УДК 004.056

АЛГОРИТМ ОБНАРУЖЕНИЯ СКОМПРОМЕТИРОВАННЫХ IOT-УСТРОЙСТВ В КОРПОРАТИВНОЙ СЕТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ DDOS АТАК

Уголев М. А.[1], Бердичевский А. С.[1]
Научный руководитель – канд. техн. наук, доцент Левко И. В.[1]
[1]Университет ИТМО
matthew.u@itmo.ru

Работа выполнена в рамках темы ВКР: «Разработка алгоритма обнаружения скомпрометированных IoT-устройств в корпоративной сети коммерческой организации в условиях DDoS атак».

Введение

Активное внедрение интернета вещей в корпоративный сектор сопровождается ростом инцидентов, связанных с компрометацией таких устройств. Согласно данным Лаборатории Касперского, количество атак на IoT-устройства за последние года увеличилось более чем в два раза [1]. Наибольшую угрозу представляет использование скомпрометированных устройств в сети для последующей реализации DDoS атак. Усугубляется все тем, что традиционные системы обнаружения вторжений (IDS), основанные на сигнатурном анализе, теряют эффективность в условиях сетевого шума. Существующие поведенческие детекторы на основе методов машинного обучения дают высокий процент ложных срабатываний при флуде, так как трафик самой DDoS атаки маскирует тонкие аномалии, характерные для работы ботов. Таким образом, актуальность работы обусловлена необходимостью создания алгоритма, сохраняющего работоспособность в условиях зашумления канала.

Основная часть

В основе предлагаемого решения лежит гибридный алгоритм, сочетающий адаптивную фильтрацию трафика и поведенческий анализ на основе эталонных профилей устройств.

Первый этап реализуется посредством преобразования временных рядов сетевых потоков. Для каждого потока формируется временной ряд, отражающий интенсивность поступления пакетов во времени. В условиях DDoS атаки временные ряды содержат высокочастотные всплески, которые маскируют низкочастотные периодические сигналы, характерные для взаимодействия скомпрометированных устройств. Далее исходный ряд раскладывается на высокочастотную и низкочастотную составляющие. Высокочастотная составляющая, соответствующая шуму DDoS атаки, отбрасывается, а по низкочастотной составляющей восстанавливается очищенный временной ряд [2].

На втором этапе выполняется поведенческий анализ каждого IoT-устройства на основе его эталонного профиля. Для формирования профилей в период штатной работы сети собирается статистика по пакетной активности каждого устройства. В профиль включаются: межпакетные интервалы, распределение размеров пакетов, соотношение входящего и исходящего трафика, наборы портов назначения и флаги TCP. Для описания нормальных состояний применяется метод одноклассовой классификации [3]. Его суть заключается в построении модели, которая описывает область нормального функционирования IoT-устройства на основе набора признаков, извлеченных ранее. В процессе детектирования каждое новое наблюдение сравнивается с этой моделью: если поведение устройства отклоняется от эталонного, оно классифицируется как подозрительное.

Выводы

Практическая значимость работы состоит в возможности интеграции алгоритма в существующие SIEM системы коммерческих организаций в качестве дополнительного модуля анализа сетевого трафика. Своевременное выявление скомпрометированных IoT-устройств до их использования в составе ботнетов позволяет снизить репутационные и финансовые риски компании. Внедрение подобных решений является актуальной задачей для обеспечения информационной безопасности корпоративных сетей.

Дальнейшие исследования планируется направить на адаптацию алгоритма к работе с шифрованным трафиком и снижение требований к вычислительным ресурсам.

Литература

1. Kaspersky releases overview of IoT-related threats in 2023 [Электронный ресурс]. – Режим доступа: https://usa.kaspersky.com/about/press-releases/kaspersky-releases-overview-of-iot-related-threats-in-2023 (Дата обращения 10.02.2026).
2. Kotenko I., Saenko I., Bortniker P. Detecting Attacks against Industrial Internet of Things by Integrating Wavelet and Statistical Analysis // IEEE Xplore. — 2025. [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/11028572 (дата обращения 10.02.2026).
3. Zahoor A., Abbasi W., Muhhamad Z., Aljohni A. Robust IoT security using isolation forest and one class SVM algorithms / Md. A. Hossain [et al.] // Scientific Reports. — 2025. [Электронный ресурс]. – Режим доступа: https://www.nature.com/articles/s41598-025-20445-4 (дата обращения 10.02.2026).
4. ПРОБЛЕМНО-ОРИЕНТИРОВАННАЯ СИСТЕМА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА МНОГОВЕКТОРНЫЕ АТАКИ В ДЕЦЕНТРАЛИЗОВАННОЙ СРЕДЕ ИНТЕРНЕТА ВЕЩЕЙ // Вопросы кибербезопасности. — 2025. [Электронный ресурс]. – Режим доступа: https://cyberrus.info/wp-content/uploads/2025/12/vokib-2025-6-st07-s069-080.pdf (дата обращения 11.02.2026).