УДК 004.85

Гурецкая Арина Максимовна

выпускник бакалавриата, Национальный исследовательский ядерный университет «МИФИ», Россия, г. Москва

Маргарян Давид Арменович

выпускник бакалавриата, Национальный исследовательский ядерный университет «МИФИ», Россия, г. Москва

МЕТОД МНОГОЭТАПНОГО ОБНАРУЖЕНИЯ РАСПРЕДЕЛЁННЫХ DDoS-АТАК НА ОСНОВЕ КОМБИНИРОВАННОГО ПРИМЕНЕНИЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Распределённые атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) продолжают оставаться одной из наиболее распространённых угроз информационной безопасности корпоративных сетей и облачных сервисов. Постоянное увеличение объёмов сетевого трафика, появление новых разновидностей атак и изменение характера сетевых взаимодействий существенно снижают эффективность традиционных сигнатурных методов обнаружения. В связи с этим возрастает актуальность применения алгоритмов машинного обучения, способных выявлять аномальное поведение на основе анализа статистических характеристик сетевого трафика.

В работе предложен многоэтапный метод обнаружения DDoS-атак, основанный на комбинированном использовании алгоритмов Isolation Forest и One-Class SVM. Предлагаемый подход включает последовательные этапы предварительной обработки сетевых данных, извлечения информативных признаков, выявления аномалий, комплексной оценки результатов классификации и принятия итогового решения. Для оценки эффективности метода использован открытый набор данных CIC-DDoS2019. Проведён сравнительный анализ с использованием метрик Accuracy, Precision, Recall, F1-score и AUC-ROC.

Результаты исследования показывают, что комбинированный подход обеспечивает повышение устойчивости системы обнаружения к несбалансированности данных и снижает количество ложноположительных срабатываний по сравнению с использованием отдельных алгоритмов. Предлагаемый метод может быть использован при разработке интеллектуальных систем мониторинга сетевой безопасности и средств раннего обнаружения распределённых атак.

Ключевые слова: информационная безопасность, DDoS-атаки, машинное обучение, обнаружение аномалий, Isolation Forest, One-Class SVM, сетевой трафик, информационные системы.

Annotation. Distributed Denial of Service (DDoS) attacks remain one of the most significant threats to modern information systems and cloud infrastructures. The continuous growth of network traffic, the emergence of new attack patterns, and the increasing complexity of network interactions significantly reduce the effectiveness of traditional signature-based intrusion detection systems. Therefore, machine learning methods capable of detecting anomalous behavior in network traffic have become increasingly important.

This paper proposes a multi-stage DDoS attack detection method based on the combined application of Isolation Forest and One-Class Support Vector Machine algorithms. The proposed approach includes network traffic preprocessing, feature extraction, anomaly detection, integrated evaluation of classification results, and final decision making. The CIC-DDoS2019 public dataset was used to evaluate the proposed method. Experimental evaluation was performed using Accuracy, Precision, Recall, F1-score, and AUC-ROC metrics.

The obtained results demonstrate that the proposed combined approach improves detection stability under highly imbalanced datasets while reducing false positive rates compared with individual machine learning models. The proposed method can be

applied in intelligent cybersecurity monitoring systems and real-time distributed attack detection platforms.

Keywords: information security, DDoS attack, machine learning, anomaly detection, Isolation Forest, One-Class SVM, network traffic analysis.

Введение

Современная цифровая инфраструктура является основой функционирования государственных информационных систем, корпоративных сетей, облачных вычислительных платформ и сервисов электронной коммерции. Постоянное увеличение объёмов передаваемых данных, широкое распространение технологий виртуализации и развитие распределённых вычислений сопровождаются ростом количества киберугроз, одной из наиболее опасных среди которых остаются распределённые атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS).

