Обзорная статья
УДК 004.056.52; DOI: 10.61260/2218-13X-2024-2-105-125

ОБЗОР ПУБЛИКАЦИЙ ЗАРУБЕЖНОГО СЕГМЕНТА ПО БЕЗОПАСНОСТИ VOIP-СЕТЕЙ: ГЕНЕРАЦИЯ DOS-АТАК И ИХ ОБНАРУЖЕНИЕ

✉Макарова Александра Константиновна;
Поляничева Анна Валерьевна.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия.
Матвеев Александр Владимирович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉alex-ecureuil@mail.ru

Аннотация. Статья посвящена проблеме защиты VoIP-систем от Dos/DDos-атак, как одних из наиболее актуальных для области цифровой телекоммуникации. Произведен обзор существенного количества публикаций зарубежных ученых, посвященных методам, как создания данного рода атак, так и противодействия им. Предложена систематизация результатов исследования в виде сравнительной таблицы по 10 следующим критериям: год публикации, этап жизненного цикла атаки, ее тип, метод защиты, степень реализации, ее работоспособность, расход сетевого ресурса, практическая применимость, результативность метода, применение машинного обучения. Сделаны основополагающие выводы по каждому из критериев, дана краткая характеристика проведенного исследования, а также пути его продолжения.

Ключевые слова: VoIP, сравнительный анализ, отказ в обслуживании, DoS, атака, безопасность

Для цитирования: Макарова А.К., Поляничева А.В., Матвеев А.В. Обзор публикаций зарубежного сегмента по безопасности VoIP-сетей: генерация DoS-атак и их обнаружение // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 105–125. DOI: 10.61260/2218-13X-2024-2-105-125.

Review article

THE REVIEW OF FOREIGN SEGMENT PUBLICATIONS ON VOIP NETWORK SECURITY: GENERATION OF DOS ATTACKS AND THEIR DETECTION

✉Makarova Alexandra K.;
Polyanicheva Anna V.
Saint-Petersburg state university of telecommunications named after professor M.A. Bonch-Bruevich, Saint-Petersburg, Russia.
Matveev Alexander V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉alex-ecureuil@mail.ru

Abstract. The paper is devoted to the problem of protecting VoIP systems from DoS/DDoS attacks, as one of the most relevant for the field of digital telecommunications. A review of a significant number of publications by foreign scientists devoted to methods of creating this type of attack, as well as countering them, was carried out. A systematization of the review results is proposed in the form of a comparative table according to the following 10 criteria: year of publication, stage of the life cycle of the attack, its type, protection method, degree of implementation, its resource intensity, practical applicability, effectiveness of the method,

application of machine learning. Fundamental conclusions were drawn for each of the criteria, a brief description of the research was given, as well as ways to continue it.

Keywords: VoIP, benchmarking, denial of service, DoS, attack, security

For citation: Makarova A.K., Polyanicheva A.V., Matveev A.V. The review of foreign segment publications on VoIP network security: generation of DoS attacks and their detection // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 105–125. DOI: 10.61260/2218-13X-2024-2-105-125.

Введение

В настоящее время одной из наиболее распространенной и опасной (с позиции простоты реализации против наносимого ущерба) угрозой для «запрос-ответ» систем является DoS (*аббр. от* Denial of Service, *перев. на рус*. отказ в обслуживании) и ее масштабируемый аналог – DDoS (*аббр. от* Distributed Denial of Service, *перев. на рус.* распределенный отказ в обслуживании), реализуемый путем проведения соответствующих одноименных атак. Их применение к области VoIP (*аббр. от* Voice Over Internet Protocol, *перев. на русс.* голосовая связь через интернет) способно не только нарушить нормальное функционирование отдельных онлайн-сервисов, веб-сайтов и целых сетей, но и привести к масштабным утечкам конфиденциальных данных, а также истощить программно-аппаратные ресурсы элементов цифровой телекоммуникации. В результате крупные компании (в том числе и государственные) не только понесут огромные финансовые и репутационные потери, но и не смогут обеспечить критически важные каналы связи.

Суть проблемы может быть озвучена как противопоставление потребностей пользователей, использующих услуги VoIP, и возможностей злоумышленников, стремящихся нарушить предоставление данного рода услуг. Так, с одной стороны, само понятие VoIP предполагает оперативное обеспечение связи двух абонентов (то есть учет ограничений по времени). С другой стороны, проведение злоумышленником DoS/DDoS-атаки (например, путем отправки большого количества сетевых пакетов) приведет к временным задержкам в общении пользователей.

При этом сама «стоимость» реализации DoS-атаки может оказаться достаточно невысокой. Так, например, генерация в рамках атаки множества сетевых пакетов может оказаться существенно менее ресурсозатратной, чем их обработка конечными устройствами. Также существуют отдельные «серые» сервисы, которые предоставляют платные услуги по проведению подобного рода злонамеренных мероприятий на заданную кампанию.

Ситуация усложняется тем, что DoS- или DDoS-атаки могут быть первичным шагом для более масштабных во время того, как основное внимание специалистов сконцентрировано вокруг перегруженной и не отвечающей на запросы системе. Как результат, злоумышленники способны внедрить вредоносное программное обеспечение (ПО) или реализовать фишинг для кражи конфиденциальной информации или нарушения ее целостности, хотя изначально атака осуществляла истощение ресурсов сервисов, нарушая тем самым лишь их доступность. Подобное развитие событий может иметь далеко идущие последствия для целевых организаций и пользователей.

Первым шагом разрешения проблемы такого нарушения функционирования VoIP-систем может стать осознанный и многосторонний подход, заключающийся в анализе большого количества исследований в области противодействия DoS/DDoS-атакам; сравнительный анализ методов борьбы с ними позволит выделить наиболее эффективные, показавшие свою работоспособность. В интересах этого далее будет произведен обзор релевантных работ зарубежных ученых (за которым в будущем последует отдельный обзор российского публикационного сегмента) и их систематизация по авторскому набору критериев.

Обзор научных работ

Проведем обзор научных работ, рассматривающих безопасность VoIP-сетей с двух диаметрально противоположных сторон: генерации DoS/DDoS-атак и их обнаружения, выявив их полный жизненный цикл. Для этого были использованы международные базы

цитирования IEEE Explorer и Sciencedirect; в качестве основных ключевых запросов использовались следующие: SIP, DoS и их синонимические аналоги (для лучшей информативности будем перед каждым обзором указывать его переводное название).

C_1. Системы сетевой безопасности для противодействия атакам типа «отказ в обслуживании» на основе SIP

В исследовании [1] рассматриваются различные подходы к противодействию трем наиболее частым типам DoS-атак на VoIP: подделке полезной нагрузки SIP-сообщений, потока самих сообщений и их лавинной рассылке. Указаны механизмы реализации, произведена их классификация и сравнение методов защиты по общим критериям. Представлен список решений по противодействию, хорошо себя зарекомендовавший с точки зрения практического опыта исследователей. Сделаны следующие выводы касательно обеспечения безопасности VoIP: атаки первого типа оперативно отражаются с помощью корректной и отказоустойчивой реализации синтаксического анализатора, а атаки второго типа – путем шифрования сообщений. Наиболее сложным остается защита от атак третьего типа, хоть и указаны несколько многообещающих подходов.

C_2. Схема защиты с использованием Cloud SFW

В работе [2] анализируются угрозы безопасности SIP, на основе чего строятся модели DoS-атаки на SIP и ее защиты, используя теорию очередей; предлагается эффективная схема защиты от атак. Данный подход реализует преимущества новых SDN (*аббр. от* Software Defined Networks*, перев. на русс.* программно-определяемые сети) и облачный SFW (*аббр. от* SIP Fire Wall *перев. на русс.* межсетевой экран SIP), значительно повышая производительность защиты от DoS-атак на SIP. Также авторы проводят эксперименты для проверки работоспособности и эффективности разработанной схемы защиты, которые показывают повышение производительности облачного SFW и экономии полосы пропускания во время атаки.

C_3. Использование SVM для обнаружения аномалий в потоке SIP-сообщений

Работа [3] посвящена разработке онлайн-фильтра, который анализирует поток входящих SIP-сообщений с целью их двухэтапной классификации на «хорошие» и «плохие». Описывается общая архитектура фильтра и исследуются несколько точек конфигурационного пространства SVM для определения необходимых параметров конфигурации, которые будут работать для классификации большой выборки SIP-сообщений, полученных из собранного трафика. Подход «обучения на примере», который применяется во втором этапе, основан на использовании классифицированных на первом этапе сообщений. Для реализации такого машинного обучения применяется метод опорных векторов (*аббр. на англ.* SVM).

