Инженерный вестник Дона, №2 (2026)
ivdon.ru/ru/magazine/archive/n2y2026/10764

Исследование подходов к защите веб-серверов от распределенных атак типа «отказ в обслуживании»

М.Ю. Каранов, Д.С. Горин, Р.Р. Шатовкин

МИРЭА – Российский технологический университет, Москва

Аннотация: Проведен анализ основных видов распределенных атак типа «отказ в обслуживании», а также исследованы классические и инновационные методы защиты веб-серверов от угроз, включающие: фильтрацию пакетов, применение систем обнаружения и предотвращения вторжений, архитектурные решения по балансировке нагрузки. На основе результатов исследования выявлены существенные ограничения традиционных подходов: низкая адаптивность к новым угрозам, высокая вероятность ложных срабатываний, неспособность эффективно противостоять современным многофакторным атакам. Выявлена перспективность применения методов искусственного интеллекта и нейронных сетей для анализа сетевого трафика и выявления сложных паттернов аномалий.
Ключевые слова: защита веб-сервера, распределенная атака, отказ в обслуживании, фильтрация трафика, фильтрация пакетов, система обнаружения вторжений.

Введение

В современном цифровом обществе веб-серверы играют ключевую роль в обеспечении доступа к информации и сервисам, что делает их привлекательной целью для кибератак, в целом, и для распределенных атак отказа в обслуживании – Distributed Denial of Service (DDoS) атак, в частности.

Актуальность темы защиты веб-серверов от DDoS-атак обусловлена не только ростом числа и сложности таких атак, но и необходимостью поддержания непрерывности и безопасности интернет-сервисов, что напрямую влияет на экономическую и социальную стабильность.

В последние годы наблюдается значительный прогресс в области применения методов искусственного интеллекта, особенно нейронных сетей, для обнаружения и предотвращения DDoS-атак. Это связано с их способностью эффективно анализировать большие объемы сетевого трафика и выявлять сложные паттерны аномалий, что затруднительно для традиционных методов защиты.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

DDoS-атаки представляют собой разновидность кибератак, направленных на выведение из строя веб-серверов путем перегрузки их запросами с множества источников. Основная цель таких атак – сделать сервис недоступным для пользователей, вызывая отказ в обслуживании [1].

В зависимости от уровня воздействия и используемых методов, DDoS-атаки классифицируются на несколько видов, каждый из которых имеет свои особенности и сложности для обнаружения и защиты.

Одним из распространенных видов являются сетевые (Network Layer) DDoS-атаки, которые ориентированы на исчерпание пропускной способности канала или ресурсов сетевого оборудования. К ним относятся атаки типа User Datagram Protocol (UDP)-флуд, Internet Control Message Protocol (ICMP)-флуд и Synchronization (SYN)-флуд, при которых большое количество пакетов генерируется с целью перегрузить сеть или сервер [2]. Эти атаки обычно характеризуются высокой скоростью трафика и относительной простой в обнаружении, однако их масштаб и распределенность делают их опасными для крупных веб-сервисов.

Атаки на уровне приложений (Application Layer) представляют собой более изощренный тип DDoS-атак, направленный на исчерпание ресурсов самого веб-приложения путем имитации легитимных запросов, например, HTTP GET или POST. Такие атаки сложнее обнаружить, так как трафик выглядит как обычный пользовательский, но при этом вызывает значительную нагрузку на сервер, что приводит к снижению производительности или полной недоступности ресурса.

Традиционные методы фильтрации и блокировки часто оказываются недостаточными, особенно против атак на уровне приложений и ботнет-атак. В этом контексте применение интеллектуальных систем, включая нейронные сети, становится перспективным направлением, позволяющим выявлять сложные паттерны аномального поведения и адаптироваться к новым видам угроз.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Таким образом, разнообразие видов DDoS-атак и их особенностей требует комплексного анализа и внедрения современных средств защиты, способных обеспечить надежную работу веб-серверов в условиях постоянно эволюционирующих угроз. Несмотря на значительный прогресс в области обнаружения и предотвращения атак, остаются вызовы, связанные с высокой сложностью трафика и необходимостью минимизации ложных срабатываний при сохранении высокой точности защиты. Это подчеркивает актуальность исследований в области применения нейронных сетей для повышения эффективности систем защиты от DDoS-атак на веб-серверы [3, 4].

Цель проводимого исследования – исследование основных особенностей, достоинств и недостатков существующих методов защиты веб-серверов от DDoS-атак.

Исследование классических методов защиты от DDoS-атак

Классические методы защиты от DDoS-атак включают в себя широкий спектр технических и организационных мер, направленных на предотвращение и минимизацию последствий распределенных атак отказа в обслуживании.