Основной целью DDoS-атак является нарушение доступности информационных ресурсов путём формирования чрезмерного объёма сетевого трафика, приводящего к перегрузке вычислительных ресурсов сервера, сетевого оборудования или каналов связи. В отличие от традиционных атак, инициируемых одним источником, распределённые атаки осуществляются одновременно большим количеством скомпрометированных устройств, объединённых в ботнеты [1]. В результате значительно возрастает сложность своевременного обнаружения атакующих воздействий и идентификации вредоносного трафика.

По данным аналитических отчётов ведущих компаний в области информационной безопасности, ежегодно наблюдается устойчивый рост количества DDoS-атак, а также увеличение их средней продолжительности и интенсивности. Современные атаки всё чаще используют комбинированные сценарии воздействия, включающие одновременно несколько сетевых протоколов и различные способы формирования аномального трафика. Кроме

того, злоумышленники активно применяют механизмы маскировки вредоносной активности под легитимное сетевое взаимодействие, что существенно снижает эффективность классических методов обнаружения вторжений.

Традиционные средства защиты, основанные на сигнатурном анализе и заранее известных шаблонах атак, позволяют эффективно обнаруживать только ранее изученные виды угроз. Однако при появлении новых разновидностей DDoS-атак или модификации существующих сценариев эффективность подобных систем существенно снижается.

Одним из наиболее перспективных направлений развития систем обнаружения вторжений является использование методов машинного обучения. Особенно эффективными являются алгоритмы обучения без учителя, позволяющие строить модель нормального функционирования сети и фиксировать отклонения от неё.

Среди наиболее известных алгоритмов обнаружения аномалий широкое распространение получили Isolation Forest и One-Class Support Vector Machine (One-Class SVM). Каждый из указанных алгоритмов обладает собственными преимуществами и ограничениями.

В связи с этим актуальной научной задачей является разработка метода интеллектуального обнаружения распределённых DDoS-атак, обеспечивающего повышение точности классификации сетевого трафика за счёт последовательного комбинированного применения нескольких алгоритмов машинного обучения и комплексной обработки результатов их работы.

Целью настоящего исследования является разработка многоэтапного метода обнаружения DDoS-атак на основе совместного использования алгоритмов Isolation Forest и One-Class SVM, позволяющего повысить эффективность выявления аномального сетевого трафика в условиях высокой размерности данных и значительной несбалансированности выборок.

Анализ существующих методов обнаружения DDoS-атак

Обнаружение распределённых атак типа «отказ в обслуживании» является одной из наиболее актуальных задач современной информационной безопасности. За последние годы предложено значительное количество методов анализа сетевого трафика, отличающихся используемыми алгоритмами обработки данных, вычислительной сложностью и областью применения. Условно существующие методы можно разделить на три основные группы: сигнатурные, статистические и интеллектуальные.

Сигнатурные методы основаны на сопоставлении анализируемого сетевого трафика с заранее сформированной базой известных признаков атак. Их преимуществом является высокая точность обнаружения известных угроз, однако они не способны эффективно выявлять ранее неизвестные атаки.

Статистические методы используют анализ количественных характеристик сетевого трафика. Они позволяют обнаруживать новые угрозы, однако отличаются высокой чувствительностью к изменениям легитимной нагрузки, что увеличивает число ложноположительных срабатываний.

Наиболее активно развивающимся направлением является применение методов машинного обучения. Алгоритмы обучения с учителем демонстрируют высокую точность при наличии размеченных данных, однако требуют значительных затрат на формирование обучающих выборок.

Особый интерес представляют методы обучения без учителя, поскольку реальные сетевые данные содержат значительно больше нормального трафика, чем вредоносного. В подобных условиях эффективно применяются алгоритмы обнаружения аномалий [2].

Одним из наиболее известных алгоритмов является Isolation Forest, основанный на случайной изоляции объектов посредством ансамбля бинарных деревьев. Другим широко используемым методом является One-Class Support

Vector Machine, формирующий границу нормального поведения объектов в пространстве признаков [3].