C_4. Исследование методов обнаружения DoS-атак на базе SIP

Публикация [4] посвящена исследованию механизмов защиты VoIP-систем путем собственного обзора опубликованных работ и сравнению двух выбранных наиболее перспективных механизмов обнаружения аномалий в потоке SIP. Первый метод (автор – Л. Карвахал) заключается в обнаружении незащищенного VoIP-трафика на основе SIP. Алгоритм метода реализован на языке C и описывается тремя этапами: сбор сетевого трафика, анализ заголовков пакетов и обнаружение незащищенных VoIP-пакетов на основе SIP. Второй метод (авторы – Д. Голайт и Н. Хуббали) заключается в вероятностном обнаружении флуда при передаче голоса по IP. Разработанная система VoIPFD (*аббр. от* Voice Over IP Flooding Detection, *перев. на русс.* обнаружение флуда при передаче голоса

по IP) основана на алгоритме обнаружения аномалий, который имеет два классических для машинного обучения этапа: обучение и тестирование.

C_5. Механизм защиты, основанный на очереди классов приоритета

В публикации [5] разрабатывается математическая система выявления DoS-атак в VoIP-сетях на основе модели анализа очередей M/M/1/K (обозначает систему массового обслуживания с марковскими поступлениями, экспоненциальным распределением времени обслуживания, одним сервером и конечной общей емкостью системы). Также предлагается механизм защиты от DoS-атак, позволяющий уменьшить влияние сервера при лавинной атаке INVITE (то есть приглашение пользователя к сеансу связи) вводом приоритетной очереди. Авторы используют аппарат моделирования для анализа эффективности защитного механизма, разработанного в рамках статьи. Полученные в статье результаты доказывают, что механизм защиты от SIP DoS-атак не только корректно продлевает время обслуживания SIP-сервера, но также обеспечивает дифференциацию законного SIP-сообщения от потока атаки.

C_6. Реализация плагина на основе принципа сбалансированного количества сообщений

В работе [6] исследуется путь улучшения производительности механизма обнаружения DoS-атак в SIP. Предлагается принцип, основанный на сбалансированном количестве сообщений, который способен отражать информацию о SIP-прокси более результативно, чем ALAS (*аббр. от* Application Layer Attack Sensor*, перев. на русс.* датчик атаки прикладного уровня), а также позволяет избежать два критичных недостатка последнего метода. Авторское решение имеет вид продукта, названного как «Плагин обнаружения SIP DoS-атак»; также создана платформа для тестирования плагина на реальных данных вызовов. Описанный механизм обеспечивает более высокую достоверность и точность обнаружения атак INVITE-флудинга.

C_7. Злоупотребление аутентификацией на объекты SIP

Работа [7] посвящена разработке нового метода обнаружения аномалий на основе профиля пользователя для выявления DOS-атак, которые некорректно используют механизм аутентификации SIP. Предлагаемый метод реализуется с помощью функций, которые используются в определенных профилях пользователей и основаны на их успешной аутентификации, а также количестве неудачных попыток аутентификации за заданный период времени. Метод способен обнаруживать неправильно используемые URI (*аббр. от* Uniform Resource Identifier*, перев. на русс.* унифицированный идентификатор ресурса) из локального домена, а его выходные данные могут быть использованы системой реагирования на вторжения для блокировки пользователей. Решение протестировано на спроектированном испытательном стенде с использованием программного обеспечения с открытым исходным кодом.

C_8. Защита с помощью фильтрации IP-адресов на основе истории

Работа [8] посвящена исследованию защиты сервера регистрации от DoS-атак с учетом загрузки центрального процессора (ЦП). Защита достигается путем блокировки SIP-пакетов из ранее неизвестных источников. Предлагаемый подход представляет собой облегченную версию IP-фильтрации на основе истории. Во время DoS-атаки метод способен блокировать атакующий трафик, позволяя тем самым легальным пакетам достигать конечных пользователей. В работе произведена эмпирическая оценка, которая показывает, что реализованный метод позволяет значительно уменьшить загрузку ЦП при DoS-атаках.

C_9. Формальный анализ на основе расширенных конечных автоматов SIP

В публикации [9] описан расширенный конечный автомат с параметрами, который используется для формального анализа DoS-атак на SIP. Данный метод был выбран авторами, так как он способен отразить структуру протокола в форме желательных или нежелательных состояний протокола и переходов между ними. Создана формальная модель описания SIP с использованием расширенного конечного автомата с параметрами, которая играет важную роль в проверке протокола, его синтезе и тестировании на соответствие. Также авторами представлена модель DoS-атаки на SIP и подробно исследован вопрос ее формального анализа на основе SIP EFSM (*аббр. от* Extended Finite State Machine, *перев. на русс.* расширенный конечный автомат).

C_10. Использование балансировщика нагрузки для обнаружения и смягчения последствий

Исследование [10] относится к разработке нового балансировщика нагрузки SIP для обнаружения низкоскоростных и многоатрибутных DDoS-атак, который основан на расстояние Хеллингера и использует модели и методы машинного обучения. Предложенная схема реализована на базе модификации прокси-сервера SIP kamailio с открытым исходным кодом. Для оценки разработанного балансировщика создана экспериментальная тестовая установка; также установлено, что полученные авторами результаты превосходят существующие схемы предотвращения DDoS-атак. Достигнут высокий уровень обнаружения DDoS-атаки по сравнению с адаптивным порогом и CUSUM-алгоритмы (статистический тест для проверки стабильности параметров модели на всей выборке). Авторы отмечают, что балансировщик нагрузки легко развертывается в реальные сети VoIP.

C_11. Обнаружение атак на IP-мультимедийную подсистему (IMS)

Работа [11] посвящена разработке нового подхода к обнаружению DoS-атак по SIP-сообщениям в архитектуре IMS (*аббр. от* IP Multimedia Subsystem, *перев. на русс.* IP-мультимедийная подсистема). Полученное решение основано на алгоритме непараметрической кумулятивной суммы (CUSUM), а в качестве атаки используется флуд REGISTER (отправка большого количества пакетов SIP REGISTER на SIP-сервер). Производительность предложенного авторами алгоритма была оценена с использованием платформы Open IMS Core. Результат оценки показал, что атаки SIP-флудинга выводят из строя сервер IMS за достаточно короткое время, а разработанный непараметрический метод CUSUM позволяет их эффективно выявлять, что, соответственно, повышает и общую эффективность противодействия.

C_12. Механизм защиты, основанный на индивидуальном взвешенном справедливом планировании очереди

В публикации [12] авторами предложен новый механизм защиты от лавинной атаки INVITE DoS, основанный на CWFQ (*аббр. от англ.* Custom Weighted Fair Queue, *перев. на русс.* организация очередей на основе классов) путем классификации сообщений, не являющихся INVITE или состоящих из правильного SIP-сообщения, а также сообщений об атаке лавинной рассылки INVTE. Сообщения INVITE подразделяются на очереди сообщений, состоящих из легальных и нелегальных. Поскольку нелегальные сообщения INVITE помещаются в очередь с низким приоритетом, они с большой вероятностью будут отброшены при перегрузке SIP-сервера. Результат моделирования доказывает, что

предложенная авторами схема более эффективна, чем очередь FIFO (*аббр. от* First In, First Out, *перев. на русс.* первым пришёл – первым ушёл) и PQ (*аббр. от* Priority Queue, *перев. на русс.* очередь приоритетов) для защиты от атаки INVITE-атак.

C_13. Подход с использованием белого списка

Авторы исследования [13] предлагают использовать белый список как стратегию защиты от лавинных атак, обосновывая это тем, что таким образом хранится более полная и актуальная информация о легальных SIP-клиентах без какой-либо интеграции с SIP-сервером. Исходя из того, что большинство SIP-клиентов, как правило, имеют постоянное соединение со своим сервером, белый список легко поддерживаем. Согласно мнению авторов, реализация метода достаточно проста, поскольку она не требует интеграции с SIP-сервером. В экспериментальную оценку было включено влияние различных атак на SIP-сервер (различной мощности) и оценка эффективности авторского подхода. В качестве ограничения применимости решения указано снижение эффективности при противодействии атаками от крупных ботнетов (компьютерных сетей, сформированных из большого количества узлов с запущенными ботами), состоящих из взломанных точек связи с действующими учетными записями пользователя. Преодолеть это ограничение возможно объединив предложенный подход с каким-либо механизмом «черного списка», таким как PIKE (модуль, предоставляющий простой механизм защиты от DoS на основе флуда на сетевом уровне) в SER (*аббр. от* SIP Express Router*, перев. на русс.* SIP экспресс маршрутизатор).