Основные подходы традиционной защиты базируются на фильтрации трафика, ограничении пропускной способности, использовании систем обнаружения вторжений – Intrusion Detection System (IDS) и систем предотвращения вторжений – Intrusion Prevention System (IPS), а также на архитектурных решениях, таких как балансировка нагрузки и изоляция критически важных ресурсов. Ключевым элементом в этом случае является мониторинг сетевого трафика с целью выявления аномалий, характерных для DDoS-атак, например, резкого увеличения количества запросов или появления трафика с подозрительных IP-адресов.

Одним из наиболее распространенных методов является фильтрация пакетов по IP-адресам и портам, что позволяет блокировать трафик с известных вредоносных источников. Однако данный подход страдает от недостаточной

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

гибкости и неэффективен против атак с использованием поддельных или динамически меняющихся адресов.

Методы ограничения пропускной способности (rate limiting) позволяют снизить нагрузку на сервер, но могут привести к блокировке легитимных пользователей при высокой интенсивности трафика. Использование систем IDS и IPS помогает обнаружить и заблокировать подозрительные пакеты, однако данные системы часто испытывают трудности с точной классификацией трафика, что ведет к ложным срабатываниям и пропуску вредоносных запросов [5].

Архитектурные решения, такие как балансировка нагрузки и распределение ресурсов, позволяют повысить устойчивость веб-серверов, но не устраняют саму причину атак.

Кроме того, классические методы часто требуют значительных вычислительных ресурсов и ручного администрирования, что затрудняет их масштабирование и адаптацию к быстро меняющимся условиям атаки. Важным ограничением является также неспособность традиционных систем эффективно выявлять новые, неизвестные типы DDoS-атак, особенно когда злоумышленники используют сложные схемы маскировки и распределенные ботнеты.

Таким образом, классические методы защиты от DDoS-атак обладают рядом существенных ограничений: низкой адаптивностью, высокой вероятностью ложных срабатываний, ограниченной способностью противостоять современным многофакторным и распределенным атакам, а также серьезными требованиями к ресурсам и квалификации персонала [6].

Исследование инновационных подходов к защите от DDoS-атак

В 2002 году J. Mirkovic и P. Reiher опубликовали результаты своего исследования [7], в котором предлагается новый подход к защите от DDoS – применение для защиты системы DDoS Network Attack Recognition and Defense (D-WARD), работающей на стороне источника атаки, а не на стороне жертвы.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Суть подхода заключается в том, чтобы обнаруживать и блокировать вредоносный трафик еще до того, как он покинет сеть-источник и начнет причинять ущерб. D-WARD – это система, которая устанавливается на граничном маршрутизаторе сети (так называемом «выходном роутере») и отслеживает двусторонний трафик между внутренними хостами и внешними узлами в интернете. Система анализирует не только объем трафика, но и его поведенческие характеристики, сравнивая текущие параметры с моделями нормального трафика.

Ключевая идея – большинство сетевых взаимодействий имеют двусторонний характер. Например, при HTTP-запросе клиент отправляет запрос, а сервер возвращает ответ. Если из сети идет большой объем трафика на определенный адрес, но обратно приходит мало или совсем нет ответов, это может указывать на DDoS-атаку.

Архитектура системы D-WARD включает:

1. Компонент наблюдения (Observation Component):

– собирает статистику по каждому внешнему IP-адресу, с которым общаются внутренние хосты;

– отслеживает количество отправленных и полученных пакетов, их объем, время между пакетами;

– классифицирует трафик по типам: Transmission Control Protocol (TCP), UDP, ICMP и т.д.

2. Компонент ограничения (Throttling Component):

– при обнаружении подозрительной активности ограничивает скорость отправки трафика на целевой адрес;

– использует адаптивные алгоритмы, похожие на механизмы контроля перегрузок в TCP;

– динамически регулирует ограничения в зависимости от поведения трафика.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Система D-WARD использует статистические модели нормального трафика, созданные в период «обучения». Для каждого типа трафика (TCP, UDP, ICMP) определяются типичные параметры взаимодействия. В рабочем режиме система постоянно сравнивает текущий трафик с этими моделями.

Ключевые этапы обнаружения:

1. Сбор статистики в реальном времени.

Для каждого внешнего IP-адреса (с которым общаются хосты защищаемой сети) система собирает:

p_sent – количество пакетов, отправленных на данный адрес;

p_rec – количество пакетов, полученных от данного адреса;

B_sent – количество байт, отправленных на адрес;

B_drop – количество байт, отброшенных из-за ограничения скорости;

int_sent – интервал времени между отправляемыми пакетами;

int_rec – интервал времени между получаемыми пакетами;

mean_rto – сглаженное среднее отношение отправленных к полученным пакетам.

