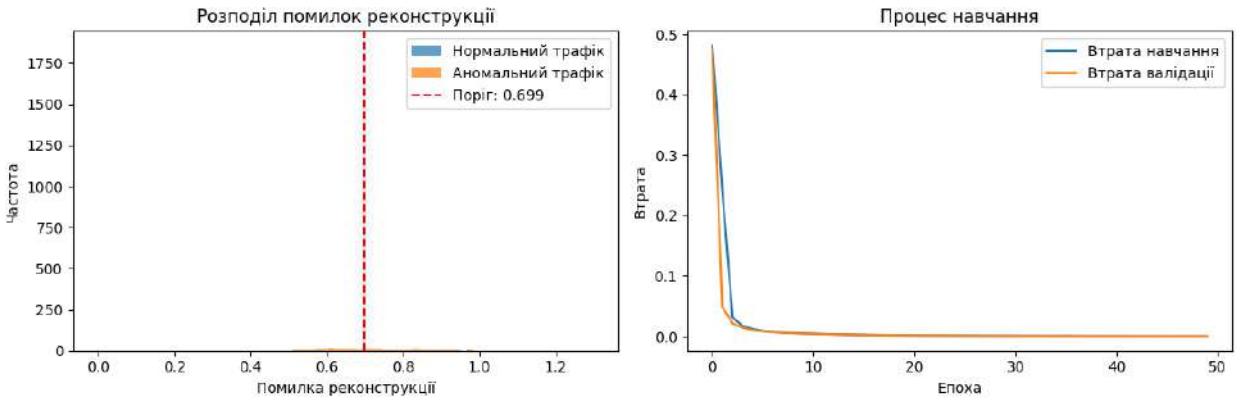

Рис. 1. Розподіл помилок реконструкції та поріг виявлення аномалій у трафіку IoT

Подальший розвиток систем виявлення аномалій в IoT-мережах передбачає інтеграцію пояснювального штучного інтелекту (XAI) для підвищення прозорості рішень та довіри користувачів. Важливим напрямком є розробка легких алгоритмів, адаптованих для роботи на edge-пристроях з обмеженими ресурсами. Федеративне навчання продовжує розвиватися в

напрямку підвищення стійкості до атак отруєння та забезпечення диференціальної приватності. Гібридні підходи, що поєднують різні методи машинного навчання, демонструють найбільш перспективні результати у досягненні високої точності виявлення при мінімальній кількості хибних спрацювань. Аналіз сучасних механізмів виявлення аномалій у трафіку IoT показує, що методи машинного навчання, зокрема глибоке навчання (автоенкодери, LSTM-мережі, механізми уваги), є найефективнішими для кібербезпеки IoT-екосистем, забезпечуючи високу точність виявлення відомих і невідомих атак. Федеративне навчання вирішує проблеми приватності даних і масштабованості, дозволяючи створювати децентралізовані системи захисту, які перевищують ефективність традиційних централізованих рішень.

Практичне впровадження цих технологій потребує врахування обмежень IoT-середовища: ресурсних обмежень пристроїв, динамічності мережевого трафіку та необхідності роботи в реальному часі. Оптимізація алгоритмів через відбір ознак і налаштування гіперпараметрів критично важлива для балансу між точністю виявлення та обчислювальною ефективністю. Майбутні дослідження мають зосередитися на розробці пояснювальних моделей, підвищенні стійкості до адверсарних атак і створенні адаптивних систем, здатних автоматично еволюціонувати для протидії новим типам загроз.

СПИСОК ЛІТЕРАТУРИ

1. Reis, M. J. C. S. (2025). Edge-FLGuard: A Federated Learning Framework for Real-Time Anomaly Detection in 5G-Enabled IoT Ecosystems. Applied Sciences, 15(12), 6452. DOI: https://doi.org/10.3390/app15126452 URL: https://www.mdpi.com/2076-3417/15/12/6452

2. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Morales-Reyes, A. (2025). Network traffic inspection to enhance anomaly detection in the Internet of Things using attention-driven Deep Learning. Integration, 103, 102398. DOI: https://doi.org/10.1016/j.vlsi.2025.102398 URL: https://www.sciencedirect.com/science/article/abs/pii/S0167926025000550