Сведения об авторах

Александр Дмитриевич Золотов – кандидат технических наук кафедры «Автоматизация, информационные технологии и градостроительство»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: azol64@mail.ru

Әкежан Ержанұлы Уалиев – магистрант кафедры «Автоматизация, информационные технологии и градостроительство»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: boss.hgff@mail.ru

Ербол Амангазович Оспанов – ассоциированный профессор кафедры «Автоматизация, информационные технологии и градостроительство», доктор философии PhD, НАО «Университет имени Шакарима города Семей», г. Семей, Казахстан; e-mail: 78oea@mail.ru

Артур Рихарт– студент группы АУ 101 кафедры «Автоматизация, информационные технологии и градостроительство»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: rihartartur24@gmail.com

Авторлар туралы мәліметтер

Александр Дмитриевич Золотов – «Автоматтандыру, ақпараттық технологиялар және қала құрылысы» кафедрасының техника ғылымдарының кандидаты; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: azol64@mail.ru.

Әкежан Ержанұлы Уалиев – «Автоматтандыру, ақпараттық технологиялар және қала құрылысы» кафедрасының магистранты; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: boss.hgff@mail.ru.

Ербол Амангазович Оспанов – «Автоматтандыру, ақпараттық технологиялар және қалақұрылысы» каферасының қауымдастырылған профессоры, PhD философия докторы, «Семей қаласының Шәкәрім атындағы университеті» КеАҚ, Семей қ., Қазақстан; e-mail: 78oea@mail.ru.

Артур Рихарт – «Автоматтандыру, ақпараттық технологиялар және қала құрылысы» кафедрасының АУ 101 тобының студенті; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; E-mail: rihartartur24@gmail.com.

Information about the authors

Alexander Zolotov – Candidate of Technical Sciences Department of Automation, Information Technology and Urban Planning, Shakarim University of Semey, Republic of Kazakhstan; e-mail: azol64@mail.ru.

Akezhan Ualiyev – master's student of the Department of Automation, Information Technology and Urban Planning, Shakarim University of Semey, Republic of Kazakhstan; e-mail: boss.hgff@mail.ru.

Yerbol Ospanov – Associate Professor of the Department of Automation, Information Technology and Urban Planning, Doctor of Philosophy PhD, Non-profit limited company «Semey University named after Shakarim, Semey, Kazakhstan; e-mail: 78oea@mail.ru.

Arthur Richard – student of AU 101 group of the Department of Automation, Information Technology and Urban Planning; Shakarim University of Semey, Republic of Kazakhstan; e-mail: rihartartur24@gmail.com.

Поступила в редакцию 29.04.2024
Принята к публикации 10.05.2024

DOI: 10.53360/2788-7995-2024-2(14)-3

МРНТИ: 50.05.17

Б.М. Ильясов*, Ж.М. Алимжанова
Казахский национальный университет имени аль-Фараби,
050040, Республика Казахстан, г. Алматы, пр. аль-Фараби, 71
e-mail*: bahalar49@gmail.com

ИССЛЕДОВАНИЕ МОДЕЛИ ЗАЩИТЫ ОТ DDOS АТАК

Аннотация. *Это исследование исследует распределенную модель защиты от отказа в обслуживании (DDoS), фокусируясь на атаках flooding, когда злоумышленники перегружают сервер чрезмерными запросами, чтобы ухудшить его вычислительные возможности. В отличие от традиционных подходов, которые просто направлены на смягчение последствий DDoS-атак, в нашем исследовании особое внимание уделяется разработке надежных моделей защиты от таких*

угроз. Мы представляем новую стратегию защиты, которая включает в себя алгоритмы ограничения скорости для контроля притока запросов, гарантируя, что только законный трафик достигнет сервера. Кроме того, мы исследуем фильтрацию пакетов на основе допустимых значений Time-To-Live (TTL) в сочетании с инновационными методами планирования пакетов, включая методологию First-Come, First-Served (FCFS) и Priority Queue, для повышения оперативности и эффективности работы сервера. Благодаря моделированию, наши результаты показывают значительное улучшение производительности сервера в условиях DDoS-атаки, о чем свидетельствует снижение скорости отбрасывания пакетов и улучшение времени отклика. Успешная реализация этих моделей защиты демонстрирует их потенциал в защите сетей от разрушительного воздействия DDoS-атак, предлагая перспективное направление для будущих исследований в области кибербезопасности.

Ключевые слова: *DDoS-защита; флуд-атаки; ограничение скорости; TTL; планирование пакетов; кибербезопасность.*

Введение

DDoS-атаки более сложны, и их труднее предотвратить по сравнению с традиционными DoS-атаками. Поскольку в них задействовано множество невольных хостов, распознать атакующие хосты и отреагировать на них непросто. Рост числа компьютерных уязвимостей привел к увеличению числа, сложности и серьезности DDoS-атак, что позволяет злоумышленникам проникать на многие компьютеры и устанавливать средства атаки.