C_14. Новая атака SR-DRDoS и эффективный механизм защиты

Работа [14] посвящена разработке новой атаки на основе SIP под названием «SR-DRDoS», которая использует менее известные функциональные уязвимости SIP путем применения техники IP-спуфинга и на основе отражения в сигнализации SIP на основе UDP (*аббр. от* User Datagram Protocol*, перев. на русс.* протокол пользовательских датаграмм). Кроме того, авторы предлагают инструмент «Mr. SIP», используемый ими для проведения атаки SR-DRDoS в смоделированной версии SIP-сети корпоративного уровня. Поскольку атака создает легитимный трафик в сети SIP с использованием методов отражения, она обходит черные списки, а также системы ограничения скорости по IP, количеству пакетов или сеансов/транзакций и автоматическое обнаружение сгенерированных сообщений (которые существуют в современных системах защиты). Также предлагается новый механизм защиты, который эффективно смягчает разработанную в данной статье атаку.

C_15. Расширенная атака флуда на SIP-сервер

Исследование [15] посвящено разработке улучшенной системы безопасности ISESS (*аббр. от* Improved Security-Enhanced SIP System*, перев. на русс.* улучшенная SIP-система с повышенной безопасностью), которая обеспечивает проверку одноразовых номеров с прогнозированием и приемом временных запросов вместе с протоколом синхронизации KASP (*аббр. от* Known Address Synchronisation Protocol*, перев. на русс.* протокол синхронизации известных адресов). Практическое преимущество данного решения заключается в простоте реализации и интегрируемости в систему за счет того, что оно является полностью серверным и не требует изменений в SIP-клиентах. В исследовании доказано, что ISESS смягчает атаки лавинной рассылки SIP-запросов INVITE/REGISTER и повышает производительность обслуживания легальных пользователей во время атаки. Также авторы указывают, что ISESS является мощной мерой противодействия другим типам SIP-флуд-атак.

C_16. Обзор практических систем безопасности для защиты систем VoIP

В работе [16] предлагается новый способ оценки критериев и сравнительное исследование идей исследователей на основе используемых моделей, сетевых архитектур и результатов. В дополнение даются рекомендации о том, как можно в дальнейшем противостоять атакам на сети VoIP. Разработана новая методика оценки, известная как набор критериев DADMV, который состоит из следующих основных групп: описание (Depiction), архитектура (Architecture), обнаружение (Detection), смягчение (Mitigation) последствий и проверка (Validation). Методика позволяет определить, какая VoIP-система лучше всего подходит для определенной компании.

C_17. Алгоритм смягчения последствий атак

Публикация [17] посвящена разработке новой схемы смягчения последствий для систем VoIP на основе SIP, включающей механизм защиты от DoS-атак на основе лавинной рассылки. Данная схема основана на обработке сообщений INVITE и BYE протокола SIP. Также разработан и реализован прототип системы для реализации DoS-атаки на основе лавинной рассылки. Авторами детально описаны этапы реализации механизма защиты в пользовательском пространстве, независимом от SIP-сервера, а также на SIP-сервере Asterisk. В результате тестирования эффективность предлагаемой системы оказалась выше, чем у других существующих механизмов.

C_18. Обнаружение DoS-атак на SIP-системы

В работе [18] разрабатывается метод обнаружения входящих SIP-сообщений от нелегитимных узлов. Авторы предлагают идентифицировать DoS-атаку путем подсчета количества нелегитимных транзакций и выявления ряда аномалий. Для этого модифицируются исходные конечные автоматы на основе SIP таким образом, чтобы можно было обнаружить аномалии с учетом состояний. Также используются четыре выбранных пороговых параметра для подтверждения атаки: UTE (верхняя граница количества разрешенных ошибок транзакций в секунду), UAE (максимальное количество сообщений в 300–699, которое можно принять в секунду), UT/N (верхняя граница количества разрешенных транзакций на узел) и UP/T (верхняя граница количества разрешенных пакетов). Если какое-либо пороговое значение достигнуто, система обнаружения поднимает тревогу. Предложенный в рамках работы метод способен обнаружить аномалии как в отдельном процессе, так и в узле.

C_19. Новый метод гарантии QoS для IPTV

Исследование [19] направлено на разработку нового механизма, гарантирующего сохранение качества обслуживания для сетей IPTV во время DOS-атак. В данный механизм введена процедура обслуживания передачи потокового мультимедиа, в которой динамически создаются новые сеансы с альтернативными медиа-серверами для замены сеансов с атакуемых серверов, чтобы гарантировать высокий уровень качества обслуживания. Создаются условия для обеспечения защиты от DOS-атаки, не отвлекая пользователя (то есть во время воспроизведения просматриваемого контента) за счет динамического изменения маршрутов к пользователям на более надежные и безопасные. При этом весь остальной трафик блокируется, чтобы гарантировать лучшие условия QoS для законных пользователей.

C_20. Байесовская модель точки изменения для обнаружения атак

В работе [20] разрабатывается байесовская модель множественных точек изменения для обнаружения DDoS-атак в сетях VoIP. Авторы предлагают платформу, работающую

с различными типами функций ввода, отслеживаемыми на прокси-сервере SIP. Решение отслеживает сетевой трафик и поведение SIP-сервера, а при обнаружении изменения в этом поведении – выдает сигнал тревоги. Кроме того, авторами разработана система вероятностного моделирования сети, которая способна генерировать последовательности сообщений SIP в реальном времени для установления телефонных соединений в сообществе УАТС (*сокр. от* учрежденческая автоматическая телефонная станция).

C_21. Обнаружение уязвимостей с использованием цветных сетей Петри

Исследование [21] посвящено экспериментальному применению формального метода «Цветных сетей Петри» как для обнаружения DoS-атак, так и в принципе при анализе безопасности протоколов. В результате эксперимента предложенный подход выявил уязвимое состояние транзакции INVITE, когда она на клиентской стороне находится в состоянии «Продолжение» после завершения транзакции сервера. Также была выявлена уязвимость в процессе настройки SIP-вызова, которая может быть использована для запуска DoS-атак на систему VoIP.

C_22. SIP Protector: защитная архитектура, смягчающая DDoS-атаки на SIP-серверы

В работе [22] описывается новая (то есть авторская) архитектура защиты и смягчения последствий DDoS-атак, направленных на различные типы инициализации протокола SIP. Архитектура построена на базе механизма перенаправления и сочетания фильтрации исходного и целевого трафика, используя преимущества всех методов. Обсуждаются сильные и слабые стороны разрабатываемого метода, предлагаются варианты его использования для других протоколов с аналогичным механизмом работы (например, HTTP при условии наличия механизма перенаправления).

C_23. Метод обнаружения и предотвращения на основе аномалий с использованием нечеткой логики

В работе [23] разрабатывается метод обнаружения DoS-атак в трафике протокола SIP, основанный на выявлении аномалий в различного типа пакетах сигнализации SIP. В интересах этого создается конечный автомат, с помощью которого из SIP-трафика извлекаются параметры и характеристики, используемые для дальнейшей работы метода. Решение имеет вид полностью реализованного прототипа, протестированного с помощью генератора трафика «Spirent». Предложенный метод подходит для обнаружения SIP-флуда любого типа.

C_24. Распределенная защита с помощью P4

Публикация [24] посвящена методу смягчения последствий DDoS-атак SIP INVITE с применением программирования плоскости данных и плоскости управления коммутаторов Ethernet. В ходе разработки авторы получили дополнительный компонент защиты, который можно добавить к существующим средствам обеспечения безопасности на основе пункта назначения, что позволит создать комплексное, расширяемое и экономичное решение. Поскольку концепции, представленные в статье, соответствуют SDN и NFV (*аббр. от* Network Function Virtualization*, перев. на русс.* виртуализация сетевых функций), данный метод может быть развернут в той же инфраструктуре.

C_25. Противодействие с помощью фильтров Блума

В рамках данного исследования [25] предложена схема по предотвращению DoS-атак, использующих DNS-запросы. Производится анализ причин, по которым DNS-запрос может занимать много больше положенного времени. В качестве решения предлагается схема

предотвращения атак с использованием фильтров Блума для внесения в черный список подозрительных DNS-серверов, что расширит возможности при ограниченном пространстве хранилища. В ходе исследования экспериментальная оценка показала, что разработанная схема эффективно предотвращает атаку с большим уровнем ложных срабатываний.

C_26. Смягчения последствий путем внедрения Snort

В работе [26] производится анализ и оценка контрмер, используемых для борьбы с DoS-атаками на VoIP. Авторы рассматривают различные схемы обнаружения и предотвращения DoS-атак, а также моделируют флуд-атаки (на основе SIP) против широко используемого SIP-сервера. В ходе работы также была разработана эмулированная испытательная среда, а результаты эксперимента послужили базой для предложения новой схемы смягчения последствий. Последняя заключается во внедрении Snort во встроенном режиме в качестве системы защиты от вторжений; Snort (бесплатная система предотвращения вторжений с открытым исходным кодом) используется вместе с Iptables (инструмент в Linux, который позволяет администраторам управлять входящими и исходящими пакетами данных) для обеспечения безопасности SIP-сервера.

