Impact Factor: 9.9 ISSN-L: 2544-980X

Обнаружение Ddos-Атак В Реальном Времени

Мухтаров Фаррух Мухаммадович [1], *Абдулхамидова Нилуфар Кахрамоновна* [2]

Аннотация: Атаки типа "распределенного отказа в обслуживании" являются одним из самых частых и вредоносных типов опасностей для современных компьютерных сетей. Такого типа атаки нацелены на перенапряжение возможностей целевой системы или сети, что вызывает потерю доступности услуг. В данной статье анализируются способы и стратегии, применяемые для выявления атак типа DDoS в режиме реального времени. Обзор охватывает классические подходы к изучению потока данных в сети, плюс актуальные разработки, основанные на алгоритмах искусственного интеллекта, которые направлены на увеличение эффективности и ускорение выявления. Анализируются виды атак типа "DDoS", методы их обнаружения, а также использование разнообразных технологий для сокращения вреда и усиления стойкости к подобным опасностям.

Ключевые слова: DDoS-атаки, сетевой трафик, машинное обучение, обнаружение атак, безопасность, реальное время, анализ трафика.

Введение. Атаки типа *«отказ в обслуживании» (Distributed Denial of Service — DoS)* — это атаки, направленные на прерывание связи между удаленным ресурсом и пользователем [1].

Начиная с конца 1980-х годов DoS-инструменты стали доступны широкому кругу пользователей, что привело к увеличению количества DoS-атак, особенно в начале 2000-х годов. Цель атаки — потребление вычислительных ресурсов (дополнительная нагрузка на процессор, ОЗУ) или пропускной способности. Результатом является отсутствие доступа к услугам [2]. В настоящее время DoSатаки инициируются из разрозненных распределенных сетей. Данный тип атак называется распределенными DoS- (DDoS) атаками. Цель все та же — прекращение доступа легитимных пользователей к ресурсам. Огромное количество пакетов, приходящих на сервера, делает сервисы недоступными для законных пользователей [1].

Защиту от *DoS/DDoS* атак можно подразделить на три этапа: предотвращение, обнаружение и реагирование. Обнаружение является одним из ключевых шагов в защите от DoS/DDoS атак. Однако из-за большого числа типов DoS/DDoS-атак обнаружение таких атак становится проблематичным. Качественный метод обнаружения должен иметь малое время работы и низкий процент ложных срабатываний.

Поскольку *DoS-атаки* стали одной из главных проблем при обеспечении безопасности в Интернете, необходимо более активно вести разработку средств по их обнаружению и предотвращению. Обнаружение DDoS-атак часто является частью более широкой системы обнаружения вторжений (IDS) [1, 2]. IDS можно определить как программное или аппаратное обеспечение, используемое для обнаружения несанкционированного трафика или действий, которые противоречат разрешенной политике данной сети [2]. Обнаружение вторжений не является новой областью исследований. Одной из самых ранних опубликованных работ по IDS является работа Андерсона, выпущенная в 1980 г. [3]. В 1987 г. Деннинг [3] предоставил структуру модели IDS для исследователей, работающих над ней [2]. IDS могут быть классифицированы на основе расположения источника аудита как основанные на хосте,

[1] PhD, профессор кафедры «Информационная безопасность» Ферганского филиала Ташкентского университета информационных технологий имени Мухаммад ал-Хорезми Фергана, Узбекистан
[2] Магистрант кафедры «Информационная безопасность» Ферганского филиала Ташкентского университета информационных технологий имени Мухаммад ал-Хорезми Фергана, Узбекистан

основанные на сети или как комбинация обоих. В первом варианте выполняется мониторинг данных аудита, таких как лог-файлы приложений и операционной системы, и IDS располагается на каждом хосте. Во втором варианте выполняется мониторинг сетевого трафика, и IDS располагается на машине отдельно от хостов, которые она защищает. Гибридные системы обнаружения вторжений объединяют оба описанных типа [3].

Литературный обзор. Исследовательские данные указывают на то, что выявление атак типа DDoS может быть классифицировано по трём ключевым группам: классические способы, алгоритмы искусственного интеллекта и смешанные стратегии.

Традиционные методы основаны на статистическом анализе сетевого трафика, обеспечивают быстрое обнаружение при низкой сложности и эффективно работают для базовых атак, как показали исследования Mirkovic и Peng (2004, 2007). Однако их точность снижается при увеличении сложности атак.

