Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056.5

Шаронова Елена Ивановна

Методика обнаружения DDoS-атак, основанная на машинном обучение

АВТОРЕФЕРАТ
на соискание степени магистра

по специальности 1-98 80 01 «Информационная безопасность»

Научный руководитель

Петров Сергей Николаевич
кандидат технических наук,
доцент

Минск 2024

ВВЕДЕНИЕ

Одним из перспективных подходов к обнаружению DDOS-атак является использование методов машинного обучения. Машинное обучение позволяет анализировать большие объемы данных и выявлять аномалии, которые могут свидетельствовать о проведении DDOS-атаки. Существует несколько подходов к использованию машинного обучения для обнаружения DDOS-атак. Например, можно обучить модель на основе данных о нормальном трафике в сети и затем использовать эту модель для выявления отклонений от нормы, которые могут свидетельствовать о DDOS-атаке.

Также можно использовать методы классификации, регрессии и кластеризации для выявления аномального поведения в сети. Однако, следует отметить, что использование машинного обучения для обнаружения DDOS-атак также имеет свои ограничения и вызовы. Например, необходимо постоянно обновлять модели машинного обучения, чтобы они могли распознавать новые виды атак. Также важно учитывать возможность ложных срабатываний и минимизировать их количество. В целом, использование методов машинного обучения для обнаружения DDOS-атак представляет собой перспективный подход, который может значительно улучшить защиту сетей от этого типа угрозы. Однако, необходимо постоянно совершенствовать и адаптировать эти методики.

Тема методики обнаружения DDOS-атак является очень актуальной в современном мире, так как DDOS-атаки продолжают быть серьезной угрозой для онлайн-безопасности и стабильности сетей. DDOS-атаки могут привести к недоступности веб-сайтов, сбоям в работе онлайн-сервисов и значительным финансовым потерям для компаний. Поэтому разработка эффективных методик обнаружения и защиты от DDOS-атак является приоритетной задачей для специалистов по информационной безопасности.

Целью диссертационной работы является создание программного модуля для обнаружения признаков DDoS-атаки IoT-ботнетов с использованием машинного обучения.

Для достижения указанной цели необходимо решить следующие задачи:

1. Выполнить анализ трафика Интернета вещей и моделей сетевого поведения, характерных для Интернета вещей.
2. Изучить алгоритмы машинного обучения, которые могут быть использованы для обнаружения признаков DDoS атак.
3. Провести анализ датасетов, используемых для обучения моделей обнаружению признаков DDoS атак и сформировать обучающие и тестовые выборки.
4. Провести сравнение эффективности алгоритмов машинного обучения в обнаружении признаков DDoS атак IoT ботнетов.
5. Разработать блок-схему программного модуля обнаружения признаков DDoS атак IoT ботнетов и выполнить его программную реализацию
6. Провести испытание разработанного модуля.

Объект исследования: модели машинного обучения.

Предмет исследования: метрики оценки моделей машинного обучения Accuracy, Recall, Precision, F1-Score.

Экспертиза диссертации на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 14.06.2024 г. показала корректность использования заимствованных материалов (оригинальность составляет 71.79 %).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи работы

Целью диссертационной работы является создание программного модуля для обнаружения признаков DDoS-атаки IoT-ботнетов с использованием машинного обучения.

В соответствии с поставленной целью, в работе сформированы и решены следующие задачи:

– Выполнить анализ трафика Интернета вещей и моделей сетевого поведения, характерных для Интернета вещей.

– Изучить алгоритмы машинного обучения, которые могут быть использованы для обнаружения признаков DDoS атак.

– Провести анализ датасетов, используемых для обучения моделей обнаружению признаков DDoS атак и сформировать обучающие и тестовые выборки.

– Провести сравнение эффективности алгоритмов машинного обучения в обнаружении признаков DDoS атак IoT ботнетов.

– Разработать блок-схему программного модуля обнаружения признаков DDoS атак IoT ботнетов и выполнить его программную реализацию

– Провести испытание разработанного модуля.

Положения, выносимые на защиту

– результаты исследования эффективности различных алгоритмов классификации для обнаружения DDoS атак IoT ботнетов;

– архитектура программного модуля обнаружения DDoS атаки.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует положениям главы 8 подпрограммы «Информационная безопасность и цифровое доверие» Государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы, утвержденной постановлением Совета Министров Республике Беларусь от 2 февраля 2021 г. № 66.