C_27. Быстрое обнаружение скрытых атак SIP Flood в сетях VoIP

Работа [27] посвящена разработке метода обнаружения скрытой атаки SIP-флудом на основе вейвлетов. Предлагаемый метод позволяет извлекать информацию из необработанного трафика путем разложения сигнала на уровни. Таким образом, обнаруженный процент энергии, соответствующий подробному сигналу, способен быстро выявить изменения, вызванные незаметно начатой атакой, даже если она имеет слабое влияние на легальный трафик. Также, учитывая масштабируемость предлагаемой схемы, в качестве входных данных используется техника эскизов для предоставления управляемых необработанных сигналов трафика фиксированного размера для обнаружения на основе вейвлетов независимо от количества пользователей в сети.

C_28. Обнаружение атак с истощением ресурсов на беспроводные сети VoIP на основе SIP

В работе [28] анализируется относительно новый тип DoS-атаки, который использует расширение SIP для истощения ресурсов прокси-серверов VoIP. Реализация атаки возможна, если злоумышленник установит большое значение заголовка «Session-Expires», а затем физически отключится от беспроводной сети; как результат, при многократном повторении таких действий можно занимать и удерживать ресурсы прокси-сервера, приводя к их общему истощению. В качестве контрмеры авторы предлагают схему, основанную на статистическом тесте Андерсона-Дарлинга путем анализа характеристик как нормального, так и атакующего поведения.

C_29. Обнаружение затопления SIP на основе эскизов с использованием расстояния Хеллингера

Исследование [29] посвящено разработке онлайн-схемы обнаружения SIP-флуда путем совмещения двух методов: эскиза и расстояния Хеллингера. Для создания фиксированного размера потоков сигнальных сообщений SIP используется программа Sketch (позволяет суммировать трафик, связанный с одним или несколькими физическими атрибутами в заранее определенное количество состояний с помощью операции хеширования). Свойство произвольной агрегации эскиза обеспечивает гибкость для

суммирования многомерных пользовательских данных в гораздо меньшие объемы; расстояние Хеллингера используется для профилирования нормального поведения трафика и обнаружения атак на основе распределений вероятностей, определенных по соответствующим таблицам.

C_30. Ограничительная модель (RM)

В работе [30] описывается ограничительная модель обеспечения эффективного механизма борьбы с атакой INVITE Flooding, обладающая высокой оперативностью обнаружения. Предложенный подход основан на методе управления допуском вызовов для каждого потока. Эффективность результатов демонстрируется с помощью моделирования NS2 (*аббр. от* Network Simulator*, перев. на русс.* сетевой симулятор) с тремя основными параметрами оценки, а именно – использование буфера, потери пакетов и доступность сервиса. Большое внимание в работе уделено изучению поведения атак INVITE DoS/Flooding в SIP.

Сравнительный анализ

Для сравнительного анализа методов защиты от DoS/DDoS-атак на VoIP, представленных в проведенных обзорах зарубежных статей, выделены следующие критерии (отражающие суть и отличительные особенности решений):

К_1) год публикации статьи;
К_2) этап жизненного цикла атаки – ее генерация или обнаружение;
К_3) тип DoS/DDoS атак;
К_4) используемый подход к защите от атаки (метод, модель и т.п.);
К_5) реализован ли механизм защиты от Dos/DDos-атак на практике;
К_6) проверена ли работоспособность данного механизма защиты;
К_7) степень расхода сетевого ресурса;
К_8) данные о применимости защиты от атаки в реальных VoIP сетях;
К_9) результативность данного метода как степень чувствительности к обнаружению атак;
К_10) применение машинного обучения.

Результаты сравнительного анализа методов из обзоров по введенным критериям приведены в таблице, далее будет дана расшифровка их значений. Первый критерий имеет численное значение в виде соответствующего года публикации. Второй критерий содержит информацию о методе (относительно атаки) и может принимать интуитивно понятные и логичные значения – Ген. (*сокр. от* генерация), Обн. (*сокр. от* обнаружение), Ген./Обн. Третий и четвертый критерии содержат описания соответствующих атак и методов («–» в случае отсутствия). Также для более лаконичного обозначения типов атак для третьего критерия использованы следующие сокращения: A_P.T – Вмешательство в полезную нагрузку, A_PT.DR – DRDoS (новая), A_F. T – нарушение потока, A_F – флуд, A_F.I – INVITE флуд, A_F.R – REGISTER флуд, A_F.C – CANCEL флуд, A_F.B – BYE флуд, A_F.O – OPTIONS флуд. Пятый и шестой критерии могут принимать булевские значения – то есть «Да» или «Нет», а также промежуточное – «Час.» (*сокр. от* частично). Седьмой и девятый критерии оцениваются по шкале из трех значений (по мере возрастания соответствия): «Н» (*сокр. от* низкий), «С» (*сокр. от* средний) и «В» (*сокр. от* высокий); в случае отсутствия данных для получения значения критерия это будет указываться пометкой – «?». Восьмой и десятый критерии принимают одно из двух значений: «Да» или «Нет».

Таблица

Критериальное сравнение

Название статьи	К_1	К_2	К_3	К_4	К_5	К_6	К_7	К_8	К_9	К_10
Survey of network security systems to counter SIP-based denial-of-service attacks [1]	2009	Обн.	A_ PT, A_FT, A_F	–	Нет	Нет	?	Да	С	Нет
An Efficient Defense Scheme against SIP DoS Attack in SDN Using Cloud SFW [2]	2014	Ген./ Обн.	A_F.I	Теория очередей M/M/1, + SDN и Cloud SFW	Да	Да	Н	Нет	С	Нет
On the Use of SVMs to Detect Anomalies in a Stream of SIP Messages [3]	2012	Ген./ Обн.	A_ PT	Классификатор на основе SVM	Да	Час.	?	Нет	С	Да
Comparative study on DoS attacks Detection Techniques in SIP-based VoIP networks [4]	2018	Обн.	A_F	Алгоритм обнаружения незащищенного трафика; Система VoIPFD;	Да	Да	?	Да	С	Нет
A SIP DoS flooding attack defense mechanism based on priority class queue [5]	2010	Ген./ Обн.	A_F.I	Модель M/M/1I(K/2)	Да	Час.	?	Нет	С	Нет
The design and realization of SIP DoS attack detection plugin based on balanced message number principle [6]	2009	Ген./ Обн.	A_F.I	Принцип сбалансированного количества сообщений	Да	Да	?	Нет	Н	Нет
Detecting authentication misuse attacks against SIP entities [7]	2013	Ген./ Обн.	A_F.I, A_F.R	Алгоритм на основе обнаружения неправильной аутентификации	Да	Да	?	Нет	С	Нет
Protecting SIP server from CPU-based DoS attacks using history-based IP filtering [8]	2009	Ген./ Обн.	A_F.R	Фильтрация IP адресов на базе данных IAD	Да	Да	Н	Да	В	Нет
The Formal Analyse of DoS Attack to SIP Based on the SIP Extended Finite State Machines [9]	2010	Обн.	A_F.C, A_F.B	Модель расширенного конечного автомата	Нет	Нет	?	Нет	С	Нет
Leveraging the SIP load balancer to detect and mitigate DDos attacks [10]	2015	Ген./ Обн.	A_F.I, A_F.B	Балансировка нагрузки	Да	Да	Н	Нет	С	Да

Название статьи	К_1	К_2	К_3	К_4	К_5	К_6	К_7	К_8	К_9	К_10
Detecting SIP flooding attacks on IP Multimedia Subsystem (IMS) [11]	2012	Ген./ Обн.	A_F.R	Алгоритм непараметри-ческой кумулятивной суммы	Да	Час.	Н	Нет	В	Нет
A SIP DoS Flooding Attack Defense Mechanism Based on Custom Weighted Fair Queue Scheduling [12]	2010	Обн.	A_F.I	Классификация сообщений с CWFQ	Да	Да	?	Нет	С	Нет
A whitelist approach to protect SIP servers from flooding attacks [13]	2010	Ген./ Обн.	A_F	Белый список	Да	Да	Н	Да	С	Нет
A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism [14]	2020	Ген./ Обн.	A_PT.D R	Механизм защиты DRDoS	Да	Да	Н	Нет	С	Нет
Advanced Flooding Attack on a SIP Server [15]	2009	Обн.	A_F.I, A_F.R	Улучшенная система безопасности ISESS	Да	Час.	Н	Да	С	Нет
Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks [16]	2014	Обн.	A_ PT, A_FT, A_F	Критериальная оценка DADMV	Да	Час.	?	Нет	С	Нет
Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System [17]	2015	Ген./ Обн.	A_F.I, A_F.B	Алгоритм смягчения атак	Да	Да	Н	Нет	С	Нет
Detecting DoS attacks on SIP systems [18]	2006	Обн.	A_F	Метод обнаружения сообщений от нелегитимных узлов	Да	Да	Н	Да	С	Нет
A novel method to guarantee QoS during DOS attacks for IPTV using SIP [19]	2009	Обн.	A_FT	Механизм защиты с динамически создающимися новыми сеансами	Да	Нет	?	Нет	?	Нет
A Bayesian change point model for detecting SIP-based DDoS attacks [20]	2018	Ген./ Обн.	A_F.I	Метод обнаружения на базе байесовской модели множественных изменений	Да	Да	?	Да	В	Нет