Несмотря на высокую эффективность каждого алгоритма, их самостоятельное применение имеет определённые ограничения. Isolation Forest может снижать точность при наличии большого количества взаимосвязанных признаков [4], тогда как One-Class SVM чувствителен к выбору параметров и масштабированию данных [5].

Анализ современных исследований показывает, что возможности совместного использования нескольких моделей машинного обучения изучены недостаточно. В связи с этим в настоящей работе предлагается многоэтапный метод обнаружения DDoS-атак, основанный на последовательном использовании нескольких алгоритмов машинного обучения и интегральной оценке результатов их работы, направленный на повышение точности обнаружения атак и снижение количества ложноположительных срабатываний.

Предлагаемый метод многоэтапного обнаружения распределённых DDoS-атак

Предлагаемый метод предназначен для повышения эффективности обнаружения распределённых атак типа «отказ в обслуживании» за счёт последовательной обработки сетевого трафика несколькими алгоритмами машинного обучения и объединения результатов их работы. В отличие от существующих подходов, использующих единственный классификатор, предлагаемый метод предусматривает выполнение нескольких этапов анализа, каждый из которых уменьшает влияние недостатков предыдущего этапа.

Основная идея метода заключается в последовательном преобразовании исходного сетевого трафика в пространство информативных признаков, независимой оценке степени аномальности несколькими моделями машинного обучения и формировании итогового решения на основе комплексной оценки полученных результатов.

Предлагаемый алгоритм включает шесть взаимосвязанных этапов: сбор сетевого трафика, предварительная обработка данных, формирование пространства признаков, обнаружение аномалий, интегральная оценка результатов, принятие решения. Такое разделение позволяет обеспечить модульность системы и возможность замены отдельных компонентов без изменения общей архитектуры метода.

На первом этапе осуществляется сбор информации о сетевых соединениях из журналов регистрации событий, систем мониторинга или непосредственно с сетевых интерфейсов.

В качестве исходных данных используются записи потоков (Flow Records), содержащие характеристики каждого сетевого соединения: IP-адрес источника, IP-адрес назначения, номера портов, транспортный протокол, количество переданных пакетов и байтов, продолжительность соединения, средний размер пакета и временные интервалы между пакетами.

Предварительная обработка включает удаление дублирующихся записей, исключение неполных соединений, обработку пропусков, нормализацию числовых признаков и кодирование категориальных параметров. Для нормализации используется метод Min–Max Scaling, обеспечивающий приведение признаков к единому диапазону значений.

В предлагаемом методе используются три группы признаков: статистические (длительность сеанса, число пакетов, объём данных, скорость передачи, коэффициент вариации интенсивности), временные (интервалы между пакетами, частота поступления, изменение интенсивности, число соединений за интервал времени) и поведенческие (количество уникальных IP-адресов, частота повторных соединений, соотношение входящего и исходящего трафика, количество SYN-пакетов и незавершённых TCP-соединений). Использование совокупности различных типов признаков повышает устойчивость системы к современным разновидностям DDoS-атак.

После формирования пространства признаков данные поступают на первый классификатор — алгоритм Isolation Forest. Для каждого наблюдения вычисляется коэффициент аномальности $S_{IF} \in [0; 1]$. Чем меньше глубина изоляции объекта в ансамбле случайных деревьев, тем выше вероятность того, что соединение является аномальным. Алгоритм отличается высокой скоростью обработки, устойчивостью к большим объёмам данных и не требует балансировки выборки.

Наблюдения с промежуточными значениями коэффициента аномальности дополнительно анализируются алгоритмом One-Class SVM. Для каждого соединения вычисляется значение функции решения S_{SVM} , характеризующее расстояние объекта до границы нормального состояния. Это позволяет снизить количество ложноположительных решений. Результаты объединения двух моделей с помощью взвешенной суммы представлены ниже в формуле 1:

$$R = \alpha S_{IF} + \beta S_{SVM} \quad (1)$$

где $\alpha + \beta = 1$.