Беспроводные сети также подвержены DoS-атакам, поскольку мобильные устройства используют один и тот же физический носитель для передачи сигнала. Злоумышленник может подделать, модифицировать или внедрить пакеты, чтобы нарушить соединения между законными мобильными узлами, вызывая эффект DoS (табл. 1).

Таблица 1 – Классификация DoS и DDoS атак

Тип атаки	Описание	Влияние на систему	Пример атаки
Информационный флуд	Злоумышленник отправляет огромное количество пакетов, перегружая ресурсы системы	Снижение производительности, недоступность дополнительных запросов	ICMP-флуд
Уровень сетевого устройства	Выявление и использование ошибок, существующих в сетевых устройствах	Снижение производительности сети, возможные сбои	SYN-флуд
Уровень операционной системы	Эксплуатация способов реализации протоколов операционной системы	Снижение производительности ОС, возможные сбои	TCP SYN Flooding
Атаки на основе приложений	Поддельные и вредоносные пакеты, замедляющие работу сервера, используя уязвимости приложений	Снижение производительности приложений, недоступность сервисов	HTTP-флуд
Атаки, основанные на особенностях протокола	Использование поддельных IP-адресов для сложного отслеживания источника атаки	Перегрузка сети, снижение производительности	Smurf-атака
Объемные атаки	Перегрузка пропускной способности сети огромным количеством трафика	Снижение пропускной способности, недоступность сети	DNS-атака
Переполнение буфера	Отправка большего объема данных, чем система может обработать, что приводит к сбоям	Критические отказы системы, сбои	Атака переполнения буфера

Поскольку в атаках участвует множество незаметных хостов, различить атакующие хосты и принять ответные меры затруднительно. Рост уязвимостей в компьютерных системах приводит к увеличению количества, сложности и тяжести DDoS-атак, позволяя

злоумышленникам взламывать множество компьютеров и устанавливать инструменты для атак (табл. 2, 3).

Таблица 2 – Статистика DoS и DDoS атак

Год	Количество атак	Средний объем трафика (Гбит/с)	Количество пострадавших компаний	Финансовые убытки (млн. $)
2016	6200	600	60	650
2017	7800	900	85	750
2018	9200	1300	100	850
2019	11500	1500	120	980
2020	13000	1700	140	1100
2021	15000	2000	160	1250
2022	17500	2200	180	1400
2023	20000	2500	200	1600

Таблица 3 – Примеры известных DDoS атак

Год	Атака	Объем трафика (Гбит/с)	Пострадавшие организации	Влияние
2016	Mirai-бонет	600	Dyn, OVH	Недоступность DNS-сервисов, перебои в работе
2018	GitHub DDoS атака	1300	GitHub	Перебои в работе сервисов, временная недоступность
2020	AWS DDoS атака	2300	Amazon Web Services (AWS)	Перебои в работе облачных сервисов
2022	Google Cloud DDoS атака	2600	Google Cloud	Перебои в работе сервисов, снижение производительности

Данные демонстрируют серьезность угрозы, которую представляют DoS и DDoS атаки, и подчеркивают необходимость постоянного мониторинга и улучшения мер безопасности для защиты критически важных ресурсов и услуг.

Методы и исследования

Для эффективной защиты от DoS-атак необходимо использовать различные методы, такие как:

– Мониторинг сети: внедрение инструментов мониторинга сети для обнаружения необычных паттернов трафика.

– Усиление безопасности протоколов: внедрение механизмов безопасности в сетевые протоколы для предотвращения их эксплуатации.

– Фильтрация трафика: настройка фильтров для блокировки подозрительного трафика и ограничения доступа к ресурсам для потенциальных атакующих.

SDN (Software-Defined Networking) имеет потенциал трансформировать сетевую архитектуру, обеспечивая большую гибкость и эффективное управление. Программируемый центральный контроллер предоставляет сетевым администраторам больше возможностей для управления, что позволяет осуществлять более плавный контроль. Однако централизация делает SDN уязвимой к различным атакам, среди которых особую угрозу представляют распределенные атаки типа "отказ в обслуживании" (DDoS).

Методы машинного обучения (ML), основанные на выборе функций, более эффективны, чем традиционные сигнатурные системы обнаружения вторжений (IDS), для выявления новых угроз в контексте защиты от DDoS-атак. В этом исследовании сравниваются NGBoost и четыре дополнительных алгоритма машинного обучения: сверточная нейронная сеть (CNN), стохастический градиентный спуск (SGD), дерево решений и случайный лес, чтобы оценить эффективность обнаружения DDoS на наборе данных CICDDoS2019. Основное внимание уделяется важным показателям, таким как F1-оценка, полнота, точность и аккуратность.

После разработки метода обнаружения атак и смягчения их последствий результаты тестируются и оцениваются. Оценка платформы включает в себя оценку различных алгоритмов ML и сравнение различных используемых моделей. В приведенной ниже таблице показана точность различных используемых моделей:

Из приведенной выше таблицы видно, что random forest обеспечивает наилучшую точность для классификации обычного и вредоносного трафика.

