Шаханова М.В., Солоненко Д.Ю., Шаханова Э.С. Разработка системы защиты от атаки сканирования сетевых портов // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.1. с. 67–74

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ АТАКИ СКАНИРОВАНИЯ СЕТЕВЫХ ПОРТОВ

Шаханова М.В., Солоненко Д.Ю., Шаханова Э.С.
ФГБОУ ВО «Морской государственный университет имени Г.И. Невельского», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: marinavl2007@yandex.ru

Программно-определяемая сеть (SDN от англ. Software-defined Networking, также программно-определяемая сеть) является одной из важных технологий для сетей 5G и будущих сетей 6G. Она разделяет плоскость управления сетью и плоскость данных, предоставляет пользователям гибкий программный интерфейс для управления поведением сети и значительно повышает гибкость сети. Тем не менее, как SDN, так и традиционные сети уязвимы для повреждения аномального трафика, такого как распределенные атаки типа «отказ в обслуживании» (DDoS, распределенный отказ в обслуживании) [1-2], аномальный трафик снижает безопасность и доступность сети. Для реализации обнаружения аномалий в традиционных компьютерных сетях необходимо развертывание специального оборудования. Из-за распределенного характера традиционных сетей развертывание этого специального оборудования требует больших затрат и снижает гибкость сети. По сравнению с традиционными сетями SDN позволяет создавать более надежные, масштабируемые и управляемые сети для упрощения развертывания новых сетевых функций [3]. Таким образом, обнаружение сетевых аномалий и защита от них могут быть реализованы централизованно на контроллере SDN. Однако сама сеть на основе SDN не имеет функций обнаружения аномалий и защиты, и существуют риски безопасности. Тем не менее, парадигма SDN может обеспечить новый подход к обнаружению сетевых аномалий и проектированию систем защиты по следующим причинам: SDN обеспечивает глобальное представление о сети; SDN очень удобна для сбора статистики трафика; SDN использует централизованную плоскость управления, что удобно пользователям для развертывания новых приложений [4]. ка. В то же время система обладает высокой масштабируемостью и может гибко обнаруживать различные типы аномального поведения сети.

Ключевые слова: Обнаружение вторжений Windows, программно-определяемая сеть, обнаружение аномалий, энтропия Реньи, сетевая безопасность.

DEVELOPMENT OF A PROTECTION SYSTEM AGAINST NETWORK PORT SCANNING ATTACKS

Shakhanova M. V., Solonenko D.Yu., Shakhanova E.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: marinavl2007@yandex.ru

Software-defined networking (SDN) is one of the important technologies for 5G and future 6G networks. It separates the network control plane and data plane, providing users with a flexible software interface to manage network behavior and significantly improving network flexibility. However, both SDN and traditional networks are vulnerable to anomalous traffic, such as distributed denial-of-service (DDoS) attacks [1-2]. Anomalous traffic decreases network security and availability. Traditional computer networks require specialized equipment to detect anomalies, which is costly and reduces network flexibility due to their distributed nature. Compared to traditional networks, SDN allows for the creation of more reliable, scalable, and manageable networks to simplify the deployment of new network functions [3]. Therefore, detecting network anomalies and protecting against them

can be implemented centrally on the SDN controller. However, the SDN-based network itself lacks anomaly detection and protection functions, and there are security risks. Nevertheless, the SDN paradigm can provide a new approach to network anomaly detection and protection design for the following reasons: SDN provides a global view of the network; SDN is very convenient for collecting traffic statistics; and SDN uses a centralized control plane, which is convenient for users to deploy new applications [4]. At the same time, the system has high scalability and can flexibly detect various types of anomalous network behavior.

Keywords: Windows intrusion detection, software-defined networking, anomaly detection, Renyi entropy, network security.

Исследование безопасности SDN в основном включает два аспекта. С одной стороны, исследователи сосредотачиваются на вопросах безопасности самой парадигмы SDN. Из-за характеристик централизованного управления SDN они сталкиваются с рядом проблем безопасности с точки зрения плоскости управления, плоскости приложений, плоскости данных и стандартного интерфейса, таких как вредоносные приложения, мониторинг сети, спуфинг IP-адресов, DoS/DDoS-атаки и вирусы. Атаки троянских коней и т. д. Это огромное препятствие, ограничивающее коммерциализацию SDN. С другой стороны, использование SDN для решения проблем безопасности, с которыми сталкиваются традиционные сети. Поскольку SDN имеет возможность централизованного управления сетью и детального управления трафиком, исследователи, как правило, используют технологию SDN для определения возможностей работы сетевой безопасности и механизмов реагирования на чрезвычайные ситуации.