Весовые коэффициенты определяются экспериментально. Если $R \geq T$, соединение классифицируется как потенциальная DDoS-атака. Интегральная оценка позволяет компенсировать недостатки отдельных алгоритмов и повысить достоверность классификации.

Алгоритм принятия решения

Полный цикл работы метода включает получение сетевого трафика, очистку и нормализацию данных, извлечение информативных признаков, анализ алгоритмом Isolation Forest, повторную оценку пограничных наблюдений методом One-Class SVM, вычисление интегрального коэффициента, классификацию соединения и передачу результата в систему мониторинга информационной безопасности.

Таким образом, предложенный метод обеспечивает последовательное уточнение результатов классификации и позволяет эффективно выявлять

распределённые атаки даже при высокой степени несбалансированности обучающих данных.

Формальная математическая модель предлагаемого метода

Пусть исходный набор сетевых соединений представлен множеством $X = \{x_1, x_2, \dots, x_n\}$, где каждое наблюдение $x_i = (f_1, f_2, \dots, f_m)$ представляет собой вектор признаков сетевого соединения.

После предварительной обработки формируется матрица признаков F размерности $n \times m$, каждая строка которой соответствует одному сетевому соединению.

Алгоритм Isolation Forest формирует функцию оценки $S_{IF}: X \to [0; 1]$. Для каждого объекта вычисляется коэффициент. Формула 2 для подсчета данного коэффициента представлена ниже.

$$s_i(IF) = S_{IF}(x_i) \quad (2)$$

Наблюдения, удовлетворяющие условию $T_1 < s_i(IF) < T_2$, дополнительно анализируются алгоритмом One-Class SVM, формирующим функцию решения $S_{SVM}: X \to [-1; 1]$. После нормализации вычисляется оценка $s_i(SVM) \in [0; 1]$.

Интегральная оценка определяется выражением, описанным ниже в формуле 3:

$$R_i = \alpha \cdot s_i(IF) + \beta \cdot s_i(SVM) \quad (3)$$

где $\alpha + \beta = 1$.

Окончательное решение принимается по правилу: $C(x_i) = 1$ при $R_i \geq T$ и $C(x_i) = 0$ при $R_i < T$.

Оценка вычислительной сложности метода

Данные оценки вычислительной сложности метода представлены в таблице 1.

Таблица 1.

Вычислительная сложность этапов метода

Этап	Асимптотическая сложность
Предварительная обработка	$O(nm)$
Нормализация	$O(nm)$
Isolation Forest	$O(tnlogn)$
One-Class SVM	$O(n^2) - O(n^3)$
Интегральная оценка	$O(n)$
Принятие решения	$O(n)$

где n — количество соединений; m — число признаков; t — количество деревьев Isolation Forest.

Итоговая асимптотическая сложность метода оценивается как $O(tnlogn + k^2)$, где $k \ll n$ — количество соединений, передаваемых на второй этап анализа. Это обеспечивает компромисс между точностью и скоростью обработки.

Особенности реализации и экспериментальная оценка метода

Программная реализация выполнена на Python 3.11 с использованием библиотек Scikit-learn, Pandas, NumPy и Matplotlib.

Для проведения эксперимента был выбран общедоступный набор данных CIC-DDoS2019, предоставленный Канадским институтом кибербезопасности [6]. Перед обучением выполнены очистка данных, удаление пропусков, нормализация и разделение выборки в соотношении 80:20. Параметры Isolation Forest представлены в таблице 2.

Таблица 2.

Параметры Isolation Forest

Параметр	Значение
n_estimators	100
max_samples	256
Contamination	0,01
random_state	42

Параметры One-Class SVM представлены в таблице 3.

Таблица 3.

Параметры One-Class SVM

Параметр	Значение
Ядро	RBF
gamma	scale
ν	0,05

Качество классификации оценивалось по метрикам Accuracy, Precision, Recall, F1-score и AUC-ROC. Сравнительная характеристика эффективности исследуемых методов представлена ниже в таблице 4.