Чтобы оценить производительность модели, был проведен тест с помощью процесса классификации онлайн-трафика и предотвращения атак. Для предотвращения атак были установлены правила брандмауэра, блокирующие обнаруженные атаки. Таким образом, для каждого потока, обнаруженного как вредоносный, устанавливается правило брандмауэра, блокирующее Ethernet-адрес, с которого запускается атака. Реализуется код на Python для сгенерированного прототипа, а затем обычный трафик генерируется в качестве фонового трафика и обнаруживается DDoS-атака.

Результаты исследований

В этой работе алгоритм машинного обучения random forest используется для разработки модели, которая может автоматически идентифицировать и предотвращать DDoS-атаки в сетях SDN. Все записи о потоках трафика регулярно собираются моделью, которая затем извлекает собственные функции потока и расширяет их, включая дополнительные функции. Модуль обнаружения использует пять критериев, чтобы классифицировать каждый поток как нормальный или аномальный.

Наш метод извлечения характеристик трафика учитывает уровень данных в целом. Мы используем простую сетевую архитектуру всего с двумя коммутаторами для моделирования входных и выходных шлюзов. В этой смоделированной тестовой сети один хост управляет задачей отправки пакетов со всех входящих адресов, устраняя необходимость в отдельном хосте для каждого адреса. Таким образом, в нашей сети используются только два виртуальных хоста: один для входящего трафика, а другой для исходящего. На рисунке 4 показана архитектура нашей тестовой сети.

Мы внедрили бинарные классификаторы, используя три метода, и протестировали их с помощью набора данных KDD-CUP99. Классификаторы были обучены на 40% набора данных, в то время как остальные данные были использованы для создания имитационных пакетов для тестирования.

Набор данных KDD-CUP99 не содержит адресной информации, что делает невозможным непосредственное создание пакетов с адресами. Однако он содержит флаги, указывающие на связь между пакетами и окнами. Мы предварительно обработали набор данных, разделив пакеты внутри одних и тех же окон и назначив поддельные адреса для каждого окна, что хорошо сработало в наших тестах.

Наш двоичный классификатор выдает логические выходные данные. Показатели оценки определяются следующим образом:

– Истинно положительные (TP). Правильно предсказанные положительные случаи.

– Истинно отрицательные (TN). Правильно предсказанные отрицательные случаи.

– Ложноположительные результаты (FP). Неверно предсказанные положительные случаи.

– Ложноотрицательные результаты (FN): Неверно предсказанные отрицательные случаи.

На основе этих определений получены следующие формулы для показателей оценки:

Точность: доля правильно классифицированных случаев (рис. 1).

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

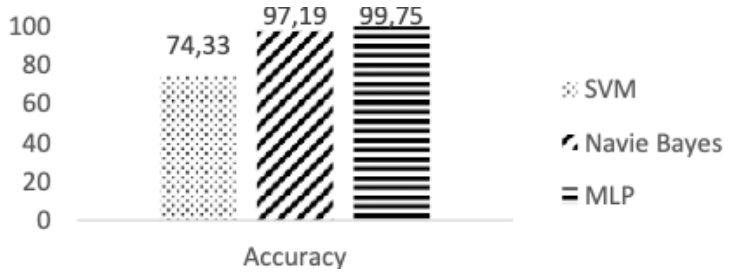

Рисунок 1 – Аккуратность

Точность: доля правильно классифицированных положительных сообщений от общего числа, классифицированных как положительные. Более высокое значение указывает на меньшее количество обычных пакетов, ошибочно классифицированных как атаки (рис. 2).

$$\text{Precision} = \frac{TP}{TP + FP}$$

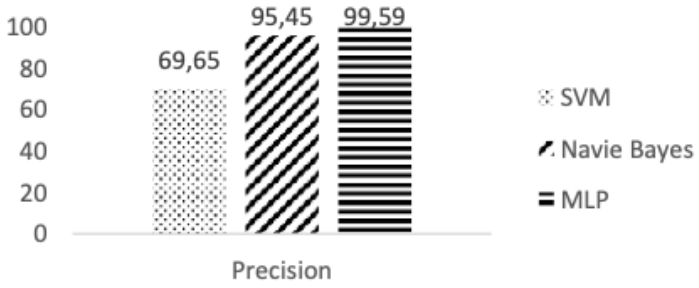

Рисунок 2 – Точность

Напомним: доля правильно классифицированных случаев срабатывания от общего числа реальных случаев срабатывания. Этот показатель имеет решающее значение, поскольку любой необнаруженный атакующий трафик может быть фатальным для сети (рис. 3).

$$\text{Recall} = \frac{TP}{TP + FN}$$

Рисунок 3 – Формула Recall

Оценка F1: гармоничное среднее значение точности и запоминания, обеспечивающее сбалансированную оценку (рис. 4).

