УДК 004.056

Методы машинного обучения для обнаружения сетевых аномалий в IoT-средах

Хабибуллин А.В., Залеткина В.В., Фронек П.А. (МИЭМ НИУ ВШЭ)
Научный руководитель – кандидат технических наук, профессор Авдошин С.М. (МИЭМ НИУ ВШЭ)

Введение. Инфраструктуры Интернета вещей (IoT) активно внедряются в промышленности, энергетике, транспорте, и «умных» городах. Рост количества подключенных устройств сопровождается увеличением числа уязвимостей и атак, что делает задачу обнаружения аномального поведения одной из ключевых проблем кибербезопасности [1]. Традиционные сигнатурные методы обнаружения вторжений ориентированы на заранее известные шаблоны атак и демонстрируют низкую эффективность при выявлении новых или модифицированных угроз.

В отечественных и зарубежных исследованиях все большее распространение получают методы машинного обучения, позволяющие строить модели нормального поведения устройств и автоматически фиксировать отклонения [2]. Однако практическое применение таких методов в IoT-средах осложняется ограниченными вычислительными ресурсами, высокой изменчивостью сетевого трафика и дисбалансом классов. В связи с этим актуальной является задача разработки подхода к выбору признаков и моделей машинного обучения, обеспечивающих высокую точность и устойчивость обнаружения аномалий.

Основная часть. В работе рассматривается подход к обнаружению сетевых аномалий IoT-устройств на основе анализа потоковых характеристик трафика и применения классических алгоритмов машинного обучения. В качестве исходных данных используются датасеты BoT-IoT, WUSTL-IIoT-2021 Dataset, IoT Network Industrial Dataset, содержащие как нормальный трафик, так и различные типы атак [3]. Также для аугментации данных была развернута изолированная лабораторная среда, состоящая из нескольких устройств Raspberry Pi 5, Wi-Fi точки доступа, атакующего узла и узла мониторинга.

Для решения задачи бинарной классификации исследуется применимость логистической регрессии, метода k ближайших соседей, случайного леса и градиентного бустинга. Сравнение моделей проводится по стандартным метрикам качествам, включая ROC-AUC, F1-score, Precision и Recall. Экспериментальные результаты показывают, что ансамблевые методы обеспечивают наилучшее соотношение точности и полноты обнаружения, а также минимальное количество ошибок классификации.

Предлагаемый подход не требует использования ресурсоемких признаков и может быть адаптирован для развертывания в реальных IoT-сетях.

Выводы. Разработан и обоснован подход к обнаружению сетевых аномалий IoT-устройств с использованием методов машинного обучения и унифицированного набора признаков. Показано, что применение ансамблевых алгоритмов позволяет достичь высокой точности выявления атак. Полученные результаты могут быть использованы при создании систем мониторинга и защиты IoT-инфраструктур. Перспективными направлениями дальнейших исследований являются расширение набора сценариев атак, внедрение интерпретируемых моделей и механизмов объяснимого искусственного интеллекта (XAI).

Список использованных источников:

1. Salayma M. Threat modelling in Internet of Things (IoT) environments using dynamic attack graph // Frontiers in the Internet of Things. – 2024. – Vol. 4. – Art. 1306465.
2. Alghanmi N., Alotaibi R., Buhari S. M. Machine Learning Approaches for Anomaly

Detection in IoT: An Overview and Future Research Directions // Wireless Personal Communications. – 2022. – Vol. 122. – P. 2309-2324.

3. Sasi T., Lashkari A. H., Lu R., Xiong P.A Comprehensive Survey on IoT Attack and Anomaly Detection // IEEE Internet of Things Journal. – 2023. – Vol. 10. – No. 5. – P. 4013-4038.