Таблица 4.

Сравнение эффективности исследуемых методов

Метод	Accuracy	Precision	Recall	F1-score	AUC-ROC
Isolation Forest	0,963	0,954	0,948	0,951	0,968
One-Class SVM	0,971	0,966	0,960	0,963	0,975
Предлагаемый метод	0,982	0,980	0,975	0,977	0,986

Совместное использование двух алгоритмов обеспечивает повышение качества классификации по всем исследуемым показателям. Предварительная

фильтрация Isolation Forest позволяет сократить число объектов, передаваемых в One-Class SVM, что уменьшает вычислительные затраты без заметной потери точности.

Обсуждение результатов

Проведённые экспериментальные исследования подтверждают, что применение методов машинного обучения позволяет существенно повысить эффективность обнаружения распределённых DDoS-атак по сравнению с традиционными подходами, основанными на сигнатурном анализе сетевого трафика. Использование интеллектуальных алгоритмов обеспечивает возможность выявления ранее неизвестных сценариев атак за счёт анализа статистических закономерностей и аномального поведения сетевых соединений.

Результаты сравнительного анализа показывают, что алгоритм Isolation Forest характеризуется высокой скоростью обработки данных и устойчивостью к несбалансированным выборкам. Алгоритм One-Class SVM обеспечивает более точное разделение нормального и аномального трафика, однако отличается более высокой вычислительной сложностью.

Предлагаемый многоэтапный метод объединяет преимущества обоих алгоритмов. Предварительная фильтрация соединений с использованием Isolation Forest и последующая обработка неоднозначных наблюдений алгоритмом One-Class SVM позволяют уменьшить вычислительную нагрузку при сохранении высокой точности обнаружения аномалий.

Использование интегральной оценки результатов классификации снижает вероятность ошибочных решений и обеспечивает более устойчивую работу системы при изменении структуры сетевого трафика. Перспективными направлениями дальнейших исследований являются автоматический отбор признаков, адаптивная настройка параметров моделей и применение ансамблевых и глубоких моделей машинного обучения.

Выводы

В работе разработан многоэтапный метод обнаружения распределённых DDoS-атак, основанный на комбинированном использовании алгоритмов Isolation Forest и One-Class Support Vector Machine. Предложенный подход реализует последовательную обработку сетевого трафика с объединением результатов нескольких этапов анализа посредством интегральной функции принятия решения.

Экспериментальная проверка на наборе данных CIC-DDoS2019 показала повышение Accuracy, Precision, Recall, F1-score и AUC-ROC по сравнению с использованием отдельных алгоритмов. Метод позволяет снизить количество ложноположительных решений при сохранении высокой полноты обнаружения атак. Практическая значимость исследования заключается в возможности применения разработанного метода в интеллектуальных системах мониторинга сетевой безопасности и обнаружения вторжений. Дальнейшее развитие связано с использованием ансамблевых моделей и методов глубокого обучения.

Список литературы:

1. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*.
2. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*.
3. CERT Recommendation. (2021). Understanding Denial-of-Service Attacks. [Электронный ресурс].
4. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. *2008 Eighth IEEE International Conference on Data Mining*.
5. Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the Support of a High-Dimensional Distribution. *Neural Computation*.

6. Canadian Institute for Cybersecurity. (2019). CIC-DDoS2019 Dataset. [Электронный ресурс]. URL: https://www.unb.ca/cic/datasets/ddos-2019.html

References:

1. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*.

2. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*.

3. CERT Recommendation. (2021). Understanding Denial-of-Service Attacks. [Электронный ресурс].

4. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. *2008 Eighth IEEE International Conference on Data Mining*.

5. Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the Support of a High-Dimensional Distribution. *Neural Computation*.

6. Canadian Institute for Cybersecurity. (2019). CIC-DDoS2019 Dataset. [Электронный ресурс]. URL: https://www.unb.ca/cic/datasets/ddos-2019.html