Методы машинного обучения (ML) включают алгоритмы, такие как SVM, нейронные сети и деревья решений, которые применяются для анализа и классификации сетевого трафика. Исследования Somani et al. (2017) и Deepthi and Ramesh (2018) доказали, что такие алгоритмы способны выявлять сложные аномалии с высокой точностью, но требуют значительных вычислительных ресурсов, что ограничивает их применение в условиях реального времени.

Аномалия-ориентированные подходы сосредоточены на обнаружении отклонений от нормального поведения сетевого трафика. Chen et al. (2019) и Ahmed et al. (2020) показали, что эти методы минимизируют ложные срабатывания и эффективны для выявления неизвестных атак, но их настройка может быть сложной и ресурсоёмкой.

Гибридные подходы объединяют традиционные и современные методы для повышения эффективности обнаружения. Например, исследования Zargar et al. (2021) продемонстрировали, что такие системы обладают высокой производительностью и способны комбинировать сигнатурный анализ с алгоритмами машинного обучения, но их реализация требует значительных технических и вычислительных усилий.

Методы обнаружения DDoS-атак

Обнаружение DDoS-атак требует применения комплексных и многослойных подходов. Существуют как традиционные методы, так и более современные подходы, основанные на анализе данных с использованием машинного обучения, а также обнаружение атак на основе аномалий.

1. Традиционные методы обнаружения

К традиционным методам относятся:

Анализ аномальных пиков в трафике. Один из самых простых способов — это мониторинг объёмов входящего трафика. В случае DDoS-атаки можно заметить резкое увеличение количества запросов, что выходит за пределы нормальных значений.

Использование фильтрации пакетов. Данный метод включает анализ каждого пакета, проходящего через сеть, на наличие признаков атаки. Например, в случае SYN Flood атаки пакеты SYN могут быть обнаружены и отклонены.

Использование статистического анализа. Включает создание моделей нормального поведения трафика и выявление отклонений от этих моделей. Такие методы могут использовать пороговые значения для сигнализации о возможных аномалиях.

2. Методы на основе машинного обучения

Современные технологии требуют использования более сложных методов, таких как машинное обучение (ML) и анализ больших данных. Эти методы обеспечивают более точное и своевременное обнаружение DDoS-атак. Сравнительный анализ различных методов представлен в таблице 1.

Алгоритмы классификации. Использование таких алгоритмов, как Random Forest, Support Vector Machines (SVM) и нейронные сети, позволяет анализировать исторические данные и выявлять шаблоны трафика, характерные для DDoS-атак.

Алгоритмы кластеризации. Методы, такие как K-means и DBSCAN, позволяют группировать данные и обнаруживать аномалии, которые могут указывать на атаку. Эти методы полезны, когда нет чётко определённых паттернов.

Рекуррентные нейронные сети (RNN) и LSTM. Эти алгоритмы могут работать с временными последовательностями данных и эффективно анализировать трафик в реальном времени, что особенно полезно для выявления сложных атак, таких как HTTP Flood или другие атаки на уровне приложений.

3. Обнаружение атак на основе аномалий.

Методы обнаружения вторжений, основанные на противоречивости, распознают необычную активность и создают предупреждения аномалий в действиях системы или действиях приложений. Обычные специфические действия, которые могли бы быть перехвачены, включают:

Злоупотребление системными соглашениями, например, скрытие интервала IP-адресов и выполнение стандартного соглашения на скрытом порту;

Уникальные паттерны трафика, например, больше UDPпакетов по сравнению с TCP;

Подозрительные примеры в полезных данных приложения. Наибольшие трудности в использовании методов обнаружения на основе аномалий заключаются в определении типичного поведения системы, выборе предела для срабатывания предупреждения и предотвращении ложных предупреждений.

Пользователи системы, как правило, люди, и их поведение трудно предвидеть. В том случае, если обычная модель не будет охарактеризована подробным образом, возникнет множество ложных срабатываний, и система обнаружения будет испытывать негативные последствия неверного исполнения. В связи с развитием средств машинного обучения на сегодняшний день многие исследователи предпочитают применять алгоритмы машинного обучения и искусственные нейронные сети для обнаружения различных угроз.

Обсуждения. Методы анализа сетевого трафика играют важную роль в выявлении аномалий и обеспечении кибербезопасности. В зависимости от поставленных задач и доступных ресурсов применяются различные подходы, каждый из которых обладает своими характеристиками, преимуществами и недостатками. В таблице представлены три популярных метода: статистический анализ, алгоритмы классификации (SVM) и рекуррентные нейронные сети (LSTM). Статистический анализ выделяется своей простотой и низкими затратами, но может приводить к ложным срабатываниям. Алгоритмы классификации обеспечивают высокую точность и адаптивность, однако требуют значительных объемов данных для обучения. Модели LSTM способны анализировать временные ряды и выявлять сложные паттерны, но их реализация требует значительных вычислительных ресурсов. Такой сравнительный анализ позволяет выбрать наиболее подходящий метод в зависимости от требований к точности, доступным ресурсам и сложности решаемых задач.