2. Построение и использование моделей нормального трафика.

Для TCP-трафика:

– нормальное TCP-взаимодействие характеризуется близким к единице соотношением отправленных и полученных пакетов;

– типичные значения: 1,0–1,2 (с учетом сетевых задержек и особенностей реализации TCP);

– высокое соотношение (> 3,0) указывает на возможную атаку.

Для non-TCP трафика (UDP, ICMP):

– модели создаются в фазе обучения системы перед запуском;

– система запоминает типичные объемы и паттерны трафика для каждого типа сервиса.

3. Классификация трафика.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Первый этап – проверка по модели TCP-трафика. На этом этапе анализируется соотношение количества отправленных и полученных пакетов для каждого наблюдаемого IP-адреса. Если это соотношение находится ниже установленного порогового значения, характерного для нормального TCP-взаимодействия, поток классифицируется как нормальный. Если же наблюдаемое соотношение превышает TCP-порог, система переходит ко второму этапу проверки.

Второй этап – проверка по моделям non-TCP трафика. На этом этапе система проверяет, соответствует ли наблюдаемый трафик профилю нормальной активности для данного типа протокола (UDP, ICMP и др.). Для этого используются заранее созданные модели, которые описывают типичные паттерны поведения для различных типов сервисов. Если трафик соответствует профилю, установленному для данного типа протокола, он классифицируется как нормальный. Если соответствие не обнаружено или для данного типа трафика отсутствует модель, поток помечается как подозрительный и требует дальнейшего анализа.

4. Детектирование аномалий.

Система ищет следующие признаки DDoS-атак:

а) дисбаланс в двусторонней коммуникации:

– много запросов, мало/нет ответов;

– резкое изменение соотношения отправленных/полученных пакетов;

б) изменение временных характеристик:

– увеличение интервалов между ответными пакетами;

– изменение паттерна взаимодействия;

в) аномальный рост объема трафика:

– резкое увеличение отправляемых данных на конкретный адрес;

– отсутствие соответствующего роста в обратном направлении.

5. Адаптивная классификация потоков.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Нормальные (Normal) – соответствуют моделям, нет истории нарушений.

Атакующие (Attack) – параметры выходят за допустимые границы.

Переходные (Transient) – ранее классифицировались как атакующие, теперь ведут себя нормально (требуют осторожного наблюдения).

Исследователи протестировали систему D-WARD в контролируемой среде, используя реальные DDoS-инструменты (Trinoo, TFN) и легитимный трафик. Результаты тестов показали:

– система эффективно обнаруживает DDoS-атаки в течение нескольких секунд;

– ограничение трафика снижает эффективность атак на 70–90 %;

– легитимный трафик продолжает работать, хотя и с некоторыми задержками;

– использование отдельных моделей для TCP и UDP-трафика повышает точность обнаружения.

Преимуществами данного подхода являются [7]:

– работа на источнике – атака блокируется до того, как нанесет ущерб;

– автономность – не требует координации с другими сетями;

– адаптивность – подстраивается под изменения в сетевом трафике;

– совместимость – может работать на существующем оборудовании;

– постепенное внедрение – эффективность растет с увеличением числа защищенных сетей.

В 2003 году исследователи C. Jin, H. Wang и K.G. Shin представили инновационный подход к решению проблемы сетевых атак с использованием поддельного (spoofed) трафика – методику Hop-Count Filtering (HCF) – фильтрацию по количеству сетевых переходов [8].

Основой метода является наблюдение, что злоумышленник, проводящий атаку с подменой IP-адреса (IP-spoofing), может произвольно задать поле «IP-адрес источника» в пакете, но не может контролировать реальный маршрут,

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

который этот пакет пройдет до цели. Конечный получатель (сервер) способен определить расстояние до реального отправителя пакета в хопах (количестве промежуточных маршрутизаторов). Это расстояние является относительно стабильным для конкретной пары «источник-назначение» в течение длительных периодов времени.

Для вычисления этого расстояния используется поле Time to Live (TTL) в IP-заголовке. Это поле изначально устанавливается операционной системой отправителя на одно из стандартных значений (например, 64, 128, 255) и уменьшается на единицу при прохождении каждого маршрутизатора (хопа). Получив пакет, сервер анализирует конечное значение TTL и, зная вероятное начальное значение, вычисляет пройденное количество хопов.

Сервер заранее, в процессе легитимного взаимодействия (например, при первой установке соединения), обучается: для каждого IP-адреса клиента он вычисляет и сохраняет в таблице IP-to-Hop-Count (IP2HC) эталонное количество хопов. При поступлении каждого последующего пакета система сравнивает текущее вычисленное количество хопов с сохраненным в таблице для заявленного IP-адреса источника. Если значения не совпадают, это с высокой вероятностью указывает на то, что пакет пришел не с того адреса, который указан в заголовке, то есть является спуфинговым.