В диссертации поставлена и решена актуальная задача по созданию программного модуля для обнаружения признаков DDoS-атаки IoT-ботнетов с использованием машинного обучения.

Научная новизна заключается в проведении сравнительного анализа эффективности алгоритмов классификации для обнаружения признаков DDoS-атак IoT-ботнетов. Показан значительный разброс результатов классификации в зависимости от используемого датасета, что говорит о важности корректного подбора данных для обучения и тестирования моделей машинного обучение. По результатам тестирования лучшие результаты показал алгоритм SVM с ядром Linear.

Практическая ценность работы состоит в разработке программного модуля для обнаружения признаков DDoS-атаки IoT-ботнетов на основе алгоритма SVM на языке программирования Python.

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в: изучении существующих подходов обнаружения признаков DDoS атак; изучении принципов работы IoT-устройств и особенностей трафика IoT-ботнетов; работы с инструментами и сервисами, предназначенными для обучения и тестирования моделей машинного обучения; обучении и тестировании моделей для выявления аномалий сетевого трафика; разработке программного модуля.

Определение цели и задач исследований, интерпретация и обобщение полученных результатов проводились с научным руководителем, кандидатом технических наук, доцентом С.Н. Петровым.

Апробация результатов диссертации

Теоретические результаты диссертационных исследований представлены в виде тезисов на следующих научных конференциях:

– XIX Международная научно-техническая конференция «Современные средства связи», Минск, 2023 года;

– 59-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2023 г;

– XXI Белорусско-Российской научно-технической конференции «Технические средства защиты информации», Минск, 6 июня 2023 ;

– 60-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2024 г;

– XXVIII Международная научно-практическая конференция ЧУВО, «Инновационное развитие и структурная перестройка экономики», Минск 19 апреля 2024г.;

– XIV Международная научно-практическая конференция БИП, Минск, 18 апреля 2024 г.

– XXII Белорусско-Российской научно-технической конференции «Технические средства защиты информации», Минск, 6 июня 2023.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 8 печатных работ в сборниках: 59-я конференция аспирантов, магистрантов и студентов», 60-ой конференции аспирантов, магистрантов и студентов БГУИР,XIX Международная научно-техническая конференция «Современные средства связи, XXI Белорусско-Российской научно-технической конференции, XXVIII Международная научно-практическая конференция ЧУВО, XIV Международная научно-практическая конференция БИП, XXII Белорусско-Российской научно-технической конференции.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех разделов, заключения, списка использованных источников, списка собственных источников, приложений. Полный объем диссертационной работы составляет 75 страницы, включая 41 иллюстрацию, список использованных источников из 18 наименований, список собственных публикаций из 8 наименований, 5 приложений объемом 14 страниц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение содержит краткое описание работы и обоснование необходимости исследований.

В первом разделе проведен анализ существующих Dos и DDoS атак, классификация DDoS-атак и защита от них, проведен анализ интернета вещей, выделены классификаторы обычного и DDos-трафика.

Второй раздел содержит анализ существующих датасетов для обнаружения DDos-атак, определена методика исследования эффективности алгоритмов классификации для обнаружения признаков DDoS атаки Приведены алгоритмы машинного обучения, используемые в задачах классификации. Описаны угрозы, создаваемые IoT ботнетами Дана Оценка эффективности алгоритмов классификации для обнаружения признаков DDoS атак. Исследования алгоритмов классификации представлены в таблицах.

В третьем разделе представлена программная реализация модуля для обнаружения DDoS-атак. Приведены режимы работы модуля, схема работы модуля обнаружения DDoS-атак, проведен анализ практического применения разработанного модуля обнаружения, описывается процесс разработки имитационной модели сети для возможности реализации DDoS-атаки на целевую машину и проверка работоспособности разработанного модуля. Проведен анализ работы модуля. Блок-схема и листинг кода модуля представлены в Приложениях.

В заключении сформулированы основные выводы по диссертационной работе и представлены полученные результаты.

ЗАКЛЮЧЕНИЕ

В заключении исследования можно отметить следующее, машинное обучение представляет собой эффективный инструмент для обнаружения DDoS атак благодаря способности алгоритмов обучения находить зависимости в данных и распознавать аномалии в поведении сетевого трафика. Важно учитывать необходимость постоянного обновления и настройки моделей машинного обучения для адаптации к новым видам DDoS атак и изменениям в структуре сетей.