Таблица.1. Сравнительный анализ различных методов

Метод	Описание	Преимущества	Недостатки
Статистический анализ	Использование пороговых значений для анализа трафика	Простота внедрения, низкая стоимость	Высокая вероятность ложных срабатываний
Алгоритмы классификации (SVM)	Применение машинного обучения для анализа исторических данных	Высокая точность, адаптивность	Требуют большого объёма данных для обучения
Рекуррентные нейронные сети (LSTM)	Использование для анализа временных рядов трафика	Могут обнаруживать сложные паттерны	Высокие вычислительные затраты

Результаты. Обнаружение DDoS-атак в реальном времени представляет собой сложную задачу по ряду причин. Во-первых, атаки могут быть очень разнообразными, включая как большие объёмы трафика, так и небольшие, но интенсивные атаки, которые труднее заметить. Во-вторых, современные DDoS-атаки часто используют технологии маскировки, такие как использование ботов для создания трафика с различных IP-адресов, что делает их трудными для блокировки.

Для эффективного обнаружения таких атак в реальном времени системы должны обладать следующими характеристиками:

- *Высокая скорость обработки данных*. В реальном времени требуется мгновенный анализ трафика, чтобы немедленно выявить аномальные ситуации и предотвратить их развитие.
- *Низкое количество ложных срабатываний.* Важно минимизировать количество ложных тревог, так как это может привести к излишней нагрузке на систему и её неэффективности.
- *Адаптивность.* Система должна быть гибкой и способной адаптироваться к изменениям в трафике, обучаясь на новых типах атак.