Название статьи	К_1	К_2	К_3	К_4	К_5	К_6	К_7	К_8	К_9	К_10
Uncovering SIP Vulnerabilities to DoS Attacks Using Coloured Petri Nets [21]	2011	Ген./ Обн.	A_F.I	Цветные сети Петри	Да	Да	Н	Нет	Н	Нет
SIP Protector: Defense architecture mitigating DDoS flood attacks against SIP servers [22]	2012	Обн.	A_F.I, A_F.R, A_F.O	Механизм перенаправле-ния и сочетания фильтрации исходного и целевого трафика	Да	Нет	?	Нет	?	Нет
An anomaly-based VoIP DoS attack detection and prevention method using fuzzy logic [23]	2016	Ген./ Обн.	A_F.I, A_F.R, A_F.B, A_F.O	Конечная машина состояний	Да	Да	?	Да	В	Нет
Distributed SIP DDoS Defense with P4 [24]	2019	Ген./ Обн.	A_F.I, A_F.R	Плоскость данных и управления	Да	Да	Н	Нет	С	Нет
Counteract DNS Attacks on SIP Proxies Using Bloom Filters [25]	2013	Ген./ Обн.	A_F.I, A_F.B	Фильтрация Блума	Да	Да	Н	Нет	С	Нет
Coping with denial-of-service attacks on the IP telephony system [26]	2016	Ген./ Обн.	A_F.I	Snort и Iptables	Да	Да	Н	Нет	С	Нет
Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks [27]	2011	Обн.	A_F.I	Вейвлет-технологии	Да	Час.	?	Нет	В	Нет
Detection of Resource-Drained Attacks on SIP-Based Wireless VoIP Networks [28]	2010	Ген./ Обн.	A_ PT	Статистический тест Андерсона-Дарлинга	Да	Да	Н	Нет	С	Нет
Sketch-Based SIP Flooding Detection Using Hellinger Distance [29]	2009	Ген./ Обн.	A_F.I	Эскиз и расстояния Хеллингера (онлайн)	Да	Да	Н	Нет	В	Нет
A restrictive model (RM) for detection and prevention of INVITE flooding attack [30]	2013	Ген./ Обн.	A_F.I	Ограничитель-ная модель с применением UDP	Да	Да	?	Нет	С	Да

Результаты анализа

В результате критериального сравнения (табл.) можно сделать следующие выводы.

Во-первых, рассматривался только англоязычный сегмент научных публикаций, в результате чего было найдено 30 наиболее релевантных работ; при этом остальные найденные статьи имели слабую релевантность с заданной при поиске темой. Таким

образом, несмотря на достаточно высокую актуальность DoS/DDoS-атак на VoIP (и с учетом того, что часть работ касалась не их обнаружения, а генерации) [31], количество найденных исследований можно считать незначительным. Это как еще более обосновывает важность текущего исследования, так и говорит об его полноте – поскольку оно, с точки зрения авторов, охватывает практически все возможные работы в данном направлении.

Во-вторых, по критерию К_1 работы из данной тематики начали публиковаться еще с 2006 г. (1 статья), однако наибольшую популярность противодействие DoS/DDoS-атакам приобрело начиная с 2009 г. (6 публикаций) по 2010 г. (5 публикаций); гистограмма такого распределения приведена на рис. 1.

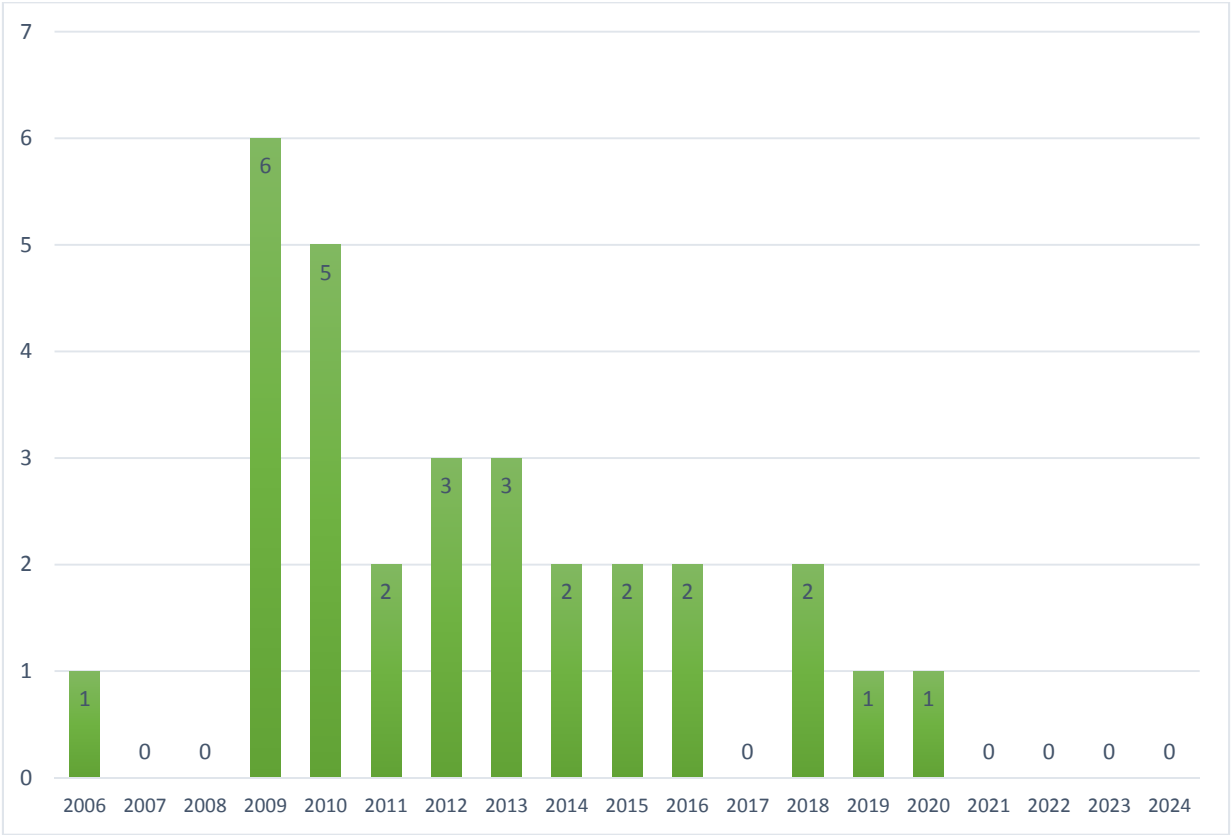

Рис. 1. **Гистограмма распределения количества публикаций по годам**

Таким образом, постепенно тематика становилась менее популярной, хотя количество Dos/DDos-атак не сократилось [32].

В-третьих, по критерию К_2 видно, что подавляющее число работ (20 или $\frac{20}{30} = \sim 67\ \%$) включает описание не только метода борьбы с Dos/DDos-атакой, но и метода ее генерации. В частности, для тестирования разработанного метода обнаружения атак используется открытое ПО и собственные разработанные генераторы.

В-четвертых, критерий К_3 показал, что подавляющее большинство работ рассматривают в своем исследовании атаку типа INVITE флуд (A_F.I -14 или $\frac{14}{30} = \sim 47\ \%$), что объясняется простотой ее реализации [33]; также существует множество открытых источников с генераторами SIP флуда данного типа. Общая схема иерархической типизации атак с указанием публикаций, в которых упоминается каждый из ее типов, приведена на рис. 2.