$$\text{F1 Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

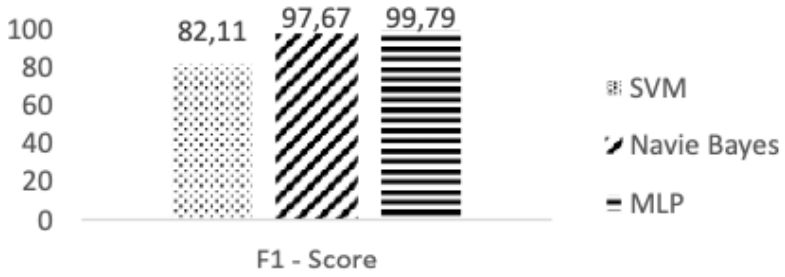

Рисунок 4 – F1 – оценка

Мы протестировали модели с использованием набора данных KDD-CUP 99, и результаты приведены в таблице 4.

Таблица 4 – Матрица путаницы

Алгоритм	Аккуратность	Точность	Отзыв	F1 Score
Дерево решений	0,97520	0,97531	0,96217	0,96864
Случайный лес	0,97791	0,97791	0,95877	0,96824
Глубокая нейронная сеть (DNN)	0,99721	0,99715	0,99662	0,99689

Наши результаты тестирования на наборе данных KDD-CUP 99 являются удовлетворительными: все три алгоритма машинного обучения достигли показателей оценки выше 0,95. Такое указывает на высокий уровень достоверности при обнаружении DDoS-атак.

В частности, алгоритмы Дерева решений и случайного леса показали схожую производительность, в то время как DNN превзошел их с показателями выше 0,99.

Обычный поток трафика генерировался с использованием протоколов ICMP, TCP и UDP. Инструмент Iperf использовался для создания и измерения пропускной способности потоков данных TCP и UDP. UDP-трафик генерировался в течение 300 секунд с помощью команды iperf -u -c server1 -t 300. Аналогичным образом TCP-трафик генерировался в течение 300 секунд с помощью команды iperf -c server1 -t 300 -p 80.

Поток трафика для атаки был смоделирован с использованием TCP SYN flood. Эта атака использует трехстороннее подтверждение связи по протоколу TCP, отправляя запросы на подключение быстрее, чем сервер может их обработать, что приводит к перенасыщению сети. Атака была выполнена с помощью команды python3 -E synattack.py server1 - server2, и статистика потоков собиралась каждые 30 секунд. Контроллер SDN отправлял сообщения с запросом OpenFlow stats на все коммутаторы для сбора обновленной статистики по потокам и портам.

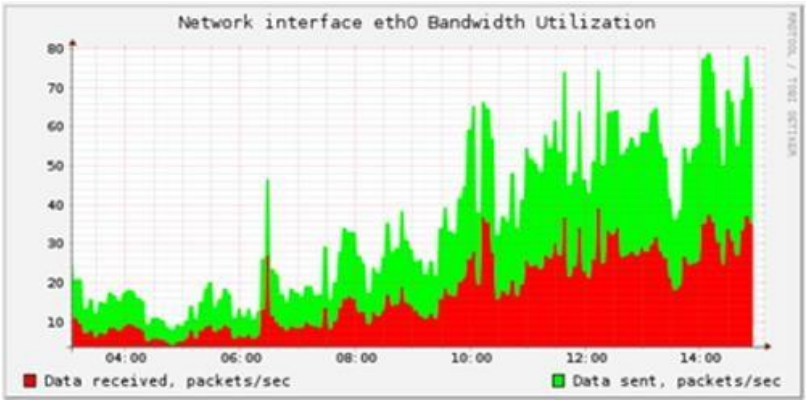

Рисунок 5 – Нагрузка на сетевой интерфейс

На графике показано использование полосы пропускания сетевого интерфейса eth0 на целевом сервере после начала атаки. По оси x отложено время суток, а по оси y – скорость передачи данных в пакетах в секунду. Зеленая область указывает на скорость приема данных, а красная – на скорость отправки данных (рис. 5).

Обсуждение научных результатов

Таблица 5 – Результаты эксперимента по сравнению эффективности

Система	Ложные срабатывания, %	Не обнаруженные вредоносные запросы, %
Kaspersky Anti-Haker	0,1	10,3
Snort	4,4	10,1
Symantec	3,4	11,9
DDOS deflate	5,7	20
Разработанное средство	0,9	2,8

У Kaspersky Anti-Hacker самый низкий показатель – 0,1%, что указывает на то, что он редко ошибочно распознает законный трафик как вредоносный (таб. 5).

Разработанный инструмент также хорошо работает с низким показателем ложных срабатываний (0,9%).

Разработанный инструмент отличается самым низким показателем необнаруженных вредоносных запросов – 2,8%.

В отличие от этого, у DDOS-атаки deflate самый высокий показатель – 20%, что указывает на то, что он пропускает значительную часть вредоносного трафика.