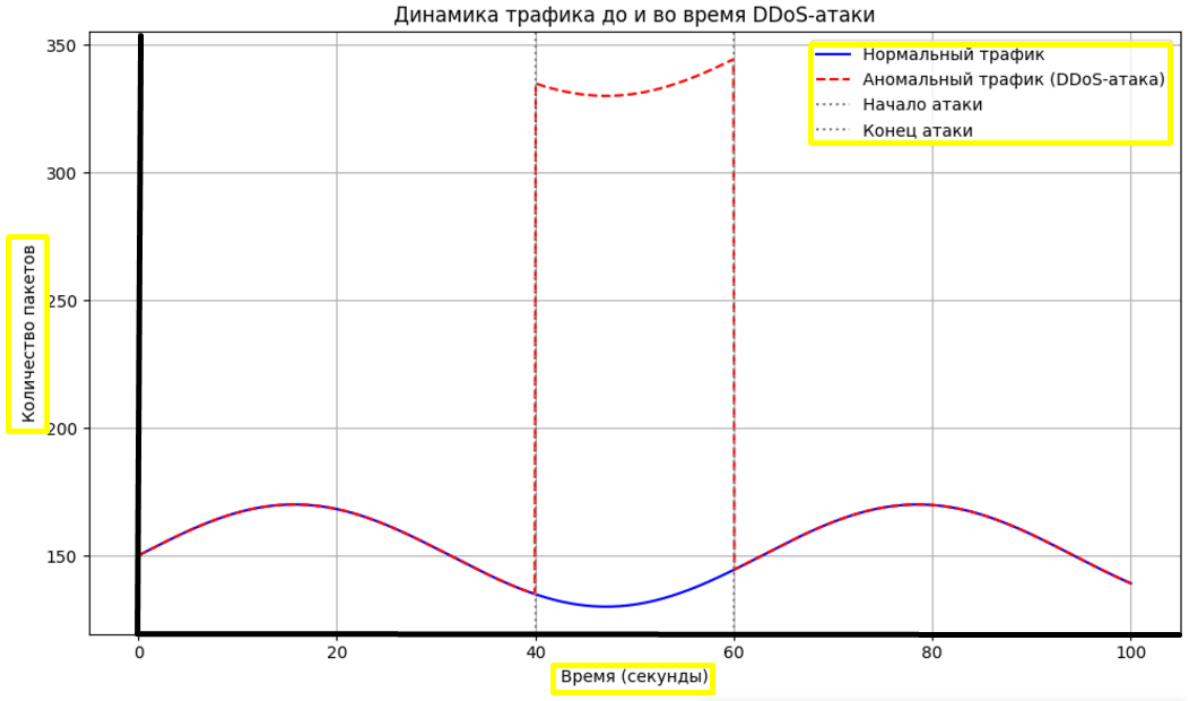

Рис.1. Динамика трафика до и вовремя DDoS-атаки

На графике показано, как резко возрастает сетевой трафик вовремя DDoS-атаки. Нормальный трафик плавно изменяется, а аномальный трафик (в момент атаки) демонстрирует резкий пик. Также, данный график помогает визуализировать, как именно атака влияет на сеть, например, как резко возрастает количество запросов, и как быстро можно обнаружить аномалию. **Синяя линия** представляет нормальный трафик, который плавно меняется с течением времени. **Красная пунктирная линия** показывает аномальный трафик в момент атаки, когда происходит резкий рост количества пакетов. **Вертикальные серые линии** обозначают начало и конец DDoS-атаки, чтобы чётко выделить момент её возникновения. (Ось X: время (в секундах); Ось Y: количество пакетов; линия 1: нормальный трафик; линия 2: аномальный трафик (в момент атаки)).

Применение современных решений и технологий. Для эффективной защиты от DDoS-атак в реальном времени широко используются специализированные решения, включая сервисы защиты, предлагаемые крупными провайдерами безопасности, такими как Cloudflare и Akamai. Эти компании предлагают масштабируемые облачные решения для фильтрации трафика и защиты от атак. Такие сервисы могут обрабатывать большие объёмы трафика и эффективно блокировать подозрительные запросы.

Кроме того, многие организации внедряют системы обнаружения и предотвращения вторжений (IDS/IPS), которые могут обнаруживать аномалии в трафике и предпринимать меры для его блокировки. Инструменты, такие как Snort и Suricata, активно используются для анализа пакетов и выявления признаков DDoS-атак.

Выводы. Обнаружение является одним из ключевых шагов в защите от DoS/DDoS-атак, однако по причине большого числа различных типов атак обнаружение таких атак становится проблематичным. В данной статье рассмотрены методы обнаружения DDoS-атак, обнаружение атак на основе аномалий. Представлена широкая классификация защитных архитектур, выполнен их обзор и указаны их преимущества и недостатки, основанные на том, где и когда выполняется обнаружение и реагирование на атаки.

Обнаружение DDoS-атак в реальном времени является неотъемлемой частью стратегий защиты компьютерных сетей. Традиционные методы, такие как анализ пиков трафика и фильтрация пакетов, уже не могут обеспечить необходимую точность и скорость, что требует применения более сложных технологий. Современные методы на основе машинного обучения, такие как нейронные сети и алгоритмы классификации, предлагают новые возможности для выявления аномальных паттернов в трафике и предотвращения атак до того, как они приведут к серьёзным последствиям. Внедрение таких решений позволит значительно повысить устойчивость систем к DDoS-угрозам и улучшить общую безопасность.

Список использованных литератур

1. Tripathi S., Gupta B., Almomani A., et al. Hadoop based defense solution to handle distributed denial of service DDoS attacks. J. Inf. Secur., 2013, vol. 4, no. 3, pp. 150–164. [1]
2. Hachem N., Ben Mustapha Y., Granadillo G.G., et al. Botnets: lifecycle and taxonomy. Conf. on Network and Information Systems Security, 2011. [2]
3. Mahajan D., Sachdeva M. DDoS attack prevention and mitigation techniques - a review. Int. J. Comput. Appl., 2013, vol. 67, no. 19, pp. 21–24. [3]
4. Абдуллаев, Н. Р., & Исаев, Д. А. (2018). Методы обнаружения DDoS-атак на основе анализа сетевого трафика. Информационная безопасность, 12(3), 45-53.
5. Козлов, А. Ю., & Петров, С. В. (2020). Применение методов машинного обучения для выявления аномалий в сетевом трафике. Вестник компьютерной безопасности, 19(2), 78-87.
6. Иванов, М. Н., & Смирнов, Е. К. (2019). Гибридные подходы к обнаружению DDoS-атак в реальном времени. Компьютерные технологии и кибербезопасность, 10(4), 123-130.

7. Chen, S., Kalbarczyk, Z., & Iyer, R. K. (2019). Network anomaly detection using time series analysis and machine learning. Proceedings of the IEEE International Conference on Dependable Systems and Networks, 452-463.
8. Савельев, Р. П., & Мухин, О. В. (2021). Анализ и классификация атак типа «отказ в обслуживании». Информационные технологии и защита данных, 15(1), 62-71.
9. Никифоров, А. Л., & Беляев, Ю. А. (2017). Использование статистических методов для обнаружения аномалий в сети. Труды Всероссийской конференции по информационной безопасности, 56-63.