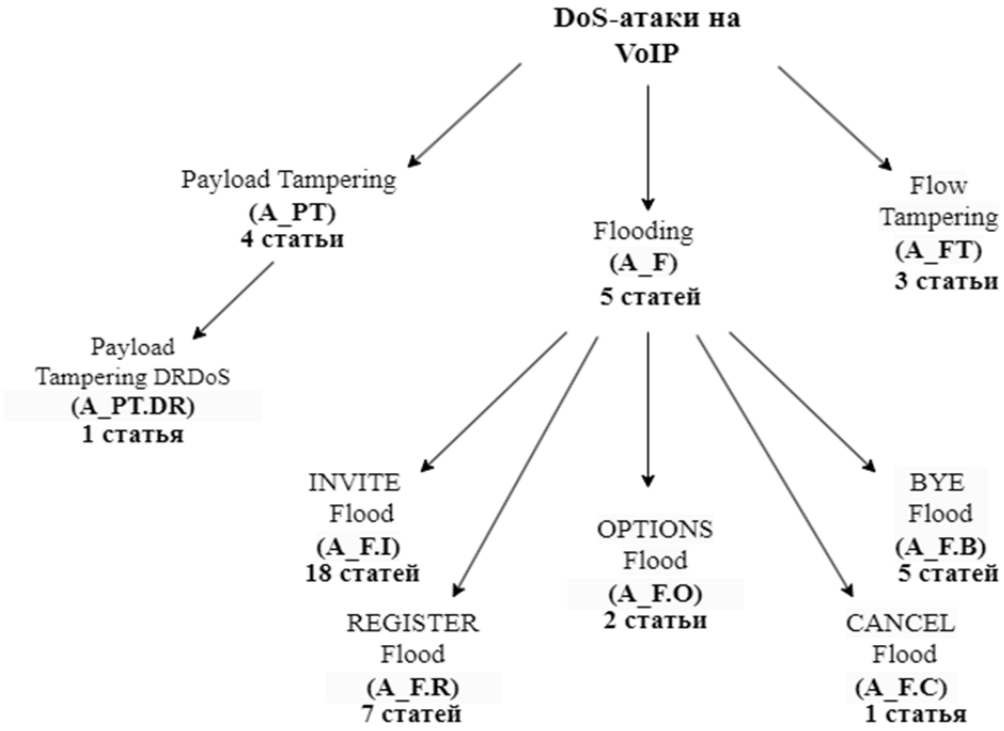

Рис. 2. **Иерархическая типизация атак с указанием количества публикаций для каждой из них**

В-пятых, согласно К_4 нет ни одного повторяющегося метода борьбы с DoS/DDoS-атаками, на основании чего можно сделать вывод о существенном разнообразии методов противодействия и отсутствии применимости единого подхода. Исключением является то, что в ряде работ [1, 13, 25] использовался белый список, как в качестве самого метода, так и в качестве этапа реализации защиты. Также в трех статьях применялся конечный автомат [9, 18, 23].

В-шестых, согласно К_5 каждый теоретически разработанный метод был реализован на практике. Незначительное количество решений (2 или $\frac{2}{30} = \sim 7\ \%$) в работах не были протестированы. Следовательно, принципиальных практических сложностей в их реализации нет.

В-седьмых, критерий К_6 показал, что почти все методы в работах (26 или $\frac{26}{30} = \sim 87\ \%$) прошли тестирование – некоторые в формате разработанного тестового стенда, другие путем математического моделирования; последние по критерию К_2 имеют значение – обнаружение, так как не было реальной генерации DoS/DDoS-атаки.

В-восьмых, согласно К_7 половина рассматриваемых в работах методов (15 или $\frac{15}{30} = \sim 50\ \%$) имеют низкий расход ресурса, а в большей части оставшихся работ (11 статей или $\frac{11}{30} = \sim 37\ \%$) информация о расходе ресурсов отсутствует; и только в четырех работах расход ресурса оценивается как средний (таким образом, работ с высоким расходом ресурса нет). Следовательно, большинство методов не перегружают сеть и выполняют функцию защиты, не препятствуя сторонней работе программно-аппаратного обеспечения.

В-девятых, согласно К_8 на основании уровня законченности результата, тестирования в реальных условиях и расхода ресурсов, только восемь работ ($\frac{8}{30} = \sim 27\ \%$) из всего обзора применимы в реальных VoIP сетях.

В-десятых, согласно К_9 большинство методов имеют среднюю результативность (20 или $\frac{20}{30} = \sim 67\ \%$), часть – высокую результативность (6 или $\frac{6}{30} = \sim 20\ \%$), остальные

же – низкую или не содержат такой информации (2 статьи или $\frac{2}{30} = \sim 7\ \%$). При этом практически во всех статьях приводятся высокие показатели уровня обнаружения DoS/DDoS-атак.

В-одиннадцатых, критерий К_9 показал, что машинное обучение применяется всего лишь в трех статьях [3, 10, 30], (3 статьи или $\frac{3}{30} = \sim 10\ \%$). Объяснением этого может быть то, что машинное обучение стало популярно лишь в последние годы, а работ с 2021 г. не было найдено в принципе.

Выводы

В работе решается задача недостаточной защиты от Dos/DDos-атак в VoIP сетях. Для этого делается обзор работ, посвященных методам генерации и обнаружения DoS-атак на VoIP. Как результат, получена сравнительная таблица, состоящая из 30 публикаций по следующим критериями: год работы, этап жизненного цикла атаки, ее тип, метод защиты, степень реализации, ее ресурсоемкость, практическая применимость, результативность метода. Произведен сравнительный анализ методов обнаружения атак и сделаны следующие основные выводы: несмотря на достаточно высокую значимость угрозы Dos/DDos-атак на VoIP, количество найденных и релевантных статей можно считать незначительным; тематика становится менее популярной в научной среде, несмотря на оставшуюся актуальность угрозы; каждый метод, указанный в рассмотренных работах, является протестированным решением с незначительной ресурсозатратностью и хорошей результативностью в обнаружении атак; все методы могут быть основой для разработки более масштабной системы защиты; наиболее распространённой сгенерированной тестовой атакой для методов является INVITE флуд, что говорит о простоте ее реализации; большинству статей необходимо тестирование в условиях реальной сети; машинное обучение применяется крайне редко.

Основным результатом текущего исследования является систематизация большого количества данных о методах генерации DoS/DDoS атак и защиты, сведенная в единую таблицу согласно выбранным критериям. Частным результатом является пул сделанных по таблице выводов. Новизна работы обосновывается тем, что произведенный обзор и сравнительный анализ публикаций зарубежных исследователей по охвату превосходит существующие; при этом использованный пул критериев сравнения является полностью авторским.

Теоретическая значимость текущей работы заключается в создании единой системы методов, обеспечивающих жизненный цикл DoS/DDoS-атак (от момента создания, до ее обнаружения); практическая же – как в возможности обоснованного выбора необходимого метода защиты от атак, так и будущей потенциальной возможности их объединения для создания нового, более эффективного метода.

Продолжением исследования должно стать усовершенствование одного или совмещение нескольких рассмотренных в работах методов в интересах обеспечения сильной и многосторонней защиты VoIP сетей [34].

Список источников

1. Ehlert S., Geneiatakis D., Magedanz T. Survey of network security systems to counter SIP-based denial-of-service attacks // Computers & Security. 2010. Vol. 29. Iss. 2. P. 225–243. DOI: 10.1016/j.cose.2009.09.004.

2. Liu Z., Yin X., Lee H. An Efficient Defense Scheme against SIP DoS Attack in SDN Using Cloud SFW // Ninth Asia Joint Conference on Information Security. Wuhan, China, 2014. P. 52–55. DOI: 10.1109/AsiaJCIS.2014.12.

3. Ferdous R., Cigno R.L., Zorat A. On the Use of SVMs to Detect Anomalies in a Stream of SIP Messages // 11th International Conference on Machine Learning and Applications. Boca Raton, FL, USA, 2012. P. 592–597. DOI: 10.1109/ICMLA.2012.109.

4. Safoine R., Mounir S., Farchi A. Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks // 6th International Conference on Multimedia Computing and Systems (ICMCS). Rabat, Morocco, 2018. P. 1–5. DOI: 10.1109/ICMCS.2018.8525878.

5. Xiao-Yu Wan, Zhang Li, Zi-Fu Fan. A SIP DoS flooding attack defense mechanism based on priority class queue // IEEE International Conference on Wireless Communications, Networking and Information Security. Beijing, China, 2010. P. 428–431. DOI: 10.1109/WCINS.2010.5541813.

6. Fan Z., Wan X. The design and realization of SIP DOS attack detection plugin based on balanced message number principle // IEEE International Conference on Communications Technology and Applications. Beijing, China, 2009. P. 780–784. DOI: 10.1109/ICCOMTA.2009.5349092.

7. Pourmohseni S., Asgharian H., Akbari A. Detecting authentication misuse attacks against SIP entities // 10th International ISC Conference on Information Security and Cryptology (ISCISC). Yazd, Iran, 2013. P. 1–5. DOI: 10.1109/ISCISC.2013.6767324.

8. Zhou C.V., Leckie C., Ramamohanarao K. Protecting SIP server from CPU-based DoS attacks using history-based IP filtering // IEEE Communications Letters. 2009. Vol. 13. № 10. P. 800–802. DOI: 10.1109/LCOMM.2009.090840.