В этом исследовании мы стремимся разработать и оценить методы обнаружения DDoS-атак с использованием методов машинного обучения. Традиционные подходы к обнаружению

DDoS-атак часто основаны на анализе пакетов на сетевом уровне, который можно обойти с помощью хорошо продуманных атак, имитирующих законный трафик. Переключив внимание на журналы базы данных, мы потенциально можем выявить закономерности, указывающие на DDoS-атаки, которые могут быть незаметны только при анализе сетевого трафика (рис. 6).

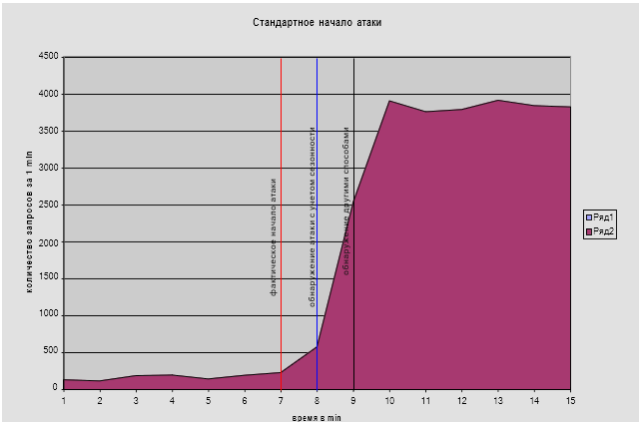

Рисунок 6 – Стандартное начало атаки

Алгоритмы обучения с подкреплением могут извлекать уроки из окружающей среды, получая обратную связь в виде вознаграждений или наказаний. В контексте обнаружения DDoS-атак алгоритм обучения с подкреплением может получать вознаграждение за правильное обнаружение атаки и наказание за ложноположительное предупреждение.

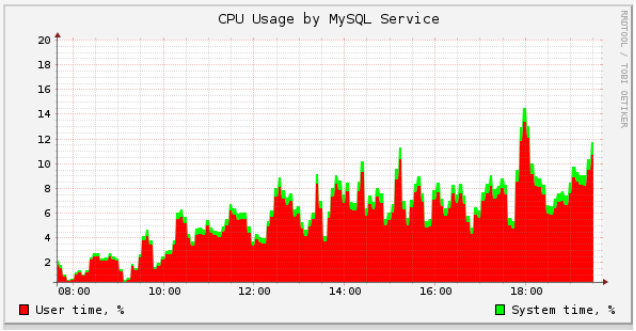

Рисунок 7 – Нагрузка со стороны сервера баз данных после начала атаки

На графике показана загрузка процессора службой MySQL на сервере баз данных после начала атаки (рис. 7). Ось x показывает время суток, а ось y – процент загрузки процессора. Снижение затрат на обеспечение безопасности: Внедрение этого инструмента привело к снижению экономических затрат, связанных с поддержанием информационной безопасности, на 20%. Это демонстрирует экономическую эффективность и финансовые выгоды для организаций, использующих этот инструмент.

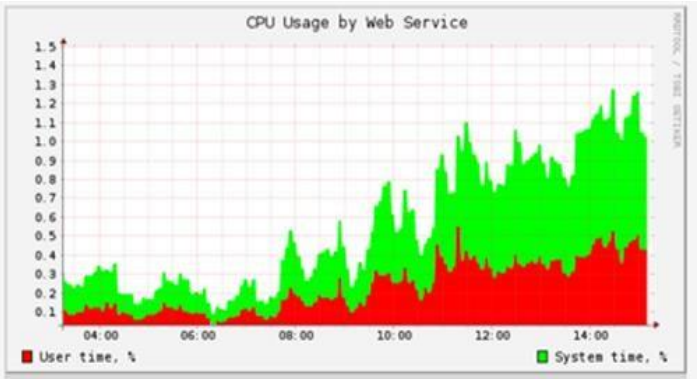

Рисунок 8 – Использование ресурсов процессора атакуемого сервера после начала атаки

Результаты оценки эффективности обнаружения начала атаки и выявление вредоносного трафика в целом соответствуют результатам, полученным при проведении тестов в нагрузочной сети (рис. 8). Отклонение для ошибки первого рода составило не более 3%, отклонение для ошибки второго рода не более 6%. Данные результаты подтверждаются актами внедрения разработанных программных средств на площадках заказчиков.

Заключение

В данной работе предложена методика раннего обнаружения начала DDoS-атаки и последующего определения вредоносных запросов. В основе разработанных методик лежат методы теории вероятности, кластерного и статистического анализа, принципы машинного обучения.