Например, опираясь на возможности точного управления трафиком SDN, можно легко реализовать обнаружение аномалий на основе трафика и контроль доступа, которые можно использовать для обнаружения и защиты от DDoS-атак и атак с расширенными постоянными угрозами в корпоративных интрасетях. Что касается планирования трафика, SDN имеет возможность гибко организовывать маршруты и может управлять сетевым трафиком, проходящим через определенные устройства безопасности, тем самым реализуя цепочки услуг безопасности по запросу. С точки зрения методов обнаружения сети, в традиционных сетях машинное обучение широко используется для классификации трафика и обнаружения аномалий [5]. Хотя методы машинного обучения обладают высокой точностью обнаружения, они часто имеют следующие ограничения: приходится полагаться на массивные размеченные обучающие данные для обучения [6].

Вычислительные ресурсы используются для своевременной обработки и обнаружения аномалий [7]; полагаются на разнообразные ресурсы сетевых устройств, такие как системы управления и различные сетевые промежуточные блоки, для сбора информации о состоянии сети.

Кроме того, методы на основе энтропии также используются для обнаружения аномального трафика в традиционных сетях [8]. Эти технологии используют теорию энтропии для моделирования состояния сети. Рассчитывая и анализируя изменение значения энтропии в течение определенного периода времени, можно обнаружить аномальное отклонение значения энтропии, чтобы определить, когда в сети возникают помехи. Исследования показали, что метод обнаружения аномалий на основе энтропии представляет собой простую в развертывании, недорогую, точную технологию мониторинга сетевой безопасности в режиме реального времени [9]. Обнаружение вторжений на основе энтропии широко изучалось, однако эти методы обычно применяются в крупномасштабных магистральных IP-

сетях и не очень применимы к маломасштабным сетям или другим типам сетей [8-11]. В то же время традиционные схемы обнаружения вторжений включают только обнаружение и классификацию аномального поведения, и большинство исследований не фокусируются на том, как диагностировать и защищаться от аномального поведения сети после обнаружения.

Преимущество SDN заключается в обнаружении и контроле глобального сетевого трафика, что облегчает детальный анализ и управление сетью в режиме реального времени. Эта сетевая парадигма оказала влияние на традиционную модель сетевой безопасности, в основном в следующие два аспекта:

1. Различия в методах развертывания устройств безопасности: в традиционных сетях устройства безопасности, такие как системы обнаружения вторжений, развертываются в ключевых точках сети, требуя, чтобы конфиденциальные данные проходили через устройства безопасности, прежде чем устройства безопасности смогут выполнять мониторинг в реальном времени и обнаружение; и в SDN все пути передачи данных контролируются контроллером SDN, и ограничения местоположения устройств безопасности снимаются.
2. Различные способы оценки состояния безопасности: в традиционных сетях сетевой администратор должен отправлять информацию запроса состояния на несколько устройств безопасности и после получения информации проводить всестороннюю оценку для получения информации о состоянии безопасности сети; в то время как в SDN, контроль Сервер регулярно собирает информацию с плоскости данных, чтобы понять общую ситуацию в сети.

В качестве модели атаки используются 3 этапа DDoS-атаки, и эти 3 этапа включают следующие аномальные действия сети:

1. Сканирование портов (сканирование портов). Злоумышленники обычно используют сканирование портов, чтобы узнать, открыт ли набор портов на удаленном узле. Некоторые открытые порты могут быть использованы злоумышленниками для атаки на целевую систему или распространения червей [12]. Обычно злоумышленник использует сценарий атаки, чтобы инициировать сканирование портов на атакуемом сервере, и сценарий отправляет несколько пакетов TCP-подключения на порты от 0 до 65536. При обнаружении открытого порта сценарий вернет злоумышленнику уведомление, и злоумышленник сможет определить, какой тип атаки может выполнять порт. Как правило, при сканировании портов создаются пакеты с фиксированными IP-адресами, но с разными номерами портов назначения TCP в сети.
2. Распространение червей. Червь — это самовоспроизводящаяся программа, которая пытается заразить другие машины, используя определенную уязвимость. Ботнеты распространяются в основном через активные атаки, через уязвимости, программное обеспечение для обмена мгновенными сообщениями, почтовые вирусы, вредоносные скрипты веб-сайтов, троянские кони и т. д. [13]. Злоумышленники также будут комбинировать технологии червей для улучшения метода распространения ботов [14], чтобы боты могли распространяться автоматически, как, например, знаменитый образец бота AgoBot [15]. Бот-программы программы, распространяемые червями, могут быстро создавать крупномасштабные бот-сети.