Сервер получает входящий пакет. Первым делом из его IP-заголовка извлекаются два ключевых поля: IP-адрес отправителя – S, и конечное значение поля TTL, которое пришло в пакете, – T. Это исходные данные для анализа.

Далее необходимо выяснить, с каким начальным значением TTL пакет покинул компьютер-источник. Это возможно, потому что большинство операционных систем используют для отправки пакетов одно из стандартных начальных чисел, чаще всего это 64, 128 или 255.

Сервер анализирует полученное значение T, чтобы определить исходное T_0. Применяется простая эвристическая логика. Если значение T больше 128,

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

то, скорее всего, пакет стартовал со значением 255. Если T больше 64, то вероятным начальным значением было 128. Во всех остальных случаях по умолчанию обычно принимается T_0 равным 64. Для повышения точности могут использоваться более детализированные таблицы, учитывающие специфику различных операционных систем и устройств.

После установления начального значения T_0 вычисляется количество пройденных пакетом хопов (маршрутизаторов) по формуле: $H_c = T_0 - T$. Результат H_c – это и есть расчетное расстояние от сервера до отправителя пакета в данный момент.

На следующем шаге сервер обращается к своей внутренней базе знаний – таблице соответствия IP-адресов и количества хопов, которая создается в период легитимного обмена данными. По IP-адресу S, указанному в пакете, в этой таблице ищется сохраненное эталонное значение количества хопов – H_s.

Наступает этап проверки. Вычисленное только что значение H_c сравнивается с эталонным H_s, найденным в таблице. Необходимо принять решение о легитимности пакета.

Если значение H_c совпадает с H_s или находится в пределах небольшого допустимого отклонения, например, плюс-минус один или два хопа, то пакет признается легитимным. Такое отклонение может быть вызвано незначительными изменениями в маршрутизации сети. Этот пакет передается далее для стандартной обработки сервисом или приложением.

Если же вычисленное количество хопов H_c существенно отличается от сохраненного эталонного H_s, пакет классифицируется как спуфинговый, то есть поддельный. Логика следующая: реальный маршрут от постоянного клиента до сервера не может измениться кардинально за короткое время, поэтому такое несоответствие говорит о том, что отправитель указал чужой IP-адрес.

В заключительной фазе, которая называется режимом действия, система применяет политику к пакетам, признанным спуфинговыми. В рабочем режиме

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

такие пакеты не передаются на обработку, а немедленно отбрасываются. Это действие блокирует атаку, предотвращая использование поддельных пакетов для перегрузки сервера или обхода систем аутентификации [8].

В 2004 году исследователи центра Ultra-Broadband Information Networks T. Peng, C. Leckie, K. Ramamohanarao опубликовали статью «Proactively Detecting Distributed Denial of Service Attacks U sing Source IP Address Monitoring» [9].

Традиционные методы защиты от DDoS-атак анализируют объем трафика, но имеют серьезные недостатки: они не отличают реальные атаки от легитимных всплесков трафика (например, при новости на популярном сайте) и плохо обнаруживают высокораспределенные атаки, где каждый источник отправляет мало данных.

Новое решение – Source IP Address Monitoring (SIM), основная идея которого заключается в следующем: вместо анализа объема трафика система следит за появлением новых IP-адресов. Это основано на наблюдении, что в течение DDoS-атаки большинство IP-адресов являются новыми для жертвы, тогда как при легитимном всплеске трафика (flash crowd) большинство пользователей уже были на сайте ранее.

Процесс состоит из нескольких этапов.

Во-первых, создается база «нормальных» IP-адресов – Integrated Access Device (IAD). Система обучается на чистом трафике без атак, и все IP-адреса, появляющиеся в этот период, сохраняются. База постоянно обновляется: добавляются новые легитимные адреса, удаляются старые. Для определения легитимности используется простое правило, например, TCP-соединение с менее чем 3 пакетами считается подозрительным.

Затем идет мониторинг в реальном времени. Каждые несколько секунд система собирает уникальные IP-адреса из входящего трафика, сравнивает их с базой «нормальных» адресов и вычисляет долю новых IP-адресов (сколько процентов адресов появились впервые). Это ключевой показатель.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Для обнаружения аномалий используется умный алгоритм CUSUM.

В нормальном режиме доля новых адресов близка к нулю. Алгоритм работает по принципу накопления доказательств: если новые адреса появляются эпизодически, ничего не происходит; но, если они продолжают появляться стабильно, система «запоминает» это. Когда «накопленных доказательств» становится достаточно, срабатывает сигнал об атаке. Это позволяет отслеживать даже слабые, но продолжительные аномалии.