В качестве основных результатов диссертационной работы можно выделить следующие:

1. Проведен мониторинг современных распределенных атак, направленных на отказ в обслуживании. Выделена новая группа атак средней и малой интенсивности, направленных в основном на региональные ресурсы. Проведен мониторинг различных программных и аппаратных средств противодействия и средств обнаружения атак такого типа. Выявлено отсутствие средств, позволяющих адекватно решать поставленные задачи по обнаружению и противодействию, для данной группы атак.
2. Предложена и обоснована гипотеза о существовании сезонности в работе различных сетевых ресурсов. Выяснены причины, влияющие на формирования и особенности сезонных периодов.
3. Предложено формальное описание сезонности сетевой нагрузки, которое позволяет выявлять сезоны различной периодичности, отличающиеся учетом неопределенного начала и завершения периода.
4. Исследование модели атаки позволило создать методику раннего обнаружения и противодействия DDoS-атакам средней и малой интенсивности. Методика является универсальной, учитывает, как региональные особенности, так и другие факторы, и может быть применена для обнаружения и противодействия DDoS-атакам различных типов и различной мощности. А также для обнаружения аномальных данных в различных сферах деятельности.
5. В процессе разработки методики создано два алгоритма: алгоритм определения точки начала атаки и алгоритм разделения смешанного трафика на благонадежный и вредоносный. Отличительной чертой алгоритмов является учет сезонных колебаний сетевой нагрузки.

Список литературы

1. Басканов А.Н. Способы противодействия и средства раннего выявления DDoS-атак / А.Н. Басканов // Экономика и качество систем связи. – 2019. – Режим доступа: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego- vyyavleniya-ddos-atak (дата обращения: 2021-06-24).
2. Gu Q. Denial of Service Attacks / Q. Gu, P. Liu // Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications. – 2012. – Vol. 3.
3. Tripathi N. DoS and DDoS Attacks: Impact, Analysis and Countermeasures. / N. Tripathi, B.M. Mehtre // Conference: Advances in Computing, Networking and Security: TEQIP II National Conference. – 2014. – Access Mode: https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Imp act_Analysis_and_Countermeasures (online; accessed: 2023-06-15).
4. Афанасьева Д.В. Проблема DDoS-атак / Д.В. Афанасьева // Наука, образование и культура. – 2019. – Режим доступа: https://cyberleninka.ru/article/n/problema-ddos-atak (дата обращения: 2021-06-23).
5. Securelist – DDoS-атаки в I квартале 2021 года. – 2021. – Режим доступа: https://securelist.ru/ddos-attacks-in-q1-2021/101390/ (дата обращения: 2021-06-24).

6. Zeb K. DDoS Attacks and Countermeasures in Cyberspace / K. Zeb, O. Baig, M.K. Asif // IEEE 2nd World Symposium on Web Applications and Networking (WSWAN). – 2015. – Mar. – P. 1-6.
7. Слеповичев И.И. Обнаружение DDoS атак нечеткой нейронной сетью. // Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика. – 2009. – Режим доступа: https://cyberleninka.ru/article/n/obnaruzhenie-ddos-atak-nechetkoy-neyronnoy-setyu (дата обращения: 2023-06-21).
8. Doriguzzi-Corin R. Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detectionn / R. Doriguzzi-Corin // IEEE Transactions on Network and Service Management. – 2020. – Feb. – P. 1-14.
9. Использование SVM для обнаружения DDoS-атак в сети SDN / Донг Ли и др. // IOP Conf. Ser.: Матер. наук. Eng. 466 012003, 2018.
10. Метод обнаружения DDoS-атак, основанный на извлечении признаков из сетей глубоких убеждений / Ицзе Ли и др. // серия конференций IOP: Наука о окружающей среде, том 252, выпуск 3. – 2019.
11. Обнаружение DDoS-атак на центры обработки данных с помощью корреляционного анализа / Пэн Сяо и др. // Компьютерные коммуникации. – 2015. – № 67.
12. Разработка и внедрение системы обнаружения DDoS-атак Интернета вещей, основанной на машинном обучении / Ю.В. Чен и др. // В материалах Европейской конференции IEEE по сетям и коммуникациям, Дубровник, Хорватия, 15-18 июня 2020. – С. 122-127.
13. Обнаружение атак типа «отказ в обслуживании» и смягчение их последствий для Интернета вещей с использованием методов машинного обучения с поддержкой ретроспективного анализа / А. Михуб и др. // Вычисл. Электр. Англ. – 2022. № 98. P. 107716.