9. Zhe C., Rong D. The Formal Analyse of DoS Attack to SIP Based on the SIP Extended Finite State Machines // International Conference on Computational Intelligence and Software Engineering. Wuhan, China, 2010. P. 1–4. DOI: 10.1109/CISE.2010.5676902.

10. Akbar A., Basha S.M., Sattar S.A. Leveraging the SIP load balancer to detect and mitigate DDos attacks // International Conference on Green Computing and Internet of Things (ICGCIoT). Greater Noida, India, 2015. P. 1204–1208. DOI: 10.1109/ICGCIoT.2015.7380646.

11. Chen Z., Wen W., Yu D. Detecting SIP flooding attacks on IP Multimedia Subsystem (IMS) // International Conference on Computing, Networking and Communications (ICNC. Maui, HI, USA, 2012. P. 154–158. DOI: 10.1109/ICCNC.2012.6167401.

12. Fan Z.F., Yang J.R., Wan X.Y. A SIP DoS Flooding Attack Defense Mechanism Based on Custom Weighted Fair Queue Scheduling // International Conference on Multimedia Technology. Ningbo, China, 2010. P. 1–4. DOI: 10.1109/ICMULT.2010.5630386.

13. Chen E.Y., Itoh M. A whitelist approach to protect SIP servers from flooding attacks // IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2010). Vancouver, BC, Canada, 2010. P. 1–6. DOI: 10.1109/CQR.2010.5619917.

14. Tas I.M., Unsalver B.G. Baktir S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism // IEEE Access. 2020. Vol. 8. P. 112574–112584. DOI: 10.1109/ACCESS.2020.3001688.

15. Deng X., Shore M. Advanced Flooding Attack on a SIP Server // International Conference on Availability, Reliability and Security. Fukuoka, Japan, 2009. P. 647–651. DOI: 10.1109/ARES.2009.15.

16. Armoogum S., Mohamudally N. Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks // IST-Africa Conference Proceedings, Pointe aux Piments. Mauritius, 2014. P. 1–11. DOI: 10.1109/ISTAFRICA.2014.6880664.

17. Bansal A., Pais A.R. Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System // IEEE International Conference on Computational Intelligence & Communication Technology. Ghaziabad, India, 2015. P. 391–396. DOI: 10.1109/CICT.2015.66.

18. Chen E.Y. Detecting DoS attacks on SIP systems // 1st IEEE Workshop on VoIP Management and Security. Vancouver, BC, Canada, 2006. P. 53–58. DOI: 10.1109/VOIPMS.2006.1638123.

19. Moh'd A., Tawalbeh L., Sowe A. A novel method to guarantee QoS during DoS attacks for IPTV using SIP // Second International Conference on the Applications of Digital Information and Web Technologies. London, UK, 2009. P. 838–842. DOI: 10.1109/ICADIWT.2009.5273867.

20. Kurt B., Yıldız Ç., Ceritli T.Y., Sankur B., Cemgil A.T. A Bayesian change point model for detecting SIP-based DDoS attacks // Digital Signal Processing. 2018. Vol. 77. P. 48–62. DOI: 10.1016/j.dsp.2017.10.009.

21. Liu L. Uncovering SIP Vulnerabilities to DoS Attacks Using Coloured Petri Nets // 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. Changsha, China, 2011. P. 29–36. DOI: 10.1109/TrustCom.2011.8.

22. Stanek J., Kencl L. SIP Protector: Defense architecture mitigating DDoS flood attacks against SIP servers // IEEE International Conference on Communications (ICC). Ottawa, ON, Canada, 2012. P. 6733–6738. DOI: 10.1109/ICC.2012.6364674.

23. Hosseinpour M., Hosseini Seno S.A., Yaghmaee Moghaddam M.H., Khosravi Roshkhari H. An anomaly based VoIP DoS attack detection and prevention method using fuzzy logic // 8th International Symposium on Telecommunications (IST). Tehran, Iran, 2016. P. 713–718. DOI: 10.1109/ISTEL.2016.7881916.

24. Febro A., Xiao H., Spring J. Distributed SIP DDoS Defense with P4 // IEEE Wireless Communications and Networking Conference (WCNC). Marrakesh, Morocco, 2019. P. 1–8. DOI: 10.1109/WCNC.2019.8885926.

25. Zhang G., Fischer-Hübner S. Counteract DNS Attacks on SIP Proxies Using Bloom Filters // International Conference on Availability, Reliability and Security. Regensburg, Germany, 2013. P. 678–684. DOI: 10.1109/ARES.2013.89.

26. Cadet F., Fokum D.T. Coping with denial-of-service attacks on the IP telephony system // SoutheastCon 2016. Norfolk, VA, USA, 2016. P. 1–7. DOI: 10.1109/SECON.2016.7506691.

27. Tang J., Cheng Y. Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks // IEEE International Conference on Communications (ICC). Kyoto, Japan, 2011. P. 1–5. DOI: 10.1109/icc.2011.5963248.

28. Tang J., Hao Y., Cheng Y., Zhou C. Detection of Resource-Drained Attacks on SIP-Based Wireless VoIP Networks // IEEE Global Telecommunications Conference GLOBECOM 2010. Miami, FL, USA, 2010. P. 1–5. DOI: 10.1109/GLOCOM.2010.5684028.

29. Tang J., Cheng Y., Zhou C. Sketch-Based SIP Flooding Detection Using Hellinger Distance // GLOBECOM 2009 – 2009 IEEE Global Telecommunications Conference. Honolulu, HI, USA, 2009. P. 1–6. DOI: 10.1109/GLOCOM.2009.5426267.

30. Raza M.A., Khan A.-u.-R., Raza M. A restrictive model (RM) for detection and prevention of INVITE flooding attack // 3rd IEEE International Conference on Computer, Control and Communication (IC4), Karachi, Pakistan, 2013. P. 1–6. DOI: 10.1109/IC4.2013.6653766.

31. Макарова А.К., Поляничева А.В., Саматова К.А. Анализ уязвимостей оборудования передачи голосового трафика // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Междунар. науч.-техн. и науч.-метод. конф. СПб.: С.-Петерб. гос. ун-т телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. Т. 1. С. 665–669. EDN JRKJAR.

32. Израилов К.Е., Макарова А.К., Шестаков А.В. Обобщенная модель защиты от кибератак на VOIP // Вопросы кибербезопасности. 2023. № 2 (54). С. 109–121. DOI: 10.21681/2311-3456-2023-2-109-121.

33. Израилов К.Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Сер.: Технические науки. 2012. № 8 (59). С. 150–153. EDN PJGOAF.

34. Основные принципы проектирования архитектуры современных систем защиты / М.В. Буйневич [и др.] // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58.

References

1. Ehlert S., Geneiatakis D., Magedanz T. Survey of network security systems to counter SIP-based denial-of-service attacks // Computers & Security. 2010. Vol. 29. Iss. 2. P. 225–243. DOI: 10.1016/j.cose.2009.09.004.

2. Liu Z., Yin X., Lee H. An Efficient Defense Scheme against SIP DoS Attack in SDN Using Cloud SFW // Ninth Asia Joint Conference on Information Security. Wuhan, China, 2014. P. 52–55. DOI: 10.1109/AsiaJCIS.2014.12.

3. Ferdous R., Cigno R.L., Zorat A. On the Use of SVMs to Detect Anomalies in a Stream of SIP Messages // 11th International Conference on Machine Learning and Applications. Boca Raton, FL, USA, 2012. P. 592–597. DOI: 10.1109/ICMLA.2012.109.

4. Safoine R., Mounir S., Farchi A. Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks // 6th International Conference on Multimedia Computing and Systems (ICMCS). Rabat, Morocco, 2018. P. 1–5. DOI: 10.1109/ICMCS.2018.8525878.

5. Xiao-Yu Wan, Zhang Li, Zi-Fu Fan. A SIP DoS flooding attack defense mechanism based on priority class queue // IEEE International Conference on Wireless Communications, Networking and Information Security. Beijing, China, 2010. P. 428–431. DOI: 10.1109/WCINS.2010.5541813.

6. Fan Z., Wan X. The design and realization of SIP DOS attack detection plugin based on balanced message number principle // IEEE International Conference on Communications Technology and Applications. Beijing, China, 2009. P. 780–784. DOI: 10.1109/ICCOMTA.2009.5349092.

7. Pourmohseni S., Asgharian H., Akbari A. Detecting authentication misuse attacks against SIP entities // 10th International ISC Conference on Information Security and Cryptology (ISCISC). Yazd, Iran, 2013. P. 1–5. DOI: 10.1109/ISCISC.2013.6767324.

8. Zhou C.V., Leckie C., Ramamohanarao K. Protecting SIP server from CPU-based DoS attacks using history-based IP filtering // IEEE Communications Letters. 2009. Vol. 13. № 10. P. 800–802. DOI: 10.1109/LCOMM.2009.090840.