Система использует двухуровневую проверку.

Первый уровень предназначен для обнаружения простых атак: он ищет отдельные IP-адреса с аномально высоким трафиком, что эффективно против атак от одного или нескольких источников.

Второй уровень (основной) предназначен для обнаружения распределенных атак: он мониторит именно долю новых IP-адресов и способен выявить «тихие» атаки с тысячью источников, каждый из которых отправляет мало данных.

Когда атака обнаружена, система реагирует. Активируется фильтр, который ограничивает трафик с новых, подозрительных IP-адресов. Если атака прекращается, фильтр отключается. В нормальном режиме система продолжает фоновое обучение, обновляя базу данных легитимных адресов.

Результаты тестирования показали высокую эффективность данного метода. Точность обнаружения очень высока: на границе сети (first-mile) – 99 % точности даже при всего 2 новых IP-адресах в атаке; перед сервером (last-mile) – 100 % точности при 18 новых IP-адресах. Срабатывание происходит быстро – в течение 10–80 секунд, при этом система не дает ложных срабатываний на легитимных всплесках трафика, в отличие от методов, основанных на объеме. Важно, что нагрузка на систему низкая: в тестах она обрабатывала трафик со скоростью до 10 Гбит/с, используя при этом мало вычислительных ресурсов.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Преимущества метода заключаются в нескольких аспектах.

Во-первых, его сложно обойти атакующему. Чтобы избежать обнаружения, злоумышленнику нужно использовать только «старые» IP-адреса из базы данных жертвы. Но для этого требуется провести предварительную разведку, чтобы «засветить» эти адреса в легитимном трафике, или использовать реальные, подконтрольные компьютеры, которые затем можно будет отследить и заблокировать.

Во-вторых, метод эффективно работает против современных, изощренных атак, особенно высокораспределенных (тысячи источников) и «тихих» (мало трафика от каждого источника).

В-третьих, он универсален и может быть развернут в разных точках сети: на границе интернет-провайдера, перед сервером или в центре обработки данных.

Практический пример наглядно показывает разницу. Ситуация: популярный сайт объявляет конкурс, и на него приходят тысячи легитимных пользователей. Старая система защиты, анализирующая объем, увидит резкий рост трафика, решит, что это DDoS-атака, и заблокирует доступ, оставив реальных пользователей за бортом. Новая система SIM поступит иначе: она посмотрит на IP-адреса, увидит, что большинство из них уже были на сайте ранее, сделает вывод о легитимности всплеска и пропустит всех пользователей.

Будущее развитие метода включает в себя комбинацию с другими параметрами трафика для повышения точности, создание распределенной системы обнаружения, где несколько узлов обмениваются данными, и адаптацию под новые сетевые технологии, такие как IPv6 и облачные сервисы.

Таким образом, метод SIM принципиально меняет подход к защите от DDoS-атак, смещая фокус с вопроса «сколько трафика?» на вопрос «кто отправляет трафик?». Это позволяет точно отличать реальные атаки от нормальной активности и обеспечивать эффективную защиту даже от самых сложных и распределенных угроз [9].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Российские исследователи проблемы DDOS-атак были О.С. Терновой и А.С. Шатохин в 2012 году выявили следующие проблемы [10]:

1. Позднее обнаружение: если злоумышленник начинает атаку постепенно («тихую» разведку или медленное наращивание), статистические границы, рассчитанные по последним данным, также плавно сдвигаются, и атака долго остается незамеченной.

2. Ложные срабатывания: сетевая нагрузка закономерно меняется в течение дня, недели (например, рост в рабочее время, спад ночью и в выходные). Метод без учета этих циклов либо дает много ложных тревог (при коротком периоде анализа), либо пропускает реальные атаки в периоды низкой нагрузки (при длительном периоде анализа).

Предлагаемое ими решение – учет сезонности (цикличности) трафика. Оно подразумевает:

– структурирование данных: сетевой трафик (например, количество запросов в час) представляется в виде матрицы, где каждая строка – сутки, а каждый столбец – одинаковый час в этих сутках;

– анализ по «похожим» периодам: вместо анализа последовательных интервалов времени, для вычисления нормальных значений и границ аномалий используются данные из одинаковых временных слотов разных дней;

– исключение аномальных периодов: из анализа исключаются данные праздников и выходных, чтобы сравнение было релевантным.

Предлагаемый подход был протестирован на реальных логах веб-серверов Apache, содержащих как нормальный трафик, так и периоды DDoS-атак. С учетом сезонности он позволил обнаружить атаку в 4 раза быстрее, чем традиционные методы при значительном сокращении числа ложных срабатываний [10].