References

1. Baskanov A.N. Sposoby protivodeistviya i sredstva rannego vyyavleniya DDoS-atak / A.N. Baskanov // Ehkonomika i kachestvo sistem svyazi. – 2019. – Rezhim dostupa: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego- vyyavleniya-ddos-atak (data obrashcheniya: 2021-06-24). (In Russian).
2. Gu Q. Denial of Service Attacks / Q. Gu, P. Liu // Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications. – 2012. – Vol. 3. (In English).
3. Tripathi N. DoS and DDoS Attacks: Impact, Analysis and Countermeasures. / N. Tripathi, B.M. Mehtre // Conference: Advances in Computing, Networking and Security: TEQIP II National Conference. – 2014. – Access Mode: https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Imp act_Analysis_and_Countermeasures (online; accessed: 2023-06-15). (In English).
4. Afanas'eva D.V. Problema DDoS-atak / D.V. Afanas'eva // Nauka, obrazovanie i kul'tura. – 2019. – Rezhim dostupa: https://cyberleninka.ru/article/n/problema-ddos-atak (data obrashcheniya: 2021-06-23). (In Russian).
5. securelist – DDoS-ataki v I kvartale 2021 goda. – 2021. – Rezhim dostupa: https://securelist.ru/ddos-attacks-in-q1-2021/101390/ (data obrashcheniya: 2021-06-24). (In English).
6. Zeb K. DDoS Attacks and Countermeasures in Cyberspace / K. Zeb, O. Baig, M.K. Asif // IEEE 2nd World Symposium on Web Applications and Networking (WSWAN). – 2015. – Mar. – P. 1-6. (In English).
7. Slepovichev I.I. Obnaruzhenie DDoS atak nechetkoi neironnoi set'yu. // Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya Matematika. Mekhanika. Informatika. –2009. – Rezhim dostupa: https://cyberleninka.ru/article/n/obnaruzhenie-ddos-atak-nechetkoy-neyronnoy-setyu (data obrashcheniya: 2023-06-21). (In Russian).
8. Doriguzzi-Corin R. Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detectionn / R. Doriguzzi-Corin // IEEE Transactions on Network and Service Management. – 2020. – Feb. – P. 1-14. (In English).
9. Ispol'zovanie SVM dlya obnaruzheniya DDoS-atak v seti SDN / Dong Li i dr. // IOP Conf. Ser.: Mater. nauk. Eng. 466 012003, 2018. (In English).

10. Metod obnaruzheniya DDoS-atak, osnovannyi na izvlechenii priznakov iz setei glubokikh ubezhdenii / Itsze Li i dr. // seriya konferentsii IOP: Nauka o okruzhayushchei srede, tom 252, vypusk 3. – 2019. (In English).
11. Obnaruzhenie DDoS-atak na tsentry obrabotki dannykh s pomoshch'yu korrelyatsionnogo analiza / Pehn Syao i dr. // Komp'yuternye kommunikatsii. – 2015. № 67. (In English).
12. Razrabotka i vnedrenie sistemy obnaruzheniya DDoS-atak Interneta veshchei, osnovannoi na mashinnom obuchenii / YU.V. Chen i dr. // V materialakh Evropeiskoi konferentsii IEEE po setyam i kommunikatsiyam, Dubrovnik, Khorvatiya, 15-18 iyunya 2020. – S. 122-127. (In English).
13. Obnaruzhenie atak tipa «otkaz v obsluzhivanil» i smyagchenie ikh posledstvii dlya Interneta veshchei s ispol'zovaniem metodov mashinnogo obucheniya s podderzhkoi retrospektivnogo analiza / A. Mikhub i dr. // Vychisl. Ehlektr. Angl. – 2022. № 98. R. 107716. (In English).

Б.М. Ильясов*, Ж.М. Әлімжанова
әл-Фараби атындағы Қазақ ұлттық университеті,
050040, Қазақстан Республикасы, Алматы қ., әл-Фараби даңғылы, 71
e-mail*: bahalar49@gmail.com

DDOS ШАБУЫЛДАРЫНАН ҚОРҒАУ МОДЕЛІН ЗЕРТТЕУ

Бұл зерттеу шабуылдаушылар серверді есептеу мүмкіндіктерін нашарлату үшін шамадан тыс сұраныстармен шамадан тыс жүктеген кезде flooding шабуылдарына назар аудара отырып, қызмет көрсетуден бас тартудың таратылған моделін (DDoS) зерттейді. DDoS шабуылдарының әсерін азайтуға бағытталған дәстүрлі тәсілдерден айырмашылығы, біздің зерттеуіміз осындай қауіптерден қорғаудың сенімді модельдерін жасауға баса назар аударады. Біз тек заңды трафиктің серверге жетуін қамтамасыз ете отырып, сұраныстардың ағынын бақылау үшін жылдамдықты шектеу алгоритмдерін қамтитын жаңа қорғаныс стратегиясын ұсынамыз. Сонымен қатар, біз сервердің тиімділігі мен тиімділігін арттыру үшін пакетті жоспарлаудың инновациялық әдістерімен, соның ішінде first-Come, First-Served (FCFS) және Priority Queue әдістемесімен біріктірілген жарамды уақыт (TTL) мәндеріне негізделген пакетті сүзуді зерттейміз. Модельдеудің арқасында біздің нәтижелер DDOS шабуылы жағдайында сервер өнімділігінің айтарлықтай жақсарғанын көрсетеді, бұл пакетті тастау жылдамдығының төмендеуімен және жауап беру уақытының жақсаруымен көрінеді. Осы қорғаныс модельдерін сәтті енгізу олардың желілерді DDoS шабуылдарының жойқын әсерінен қорғаудағы әлеуетін көрсетеді, бұл болашақ киберқауіпсіздік зерттеулерінің перспективалық бағытын ұсынады.

