УДК 004.021

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ DDOS-АТАК НА УРОВНЕ ПРИЛОЖЕНИЙ

Ефимов В. Е. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Менщиков А.А.
(Университет ИТМО)

Введение. Веб-приложения стали неотъемлемой частью современной инфраструктуры, обеспечивая доступ к широкому спектру сервисов. Однако, их доступность и производительность находятся под постоянной угрозой DDoS-атак (Distributed Denial of Service). Традиционные методы защиты, такие как сигнатурный анализ и фильтрация по IP-адресам, оказываются неэффективными против современных атак, характеризующихся высокой сложностью и адаптивностью. Атаки на уровне приложений имеют ряд особенностей, которые отличают их от других атак. Они осуществляются с помощью легитимных HTTP-пакетов. Запрос атаки практически неотличим от обычного запроса. Единственное различие заключается в намерении, а не в содержимом.

В результате большинство сетевых пакетных фильтров и даже некоторые брандмауэры прикладного уровня не могут эффективно обнаружить эти атаки. Необходимо разрабатывать интеллектуальные системы, способные выявлять аномальное поведение на уровне приложений, даже если атака маскируется под легитимный трафик. В данной работе предлагается подход к обнаружению DDoS-атак, основанный на применении графовых нейронных сетей (GNN).

Основная часть. В данной работе предложен и реализован подход к обнаружению DDoS-атак на уровне приложений с использованием графовых нейронных сетей (GNN).

Разработка включала несколько ключевых этапов. На первом этапе создан специализированный тестовый стенд, имитирующий работу веб-приложения и позволяющий генерировать как легитимный трафик, так и различные типы DDoS-атак (HTTP Flood, Slowloris и др.). Этот стенд стал цифровым полигоном для сбора данных, необходимых для обучения и тестирования модели.

На втором этапе сетевой трафик был преобразован в графовую структуру, что позволило GNN анализировать трафик не как последовательность отдельных событий, а как взаимосвязанную систему, учитывая как локальные, так и глобальные взаимодействия.

На третьем этапе разработана и обучена GNN-модель, способная классифицировать трафик как легитимный или атакующий. Особое внимание уделено архитектуре сети.

На заключительном этапе проведена серия экспериментов для оценки эффективности GNN-модели и ее сравнение с другими существующими классическими методами машинного обучения.

Выводы. В результате работы разработана практическая GNN-модель, которую можно использовать для обнаружения DDoS-атак на уровне приложений. Полученные результаты могут быть использованы для дальнейших исследований в области применения машинного обучения для обеспечения сетевой безопасности.

Список использованных источников:

1. Carela Español D. Graph neural networks for dynamic network traffic classification : дис. – Universitat Politècnica de Catalunya, 2024.
2. Zhou J. et al. Automating botnet detection with graph neural networks. arXiv 2020 //arXiv preprint arXiv:2003.06344.
3. Marimuthu S. Detecting Application Layer DDoS Attacks Among Microservices Using Spatio-Temporal Graph Convolution Networks : дис. – California State University, Northridge, 2023.