Также в 2013 году Е.В. Щерба и Д.А. Волков разработали систему обнаружения DDoS-атак на основе моделирования сети как системы массового обслуживания и оценки вероятности потери заявок [11].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Основная идея подхода заключается в том, чтобы сначала изучить, как сеть ведет себя в нормальных условиях, и зафиксировать эталонные показатели трафика. Затем, в режиме реального времени, система ищет отклонения от этой нормы. Для анализа могут использоваться различные статистические методы, но ни один из них не является универсальным решением.

В качестве математической основы авторы предлагают использовать теорию массового обслуживания. Сеть моделируется как система очередей, где поступающие запросы (заявки) обрабатываются узлами. Если узел перегружен и его очередь заполнена, запрос теряется. В нормальном режиме работы вероятность такой потери невелика и стабильна.

Суть метода обнаружения атаки сводится к непрерывной оценке вероятности потери запросов в этой модели. Когда начинается DDoS-атака, поток запросов резко возрастает, узлы перегружаются, очереди заполняются, и вероятность потерь значительно увеличивается. Система отслеживает этот скачок и интерпретирует его как признак атаки.

Для реализации этого принципа авторы разработали архитектуру системы, которая циклически выполняет следующие действия: сбор статистики о трафике; обновление параметров математической модели сети; расчет текущей вероятности потерь и сравнение ее с пороговым значением (превышение порога приводит к генерации сигнала об атаке).

Важным ограничением метода является его зависимость от стабильного, установившегося режима работы сети. Метод хорошо работает, когда сеть находится в равновесии, но во время самого начала атаки или в другие моменты резкого изменения нагрузки возникает переходный процесс. В этот период модель может давать неточные результаты, и атака может остаться незамеченной или быть определенной с задержкой. Авторы отмечают, что оценка длительности этого переходного периода и сравнение эффективности их метода с другими подходами – это задачи для будущих исследований [11].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

А в 2023 году А.С. Клименкова проводила исследование задач по кибербезопасности, что позволило перейти от пассивных методов защиты к адаптивным стратегиям, учитывающим поведение злоумышленника [12]. Это заложило основу для создания интеллектуальных систем, таких как Syncookied, которые не только фильтруют трафик, но и динамически оптимизируют параметры защиты на основе модели «защитник–нарушитель» с использованием концепции равновесия Нэша.

Процесс работы системы Syncookied начинается с этапа обнаружения DDoS-атаки, например, SYN-флуда, на защищаемый сервер. Такая атака характеризуется массовой отправкой SYN-пакетов с целью исчерпания ресурсов сервера на установление соединений.

После выявления аномальной активности система активирует механизм защиты. На маршрутизаторе настраивается статическая привязка IP-адреса атакуемого сервера к Media Access Control (MAC)-адресу межсетевого экрана. В результате весь входящий трафик, предназначенный для сервера, перенаправляется не напрямую, а через этот экран, который обладает большей пропускной способностью и вычислительными ресурсами для обработки атаки.

Когда межсетевой экран получает SYN-пакет, он не создает запись о соединении в своей таблице состояний, как это делает обычный сервер. Вместо этого он использует механизм SYN-cookie. Этот механизм позволяет сгенерировать ответный SYN-ACK пакет, в котором номер последовательности (sequence number) кодирует информацию о соединении. Cookie формируется криптографически стойким способом на основе алгоритма SHA1, секретного ключа, метки времени и основных параметров соединения – IP-адресов и портов отправителя и получателя.

Использование метки времени накладывает ограничение на время жизни cookie, например, пакет, пришедший через час, будет считаться невалидным.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Этот подход кардинально снижает нагрузку на память и процессор, так как состояние соединения не хранится, а восстанавливается из самого cookie при получении подтверждающего ACK-пакета от клиента.

Если клиент является легитимным и отвечает ACK-пакетом, то этот пакет будет содержать номер подтверждения (acknowledgment number), который на единицу больше сгенерированного cookie.

Межсетевой экран, получив ACK, проверяет его валидность: расшифровывает cookie, сверяет метку времени и секретный ключ. Если проверка проходит успешно, экран понимает, что это ответ на его же SYN-ACK, и что соединение должно быть установлено. Затем он меняет в пакете MAC-адрес на MAC-адрес настоящего защищаемого сервера и отправляет пакет дальше в сеть. Защищаемый сервер получает ACK-пакет, считает, что тройное рукопожатие прошло успешно, и переводит соединение в состояние ESTABLISHED. Если же cookie невалиден или истек его срок, пакет безжалостно отбрасывается. Таким образом, атакующие пакеты, которые не завершают рукопожатие, не доходят до сервера и не расходуют его ресурсы.

