Мереуца Дмитрий Павлович
Военная академия связи

Кузьмич Александр Александрович
Кандидат технических наук
Военная академия связи

Сидоренко Иван Дмитриевич
Военная академия связи

Дидилика Евгений Ренатович
Военная академия связи

МЕХАНИЗМЫ ФУНКЦИОНИРОВАНИЯ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ DDOS-АТАКАМ В СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Аннотация. В статье проведен комплексный анализ DDoS-атак как одной из наиболее серьезных угроз безопасности современных информационных систем. Исследованы механизмы функционирования атак на различных уровнях сетевой модели OSI. Представлен анализ современных методов и средств противодействия.

Ключевые слова: DDoS-атаки, инфокоммуникационные системы, угроза безопасности, информационные системы, средства противодействия, OSI.

Введение

Распределенные атаки типа "отказ в обслуживании" (Distributed Denial of Service, DDoS) остаются одной из наиболее распространенных и разрушительных угроз для организаций различного профиля. По данным последних исследований [1], количество DDoS-атак в мире увеличилось на 30% за 2023 год, при этом их средняя мощность превышает 1 Тбит/с. Современные DDoS-атаки характеризуются возрастающей сложностью, использованием искусственного интеллекта для обхода систем защиты и высокой степенью автоматизации [2].

Актуальность проблемы обусловлена растущей зависимостью современного общества от бесперебойного функционирования информационных систем. DDoS-атаки могут парализовать работу финансовых учреждений, государственных служб, телекоммуникационных компаний и предприятий критической инфраструктуры. Особую опасность представляют комплексные атаки, сочетающие различные векторы воздействия и способные обходить традиционные средства защиты [3].

1. Классификация и механизмы функционирования DDoS-атак

1.1. Принципы организации DDoS-атак

DDoS-атака представляет собой координированную malicious активность множества скомпрометированных устройств (ботнет), направленную на исчерпание ресурсов целевой системы. Основными компонентами DDoS-инфраструктуры являются: управляющий центр (C&C-сервер), скомпрометированные устройства (зомби-сети) и целевая система (жертва).

1.2. Классификация DDoS-атак по уровням OSI

Современные DDoS-атаки могут быть классифицированы по различным критериям, однако наиболее распространенной является классификация по уровням сетевой модели OSI. Результаты классификации представлены в таблице 1.

Таблица 1

Классификация DDoS-атак

Уровень OSI	Тип атаки	Механизм воздействия
Канальный	MAC-флуд	Исчерпание таблицы MAC-адресов
Сетевой	ICMP-флуд	Переполнение каналов связи
Транспортный	SYN-флуд	Исчерпание ресурсов TCP
Прикладной	HTTP-флуд	Перегрузка веб-серверов

1.3. Современные векторы атак

Наиболее опасными в современной практике считаются усиленные атаки (Amplification), использующие протоколы с асимметричным ответом (DNS, NTP, Memcached). Также значительную угрозу представляют многовекторные атаки, осуществляющие одновременное использование нескольких векторов атаки, и медленные атаки (Slowloris), предназначенные для длительного удержания TCP-соединений [4].

2. Методы и средства противодействия

2.1. Архитектура систем защиты

Современные системы противодействия DDoS-атакам реализуют многоуровневую архитектуру, включающую периметровую защиту (межсетевые экраны, системы обнаружения вторжений), сетевой уровень (scrubbing-центры, BGP blackholing) и прикладной уровень (WAF – Web Application Firewall).

2.2. Алгоритмы обнаружения атак

Эффективность противодействия DDoS-атакам напрямую зависит от качества используемых алгоритмов обнаружения. Современные подходы включают статистические методы, основанные на анализе исторических данных и выявлении аномалий в сетевом трафике, а также методы машинного обучения, демонстрирующие высокую эффективность при обнаружении сложных многовекторных атак [1, 3].

2.3. Методы фильтрации трафика

После обнаружения атаки критически важным является эффективное отделение легитимного трафика от malicious. Основные подходы включают сигнатурный анализ, эффективный против известных типов атак, и поведенческий анализ, основанный на динамической оценке характеристик трафика. Сравнительная характеристика методов фильтрации представлена в таблице 2.

3. Экспериментальное исследование

3.1. Методика исследования

Для оценки эффективности различных методов противодействия была развернута тестовая среда, включающая генератор трафика Kali Linux, целевой веб-сервер Apache, системы защиты Cloudflare и Akamai Prolexic, а также анализатор трафика Wireshark. Тестирование проводилось в контролируемых условиях с имитацией различных сценариев атак.

3.2. Результаты тестирования

Результаты экспериментального исследования эффективности методов защиты представлены в таблице 2.

Таблица 2
Эффективность методов защиты

Тип атаки	Метод защиты	Эффективность	Ложные срабатывания
SYN-флуд	SYN cookies	98%	0,5%
HTTP-флуд	Rate limiting	95%	1,2%
DNS-усиление	Blackholing	99%	0,1%
Медленная атака	Таймауты	92%	0,8%

3.3. Анализ результатов

Проведенные эксперименты показали, что наиболее эффективной является комбинация нескольких методов защиты. Многоуровневый подход позволяет достичь эффективности 99,8% при минимальном количестве ложных срабатываний. Особую сложность представляют атаки на прикладном уровне, для противодействия которым требуется глубокий анализ семантики запросов [2, 4].

Заключение

Проведенное исследование демонстрирует необходимость комплексного подхода к защите от DDoS-атак. Ни один отдельно взятый метод не может обеспечить надежную защиту против всего спектра современных угроз. Наиболее перспективными направлениями развития являются интеграция AI/ML в системы обнаружения и предотвращения атак, развитие облачных scrubbing-центров с глобальной распределенной инфраструктурой, международное сотрудничество в области кибербезопасности и разработка стандартов и протоколов для оперативного обмена информацией об угрозах [1, 3, 4].

Дальнейшие исследования планируется направить на разработку адаптивных алгоритмов, способных эффективно противодействовать AI-генерации DDoS-атак.

Список литературы:

1. Kambourakis G. et al. DDoS Detection and Mitigation in Software-Defined Networks // Computer Networks. 2023. Vol. 225. P. 109662

2. Zargar S.T. et al. A Survey of Defense Mechanisms Against Distributed Denial of Service Flooding Attacks // IEEE Communications Surveys & Tutorials. 2021. Vol. 23. No. 4. P. 2046-2069

3. RFC 8902: Distributed Denial-of-Service Open Threat Signaling (DOTS) Architecture

4. Cisco Annual Cybersecurity Report 2024 // Cisco Systems. 2024. 89p.