УДК 004.056

Расеева Екатерина Викторовна
ст. преподаватель, кафедра программной инженерии,
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Захватова Екатерина Михайловна
студент 4 курса, кафедра программной инженерии,
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
zakhvatovaeka@mail.ru

ПРОГНОЗИРОВАНИЕ DDOS-АТАК НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ СЕТЕВОГО ТРАФИКА

Статья посвящена прогнозированию DDoS-атак с использованием анализа временных рядов сетевого трафика. Рассматриваются этапы обработки данных, статистические и нейросетевые методы, а также современные тенденции применения искусственного интеллекта в кибербезопасности.

Ключевые слова: DDoS, временные ряды, сетевой трафик, прогнозирование, нейронные сети, кибербезопасность.

Predicting DDoS attacks based on network traffic time series analysis

The article is devoted to the forecasting of DDoS-attacks using the analysis of time series of network traffic. The stages of data processing, statistical and neural network methods, as well as modern trends in the application of artificial intelligence in cybersecurity are considered.

Keywords: DDoS, time series, network traffic, forecasting, neural networks, and cybersecurity.

Современные информационные системы подвергаются растущему числу кибератак, среди которых особое место занимают распределённые атаки типа «отказ в обслуживании» (DDoS). Их опасность заключается в масштабности и сложности предотвращения: злоумышленники используют тысячи скомпрометированных устройств, создавая мощные потоки трафика, которые перегружают ресурсы целевой системы.

По данным аналитиков, количество DDoS-атак ежегодно увеличивается, и они становятся всё более изощрёнными за счёт применения новых протоколов, методов маскировки и автоматизированных инструментов. В этих условиях прогнозирование атак на основе анализа временных рядов сетевого трафика приобретает ключевое значение для обеспечения устойчивости и безопасности сетевых инфраструктур.

Временной ряд сетевого трафика представляет собой хронологически упорядоченные наблюдения, отражающие динамику параметров сети — объёма пакетов, IP-адресов, числа подключений и т.д. Их анализ позволяет выявить скрытые закономерности, обнаружить аномалии и прогнозировать развитие событий.

DDoS-атака инициируется с использованием бот-сетей — совокупности заражённых устройств, распределённых по всему миру. В отличие от одиночных DoS-атак, она обладает значительно большей мощностью и сложнее поддаётся блокировке.

Анализ сетевого трафика включает мониторинг, захват, обработку и интерпретацию данных. Его задачи охватывают диагностику и устранение сбоев в сети, оптимизацию протоколов и их тестирование, выявление аномалий и атак, а также классификацию трафика для оптимального распределения ресурсов.

Существует несколько основных подходов. Один из них основан на использовании программных анализаторов, таких как Wireshark, позволяющих захватывать пакеты и изучать их структуру. Другой подход связан с применением статистических методов, включая математическое моделирование временных рядов, где выделяются тренды, сезонные колебания и случайные компоненты. Более современные решения основаны на нейронных сетях, которые обеспечивают возможность выявления сложных нелинейных зависимостей и более точного прогнозирования.

Для обучения моделей временной ряд обычно сегментируется на окна фиксированной длины. Сеть обучается предсказывать следующее значение

ряда, что позволяет формировать прогнозы поведения трафика и выявлять нетипичные пики активности.

Процесс анализа временных рядов сетевого трафика представляет собой последовательность шагов, направленных на преобразование «сырых» данных в осмысленную информацию, пригодную для прогнозирования и обнаружения атак. Всё начинается со сбора данных при помощи специальных инструментов, таких как NetFlow, sFlow или Wireshark. Эти средства позволяют фиксировать сетевые пакеты и агрегировать их по временным интервалам, что даёт возможность отслеживать интенсивность обмена трафиком.

Далее данные проходят предварительную обработку: из потока удаляются дубликаты и шумы, осуществляется нормализация показателей, а пропуски заполняются статистическими методами или исключаются из анализа. После этого выделяются ключевые признаки — объём и частота пакетов, распределение IP-адресов, популярные порты и использование необычных протоколов. Именно эти характеристики позволяют обнаруживать аномалии, связанные с нетипичной сетевой активностью.

Затем наступает этап моделирования временных рядов. Здесь применяются как классические статистические подходы (например, ARIMA), так и методы машинного обучения. Особое внимание уделяется трём компонентам ряда: долгосрочному тренду, повторяющимся сезонным колебаниям и случайным изменениям. В случае значительных расхождений между прогнозируемыми и фактическими значениями фиксируется потенциальная DDoS-атака.

Полученные результаты представляются в виде графиков и диаграмм, что облегчает интерпретацию и позволяет наглядно выявлять опасные всплески нагрузки. В современных условиях этот процесс всё чаще автоматизируется и интегрируется в системы управления информационной безопасностью (SIEM и SOC). Это обеспечивает не только прогнозирование возможных атак, но и их оперативное отражение в реальном времени.

Классические статистические модели остаются актуальными, однако они имеют ограничения при работе с нелинейными и многомерными данными. Поэтому в последние годы активно развиваются гибридные подходы, совмещающие методы машинного обучения, нейросетей и больших данных (Big Data).

Особое внимание уделяется глубоким нейронным сетям (LSTM, GRU), которые эффективно работают с последовательностями; гибридным моделям, объединяющим статистический анализ и нейросетевые алгоритмы; онлайн-обучению, при котором модели подстраиваются к новым данным в реальном времени; а также интеграции с системами SIEM, что позволяет не только прогнозировать атаки, но и автоматически реагировать на них.

Таким образом, прогнозирование на основе временных рядов постепенно эволюционирует в сторону интеллектуальных систем, способных адаптироваться к изменяющейся структуре атак.

Прогнозирование DDoS-атак на основе анализа временных рядов сетевого трафика является одним из ключевых направлений обеспечения кибербезопасности. Использование статистических методов позволяет выявлять закономерности и тренды, тогда как нейронные сети обеспечивают высокую точность при работе со сложными нелинейными данными.

Будущее за гибридными решениями, сочетающими математическое моделирование, искусственный интеллект и обработку больших данных. Такие системы способны не только прогнозировать атаки, но и оперативно реагировать на них, снижая риск перебоев в работе критически важных сетевых сервисов.

Список литературы

1. DDOS-атаки и методы борьбы с ними / А. О. Голубятников: [Электронный ресурс] // Режим доступа:

https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi?ysclid=mfkmxfkmuu263605851

2. Основные методы анализа сетевого трафика / А. М. Гладких: [Электронный ресурс] // Режим доступа: https://cyberleninka.ru/article/n/osnovnye-metody-analiza-setevogo-trafika?ysclid=mfkmvkztuu24768845
3. Временные ряды и требования к ним / Н. В. Кержаков: [Электронный ресурс] // Режим доступа: https://cyberleninka.ru/article/n/vremennye-ryady-i-trebovaniya-k-nim
4. Обзор методов прогнозирования временных рядов с помощью искусственных нейронных сетей / И. С. Дауб, В. А. Фатеев: [Электронный ресурс] // Режим доступа: https://cyberleninka.ru/article/n/obzor-metodov-prognozirovaniya-vremennyh-ryadov-s-pomoschyu-iskusstvennyh-neyronnyh-setey?ysclid=mfkmrdvw6w450183260