После установления соединения система продолжает его отслеживать, ведя таблицу состояний для уже валидированных сессий. В ней фиксируются состояния типа Established, Closing, а также таймауты для неактивных соединений. Это позволяет корректно завершать сессии и освобождать ресурсы. После того как интенсивность атаки снижается до нормального уровня, система защиты отключается. Для этого на маршрутизаторе удаляется статическая привязка, и весь трафик снова начинает поступать напрямую к целевому серверу, при этом уже установленные соединения не разрываются.

Параллельно с этим техническим механизмом функционирует теоретико-игровая модель, которая формализует конфликт между защитником (администратором сети) и нарушителем (злоумышленником, инициирующим DDoS-атаку).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

В этой статической игре каждый игрок выбирает свою стратегию, стремясь максимизировать собственную полезность.

Стратегией защитника является выбор двух ключевых пороговых значений: E_1 и E_2 (причем $E_2 < E_1$). Эти пороги используются для классификации входящего трафика от каждого IP-адреса (узла) на основе общей полосы пропускания, которую потребляют его потоки (ru).

Стратегией атакующего является выбор количества контролируемых им узлов (m) и количества атакующих потоков (u), запускаемых с каждого узла.

На основе порогов E_1 и E_2 строятся две сигмоидные функции-фильтры, $F_1(x)$ и $F_2(x)$, где x – это общая потребляемая узлом полоса пропускания. Эти S-образные кривые моделируют вероятностное решение брандмауэра:

– $F_1(x)$ определяет вероятность безусловного отбрасывания (drop) пакетов от узла. Она близка к нулю при низком x и резко возрастает, приближаясь к единице, когда x превышает порог E_1;

– $F_2(x)$ определяет вероятность перенаправления (redirect) трафика в специальную ловушку (honeypot). Она активируется на более низком пороге E_2.

Из этих двух функций выводятся три итоговые вероятности для трафика от любого узла:

– вероятность быть отброшенным: $F_d = F_1(x)$;

– вероятность быть перенаправленным в ловушку: $F_r = F_2(x)\,(1 - F_1(x))$;

– вероятность быть пропущенным к целевому серверу: $F_a = (1 - F_1(x)) \times (1 - F_2(x))$.

Ловушка служит для изучения тактики атакующего и отвлечения его ресурсов, но ее использование сопряжено с затратами для защитника.

Выигрыш (полезность) каждого игрока формализуется как взвешенная сумма нескольких компонентов.

Для атакующего (V^a) это:

– положительный вклад от доли захваченной им полосы пропускания (V_b^d);

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

– положительный вклад от доли потерянных легитимных потоков (V_n^d);

– отрицательный вклад от затрат на контроль атакующих узлов (V_c);

– отрицательный вклад от потоков, перенаправленных в ловушку (V_h^d).

Для защитника (V^d) компоненты те же, но с противоположными знаками: он стремится минимизировать ущерб от захвата полосы и потери легитимного трафика, но получает выгоду от затрат атакующего и от перенаправления трафика в ловушку (получение разведданных). Весовые коэффициенты (w) отражают важность каждого компонента для соответствующего игрока.

Цель анализа – найти равновесие Нэша в этой игре, то есть такой набор стратегий (m, u, E_1, E_2), при котором ни атакующий, ни защитник не могут в одиночку изменить свою стратегию и увеличить свой выигрыш, если противник свою стратегию не меняет. Это состояние представляет собой устойчивое, оптимальное с точки зрения теории игр решение конфликта [12].

Таким образом, инновационные подходы к защите веб-серверов от DDoS-атак опираются на методы искусственного интеллекта и нейронных сетей: анализируется не только объем трафика, но и его поведенческие характеристики, и сравниваются текущие параметры с моделями нормального трафика; производится фильтрация по количеству сетевых переходов; вместо анализа объема трафика отслеживается появление новых IP-адресов; учет сезонности (цикличности) трафика; непрерывная оценка вероятности потери запросов; применение адаптивных стратегий, учитывающих поведение злоумышленника и позволяющих динамически оптимизировать параметры защиты.

Заключение

Проведенное исследование показало, что:

1. Классические подходы к защите веб-серверов от DDoS-атак обладают рядом существенных ограничений, не позволяющим эффективно противостоять современным многофакторным и распределенным атакам.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

При этом предъявляются высокие требованиями к вычислительным ресурсам и квалификации персонала.

2. Инновационные подходы к защите веб-серверов от DDoS-атак опираются на методы искусственного интеллекта и нейронных сетей, что позволяет им производить анализ вида атаки и адаптироваться к ней.

3. Полученные результаты обусловливают перспективность применения методов искусственного интеллекта и нейронных сетей для анализа сетевого трафика и выявления сложных паттернов аномалий.

Литература

1. Георгица И.В., Гончаров С.А., Мохов В.А. Мультиагентное моделирование сетевой атаки типа DDoS// Инженерный вестник Дона. 2013, № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852/.