9. Zhe C., Rong D. The Formal Analyse of DoS Attack to SIP Based on the SIP Extended Finite State Machines // International Conference on Computational Intelligence and Software Engineering. Wuhan, China, 2010. P. 1–4. DOI: 10.1109/CISE.2010.5676902.

10. Akbar A., Basha S.M., Sattar S.A. Leveraging the SIP load balancer to detect and mitigate DDos attacks // International Conference on Green Computing and Internet of Things (ICGCIoT). Greater Noida, India, 2015. P. 1204–1208. DOI: 10.1109/ICGCIoT.2015.7380646.

11. Chen Z., Wen W., Yu D. Detecting SIP flooding attacks on IP Multimedia Subsystem (IMS) // International Conference on Computing, Networking and Communications (ICNC. Maui, HI, USA, 2012. P. 154–158. DOI: 10.1109/ICCNC.2012.6167401.

12. Fan Z.F., Yang J.R., Wan X.Y. A SIP DoS Flooding Attack Defense Mechanism Based on Custom Weighted Fair Queue Scheduling // International Conference on Multimedia Technology. Ningbo, China, 2010. P. 1–4. DOI: 10.1109/ICMULT.2010.5630386.

13. Chen E.Y., Itoh M. A whitelist approach to protect SIP servers from flooding attacks // IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2010). Vancouver, BC, Canada, 2010. P. 1–6. DOI: 10.1109/CQR.2010.5619917.

14. Tas I.M., Unsalver B.G. Baktir S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism // IEEE Access. 2020. Vol. 8. P. 112574–112584. DOI: 10.1109/ACCESS.2020.3001688.

15. Deng X., Shore M. Advanced Flooding Attack on a SIP Server // International Conference on Availability, Reliability and Security. Fukuoka, Japan, 2009. P. 647–651. DOI: 10.1109/ARES.2009.15.

16. Armoogum S., Mohamudally N. Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks // IST-Africa Conference Proceedings, Pointe aux Piments. Mauritius, 2014. P. 1–11. DOI: 10.1109/ISTAFRICA.2014.6880664.

17. Bansal A., Pais A.R. Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System // IEEE International Conference on Computational Intelligence & Communication Technology. Ghaziabad, India, 2015. P. 391–396. DOI: 10.1109/CICT.2015.66.

18. Chen E.Y. Detecting DoS attacks on SIP systems // 1st IEEE Workshop on VoIP Management and Security. Vancouver, BC, Canada, 2006. P. 53–58. DOI: 10.1109/VOIPMS.2006.1638123.

19. Moh'd A., Tawalbeh L., Sowe A. A novel method to guarantee QoS during DoS attacks for IPTV using SIP // Second International Conference on the Applications of Digital Information and Web Technologies. London, UK, 2009. P. 838–842. DOI: 10.1109/ICADIWT.2009.5273867.

20. Kurt B., Yıldız Ç., Ceritli T.Y., Sankur B., Cemgil A.T. A Bayesian change point model for detecting SIP-based DDoS attacks // Digital Signal Processing. 2018. Vol. 77. P. 48–62. DOI: 10.1016/j.dsp.2017.10.009.

21. Liu L. Uncovering SIP Vulnerabilities to DoS Attacks Using Coloured Petri Nets // 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. Changsha, China, 2011. P. 29–36. DOI: 10.1109/TrustCom.2011.8.

22. Stanek J., Kencl L. SIP Protector: Defense architecture mitigating DDoS flood attacks against SIP servers // IEEE International Conference on Communications (ICC). Ottawa, ON, Canada, 2012. P. 6733–6738. DOI: 10.1109/ICC.2012.6364674.

23. Hosseinpour M., Hosseini Seno S.A., Yaghmaee Moghaddam M.H., Khosravi Roshkhari H. An anomaly based VoIP DoS attack detection and prevention method using fuzzy logic // 8th International Symposium on Telecommunications (IST). Tehran, Iran, 2016. P. 713–718. DOI: 10.1109/ISTEL.2016.7881916.

24. Febro A., Xiao H., Spring J. Distributed SIP DDoS Defense with P4 // IEEE Wireless Communications and Networking Conference (WCNC). Marrakesh, Morocco, 2019. P. 1–8. DOI: 10.1109/WCNC.2019.8885926.

25. Zhang G., Fischer-Hübner S. Counteract DNS Attacks on SIP Proxies Using Bloom Filters // International Conference on Availability, Reliability and Security. Regensburg, Germany, 2013. P. 678–684. DOI: 10.1109/ARES.2013.89.

26. Cadet F., Fokum D.T. Coping with denial-of-service attacks on the IP telephony system // SoutheastCon 2016. Norfolk, VA, USA, 2016. P. 1–7. DOI: 10.1109/SECON.2016.7506691.

27. Tang J., Cheng Y. Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks // IEEE International Conference on Communications (ICC). Kyoto, Japan, 2011. P. 1–5. DOI: 10.1109/icc.2011.5963248.

28. Tang J., Hao Y., Cheng Y., Zhou C. Detection of Resource-Drained Attacks on SIP-Based Wireless VoIP Networks // IEEE Global Telecommunications Conference GLOBECOM 2010. Miami, FL, USA, 2010. P. 1–5. DOI: 10.1109/GLOCOM.2010.5684028.

29. Tang J., Cheng Y., Zhou C. Sketch-Based SIP Flooding Detection Using Hellinger Distance // GLOBECOM 2009 – 2009 IEEE Global Telecommunications Conference. Honolulu, HI, USA, 2009. P. 1–6. DOI: 10.1109/GLOCOM.2009.5426267.

30. Raza M.A., Khan A.-u.-R., Raza M. A restrictive model (RM) for detection and prevention of INVITE flooding attack // 3rd IEEE International Conference on Computer, Control and Communication (IC4), Karachi, Pakistan, 2013. P. 1–6. DOI: 10.1109/IC4.2013.6653766.

31. Makarova A.K., Polyanicheva A.V., Samatova K.A. Analiz uyazvimostej oborudovaniya peredachi golosovogo trafika // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2022): XI Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. SPb.: S.-Peterb. gos. un-t telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2022. T. 1. S. 665–669. EDN JRKJAR.

32. Izrailov K.E., Makarova A.K., SHestakov A.V. Obobshchennaya model' zashchity ot kiberatak na VOIP // Voprosy kiberbezopasnosti. 2023. № 2 (54). S. 109–121. DOI: 10.21681/2311-3456-2023-2-109-121.

33. Izrailov K.E. Model' prognozirovaniya ugroz telekommunikacionnoj sistemy na baze iskusstvennoj nejronnoj seti // Vestnik INZHEKONa. Ser.: Tekhnicheskie nauki. 2012. № 8 (59). S. 150–153. EDN PJGOAF.

34. Osnovnye principy proektirovaniya arhitektury sovremennyh sistem zashchity / M.V. Bujnevich [i dr.] // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2020. № 3 (31). S. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58.

Информация о статье:
Статья поступила в редакцию: 23.05.2024; одобрена после рецензирования: 10.06.2024; принята к публикации: 13.06.2024
Information about the article:
The article was submitted to the editorial office: 23.05.2024; approved after review: 10.06.2024; accepted for publication: 13.06.2024

Сведения об авторах:
Макарова Александра Константиновна, магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (193232, Санкт-Петербург, пр. Большевиков, д. 22/1), e-mail: alex-ecureuil@mail.ru, https://orcid.org/0000-0001-7745-3364, SPIN-код: 5179-9199
Поляничева Анна Валерьевна, старший преподаватель кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (193232, Санкт-Петербург, пр. Большевиков, д. 22/1), e-mail: polyanicheva.av@sut.ru, https://orcid.org/0000-0003-1283-9180, SPIN-код: 5939-4865
Матвеев Александр Владимирович, заведующий кафедрой прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: fcvega_10@mail.ru, https://orcid.org/0000-0002-0778-3218, SPIN-код: 5778-8832

Information about the authors:
Makarova Alexandra K., graduate student of the Saint-Petersburg state university of telecommunications named after professor M.A. Bonch-Bruevich (193232, Saint-Petersburg, Bolshevikov ave., 22/1), e-mail: alex-ecureuil@mail.ru, https://orcid.org/0000-0001-7745-3364, SPIN: 5179-9199
Polyanicheva Anna V., senior lecturer at the department of secure communication networks of the Saint-Petersburg state university of telecommunications named after professor M.A. Bonch-Bruevich (193232, Saint-Petersburg, Bolshevikov ave., 22/1), e-mail: polyanicheva.av@sut.ru, https://orcid.org/0000-0003-1283-9180, SPIN: 5939-4865
Matveev Alexander V., head of the department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: fcvega_10@mail.ru, https://orcid.org/0000-0002-0778-3218, SPIN: 5778-8832