Түйін сөздер: *DDoS қорғанысы; flooding шабуылдары; жылдамдықты шектеу; TTL; пакетті жоспарлау; киберқауіпсіздік.*

B.M. Ilyasov*, Zh.M. Alimzhanova
al-Farabi Kazakh National University,
050040, Republic of Kazakhstan, Almaty, al-Farabi Ave., 71
e-mail*: bahalar49@gmail.com

RESEARCH OF THE MODEL OF PROTECTION AGAINST DDOS ATTACKS

This research investigates the Distributed Denial-of-Service (DDoS) protection model, focusing on flooding attacks, where attackers overwhelm a server with excessive requests to degrade its processing capabilities. Unlike traditional approaches that merely aim to mitigate the impact of DDoS attacks, our study emphasizes developing robust protection models to safeguard against such threats. We introduce a novel protection strategy that incorporates rate-limiting algorithms to control the influx of requests, ensuring that only legitimate traffic reaches the server. Further, we explore packet filtering based on valid Time-to-Live (TTL) values, coupled with innovative packet scheduling techniques: including First-Come, First-Served (FCFS) and Priority Queue methodologies to enhance server responsiveness and efficiency. Through simulations our findings reveal significant improvements in server performance under DDoS attack conditions, evidenced by reduced packet drop rates and improved response times. The successful implementation of these protection models demonstrates their potential in securing networks against the disruptive effects of DDoS attacks, offering a promising direction for future research in cybersecurity.

Key words: *DDoS protection; flooding attacks; rate-limiting; TTL; packet scheduling; cybersecurity.*

Сведения об авторах

Бахтияр Муратулы Ильясов* – магистрант, Системы информационной безопасности; Казахский Национальный университет имени аль- Фараби; Республика Казахстан; e-mail: bahalar49@gmail.com.

Жанна Муратбековна Алимжанова– кандидат физико-математических наук, старший препопадаватель; Казахский Национальный университет имени аль- Фараби; Республика Казахстан.

Авторлар туралы мәліметтер

Бахтияр Мұратұлы Ильясов* – «Ақпараттық қауіпсіздік жүйелері» магистранты; әл-Фараби атындағы Қазақ ұлттық университеті; Қазақстан Республикасы; e-mail: bahalar49@gmail.com.

Жанна Мұратбекқызы Әлімжанова – физика-математика ғылымдарының кандидаты, аға оқытушы; әл-Фараби атындағы Қазақ ұлттық университеті; Қазақстан Республикасы.

Information about the authors

Bakhtiyar Muratuly Ilyassov* – Master's student, Information Security Systems; Al-Farabi Kazakh National University; The Republic of Kazakhstan; e-mail: bahalar49@gmail.com.

Zhanna Muratbekovna Alimzhanova – candidate of physical and mathematical sciences, senior teacher; Al-Farabi Kazakh National University; The Republic of Kazakhstan.

Поступила в редакцию 28.05.2024
Поступила после доработки 12.06.2024
Принята к публикации 13.06.2024

DOI: 10.53360/2788-7995-2024-2(14)-4

МРНТИ: 49.38.49

А.А. Мухамедин*, Г.А. Абитова
Astana IT University
010000, Республика Казахстан, г. Астана, пр. Мангилик Ел, 55/11
*e-mail: 222153@astanait.edu.kz

ИССЛЕДОВАНИЕ REACT NATIVE И FLUTTER, КРОССПЛАТФОРМЕННЫХ ФРЕЙМВОРКОВ ДЛЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Аннотация: *В статье выявлено, что создание мобильных приложений отдельно для Android и iOS становится сложным и затратным процессом. Появляется необходимость в общем решении, которое упростит процесс разработки, поддержки, тестирования и развертывания на различных платформах. Это решение должно стандартизировать процесс создания мобильных приложений.*

React Native, созданный Facebook, представляет собой значимый этап в развитии кроссплатформенной разработки мобильных приложений. Благодаря активному и мощному сообществу, React Native стал самым востребованным инструментом для создания кроссплатформенных приложений. Тем не менее, Google решил разработать свое собственное решение, Flutter, после тщательного анализа преимуществ и недостатков React Native. Flutter нацелен на оптимизацию для мобильных устройств и стремится предоставить разработчикам полноценное и окончательное решение для создания кроссплатформенных приложений.

В данной статье анализируются ключевые характеристики React Native и Flutter, проводится исследование и сравнение этих характеристик с целью выявления причин их различий. Авторы статьи надеются, что результаты исследования помогут совершенствовать кроссплатформенную разработку и обеспечат дальнейший прогресс в этой области.

Ключевые слова: *Andorid, фильмы, разработка, искусственный интеллект, Архитектура, кроссплатформенный, исследование, интеграция, IOS, React Native, Flutter.*

Введение

С каждым днем мобильные приложения становятся все более существенными для нашей повседневной жизни. Согласно данным с ноября 2016 года, объем сетевого трафика, который передается через мобильные устройства, составляет 48,19%, что превышает объем трафика от настольных компьютеров и ноутбуков (47%) [1].