2. Бекенева Я.А. Анализ актуальных типов DDoS-атак и методов защиты от них. Известия СПбГЭТУ «ЛЭТИ». 2016. № 7. С. 7–12.

3. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня. Вопросы кибербезопасности. 2017. № 5. С. 23–29.

4. Абрамов Е.С., Тарасов Я.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона. 2017, № 3 URL: ivdon.ru/ru/magazine/archive/N3y2017/4354/.

5. Басканов А.Н. Способы противодействия и средства раннего выявления DDoS-атак. Экономика и качество связи. 2022. № 3. С. 68–75.

6. Пальчевский Е.В., Христодуло О.И. Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак. Программные продукты и системы. 2019. Т. 32. № 4. С. 613–627.

7. Mirkovic J., Reiher P. D-WARD: DDoS Network Attack Recognition and Defense: Dissertation Prospectus. 2002. 28 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

8. Jin C., Wang H., Shin K.G. Hop-count filtering: An effective defense against spoofed DDoS traffic. II Proc. of 10th ACM Conference on Computer and Communications Security. Washington, October 27–30 2003. Pp. 30–41.

9. Peng T., Leckie C., Ramamohanarao K. Proactively detecting distributed denial of service attacks using source IP address monitoring. International conference on research in networking. Athens, Greece, 9–14 May 2004. Pp. 771-782.

10. Терновой О.С., Шатохин А.С. Раннее обнаружение DDOS-атак статистическими методами при учете сезонности. Доклады ТУСУР. 2012. № 1 (25). Часть 1. С. 104–107.

11. Щерба Е.В., Волков Д.А. Разработка системы обнаружения распределенных сетевых атак типа «отказ в обслуживании». Прикладная дискретная математика. Приложение. 2013. № 6. URL: cyberleninka.ru/article/n/razrabotka-sistemy-obnaruzheniya-raspredelyonnyh-setevyh-atak-tipa-otkaz-v-obsluzhivanii (дата обращения: 10.12.2025).

12. Клименкова А.С. Приложение, реализующее систему защиты Syncookied от DDOS-атак с использованием элементов теории игр. Математические структуры и моделирование. Омск: Омский государственный университет, 2023. № 1 (65). С. 86–107.

References

1. Georgitsa I.V., Goncharov S.A., Mokhov V.A. Inzhenernyj vestnik Dona. 2013, № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852/.

2. Bekeneva YA.A. Izvestiya SPBG·ETU «L·ETI». 2016. № 7. Pp. 7–12.

3. Tarasov YA.V. Voprosy kiberbezopasnosti. 2017. № 5. Pp. 23–29.

4. Abramov YE.S., Tarasov YA.V. Inzhenernyj vestnik Dona. 2017, № 3. URL: ivdon.ru/ru/magazine/archive/N3y2017/4354/.

5. Baskanov A.N. Ekonomika i kachestvo svyazi. 2022. № 3. Pp. 68–75.

6. Pal'chevskiy YE.V., Khristodulo O.I. Programmnye produkty i sistemy. 2019. T. 32. № 4. Pp. 613–627.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

7. Mirkovic J., Reiher P. D-WARD: DDoS Network Attack Recognition and Defense: Dissertation Prospectus. 2002. 28 p.

8. Jin C., Wang H., Shin K.G. Hop-count filtering: An effective defense against spoofed DDoS traffic. II Proc. of 10th ACM Conference on Computer and Communications Security. Washington, October 27–30 2003. Pp. 30–41.

9. Peng T., Leckie C., Ramamohanarao K. International conference on research in networking. Athens, Greece, 9–14 May 2004. Pp. 771-782.

10. Ternovoy O.S., Shatokhin A.S. Ranneye obnaruzheniye DDOS-atak statisticheskimi metodami pri uchete sezonnosti. Doklady TUSUR. 2012. № 1 (25). Chast' 1. Pp. 104–107.

11. Shcherba YE.V., Volkov D.A. Prikladnaya diskretnaya matematika. Prilozheniye. 2013. № 6. URL: cyberleninka.ru/article/ n/razrabotka-sistemy-obnaruzheniya-raspredelyonnyh-setevyh-atak-tipa-otkaz-v-obsluzhivanii (data obrashcheniya: 10.12.2025).

12. Klimenkova A.S. Prilozheniye, realizuyushcheye sistemu zashchity Syncookied ot DDOS-atak s ispol'zovaniyem elementov teorii igr. Matematicheskiye struktury i modelirovaniye. Omsk: Omskiy gosudarstvennyy universitet, 2023. № 1 (65). Pp. 86–107.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 14.12.2025

Дата публикации: 7.02.2026

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026