Проведен анализ видов атак типа «отказ в обслуживании» (DoS, DDoS) и их последствий. Рассмотрено применение ботнетов, совокупности устройств, подключенных через Интернет, на каждом из которых работает один или серия ботов, для проведения DDoS атак. Рассмотрены ботнеты, построенные на основе IoT устройств. Проведен анализ признаков сетевого трафика IoT устройств, которые используются для обнаружения аномалий и, соответственно, обнаружения DDoS атак.

Проведен анализ открытых датасетов для обнаружения DDoS атак IoT-ботнетов (Edge-IIoTset, N-BaIoT, TON_IoT и CIC-DdoS2019). На основе открытых датасетов созданы обучающие и тестовые выборки данных. Анализ открытых источников показал, что не существует единого и рекомендованного к использованию в качестве референсного набора данных для обучения моделей обнаружению DDoS-атак IoT-ботнетов.

Проведен сравнительный анализ эффективности алгоритмов классификации для обнаружения признаков DDoS-атак IoT-ботнетов с использованием сервиса Google Colab. Показан значительный разброс результатов классификации в зависимости от используемого датасета, что говорит о важности корректного подбора данных для обучения и тестирования моделей машинного обучение. По результатам тестирования лучшие результаты показал алгоритм SVM с ядром Linear

Разработан программный модуль для обнаружения признаков DDoS-атаки IoT-ботнетов на основе алгоритма SVM (linear) с использованием языка программирования Python. Проведено тестирование программного модуля с использованием имитационной модели сети. DDoS атака эмулировалась с помощью утилиты hping3. Испытания показали результативность модуля.

Представлена схема создания датасетов для обучения моделей машинного обучения обнаружению DDoS атак IoT ботнетов.

В целом, применение методов машинного обучения для обнаружения DDoS атак имеет большой потенциал и требует дальнейших исследований и развития для повышения эффективности защиты информационных ресурсов от подобных угроз.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Шаронова Е.И. Обеспечение бесперебойной работы интегрированной информационной системы БГУИР / Петров С.Н., Матюшкин С.И., Шаронова Е.И. /В книге: Управление информационными ресурсами. Материалы XIX Международной научно-практической конференции. Минск, 2023. С. 249-251.

2–А. Шаронова, Е. И. Возможности машинного обучения для обнаружения DDoS атак - Machine learning capabilities for detecting DDoS attacks / Шаронова Е. И. // Информационная безопасность : сборник материалов 59-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 31–35.

3–А. Шаронова, Е.И. Обеспечение безопасности информационных систем университета / Е. И. Шаронова, С. И. Матюшкин // Технические средства защиты информации : тезисы докладов XXI Белорусско-российской научно-технической конференции, Минск, 6 июня 2023 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Т. В. Борботько [и др.]. – Минск, 2023. – С. 97–98.

4–А. Шаронова, Е.И. Модели обнаружения атрибутов кибернетических-атак с устройств IoT, А.Б. Гуринович, Шаронова Е.И // XXVIII Международная научно-практическая конференция «Инновационное развитие и структурная перестройка экономики»./ ЧУВО «Международный институт управления и предпринимательства» , Минск,2024

5–А. Шаронова, Е.И. Байесовский подход в обнаружение DDOS-атак Е.И. Шаронова, А.Б. Гуринович, // XIV Международная научно-практическая конференция БИП,Минск, 18 апреля 2024 г./ Университет права и социально информационных технологий, Минск, 2024

6–А. Шаронова, Е.И., Метрики для обнаружения DDoS-атак. Материалы 60-й юбилейной научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» Минск, 2024

7–А. Шаронова, Е.И. Защита информации в автоматизированных системах обработки информации. Габриелева Е.Г., Шаронова Е.И. //Материалы 60-й юбилейной научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» Минск, 2024

8–А. Шаронова, Е.И. Нормативные аспекты защиты информации государственных и коммерческих организаций/ Е. И. Шаронова, В. М. Хиль //

Технические средства защиты информации: тезисы докладов XXII Белорусско-российской научно-технической конференции, Минск, 12 июня 2024 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Т. В. Борботько [и др.]. – Минск, 2024. – С. 95.