Распределенная атака типа «отказ в обслуживании». После формирования в SDN ботнета определенного масштаба могут быть запущены DDoS-атаки. Существует множество способов DDoS-атак: можно переполнить таблицу потоков конкретного коммутатора, создав большое количество поддельного трафика, или перегрузить контроллер SDN, генерируя несколько

пакетов packet_in. Обычно эти атаки проявляются в виде большого количества различных исходных IP-адресов, обращающихся к определенному IP-адресу назначения.

Основные принципы предлагаемой системы

Энтропия Шеннона и энтропия Реньи: энтропия измеряет неопределенность событий, связанных с распределением вероятностей X. Для данной системы, X является дискретной переменной, чей возможный результат выглядит как $\{x_1, x_2, \dots, x_n\}$, т.о. формальное определение энтропии Шеннона есть:

$$H(X) = \sum_{i=1}^{n} p_i lb \frac{1}{p_i} = -\sum_{i=1}^{n} p_i lb p_i \qquad (1)$$

где $p_i \in \{p_1, p_2, \dots, p_n\}$ - вероятность случайной величины X. Чем выше значение энтропии, тем сильнее случайность переменной X, чем меньше значение энтропии, тем выше определенность переменной X.

Энтропия Шеннона имеет большое количество приложений в различных областях, но для измерения малых потоков энтропия Реньи может увеличить разницу между случайными величинами разных распределений больше, чем энтропия Шеннона. Определение энтропии Реньи приведено в формуле (2):

$$H_\alpha(X) = \frac{1}{1-\alpha} lb(\sum_{i=1}^{n} p_i^\alpha) \qquad (2)$$

при $\alpha \geq 0$, $\alpha \neq 1$. Можно доказать, что когда $\alpha = 0$, $H_\alpha(X)$ принимает максимальное значение, т.е.

$$\max(H_\alpha(X)) = lbn \qquad (3)$$

В случае, когда $\alpha \to 1$, энтропия Реньи сходится к энтропии Шеннона, а именно:

$$\lim_{\alpha \to 1} H_\alpha(X) = -\sum_{I=1}^{n} p_i lb p_i \qquad (4)$$

Сетевой поток представляет собой коммуникация передачей сетевых пакетов между двумя точками. Вектор маркировки вредоносного поведения отмечает разновидность сетевого злонамеренного поведения в двоичном коде, и сравнение вредоносного поведения показано в Таблице 1.

Например, когда в сети нет аномалий, вектор метки вредоносного поведения равен (0,0,0,0,0,0). Однако, когда происходит сканирование портов, количество типов номеров портов назначения в сети значительно увеличивается, а соответствующее значение энтропии резко возрастает. Как только модуль обнаружения аномалий обнаружит изменение значения энтропии, он установит положение номер порта назначения на «1».

Таблица 1 – Сравнение аномального поведения

Вредоносное поведение	Маркер векторной сети	Характер аномального поведения
(0,1,0,0,0,0)	Номер порта назначения и источник	Значение энтропии номера порта назначения сканирования портов значительно увеличивается
(0,1,1,0,0,0)	Распространение червя	Значительное снижение IP-энтропии
(0,1,0,1,0,0)	DDoS-атака	IP-адрес назначения и номер порта назначения значительно снизились

Обнаружение, диагностика и защита от аномального поведения в SDN могут быть реализованы с использованием информации из базы потоков коммутатора OpenFlow и протокола OpenFlow. После обнаружения аномального значения энтропии соответствующий элемент трафика извлекается и отправляется в модуль диагностики вредоносного поведения. Этап диагностики сети в основном отвечает за диагностику и защиту от злонамеренного поведения. Модуль диагностики вредоносного поведения получает записи потока, диагностирует вредоносный трафик и исходный IP-адрес вредоносного трафика и отправляет его в модуль сетевой защиты для блокировки вредоносного трафика. Система может оценивать три вида злонамеренного поведения и отправлять записи базы данных для других неопознанных аномальных действий для дальнейшего анализа в последующей работе.

Компоненты системы. В таблице 2: модуль сбора информации: он в основном отвечает за периодический сбор информации о трафике на уровне данных, и информация о трафике представлена в виде снимков информации таблицы потоков. Модуль сбора информации отправляет запрос на извлечение информации из таблицы потоков на сетевой контроллер через интерфейс приложения передачи репрезентативного состояния (Rest API), чтобы запросить состояние всего трафика в плоскости данных. После получения информации таблицы потоков от сетевого контроллера модуль сбора информации анализирует и организует соответствующие данные для формирования моментального снимка информации таблиц.

Таблица 2 – Поля соответствия OpenFlow

порт назначения	исходный IP-адрес	IP-адрес источника	MAC-адрес назначения
tcp_src	ipv4_src	ipv4_dst	eth_dst

Каждый поток соответствует тройному набору признаков, набор функций определяется спецификацией OpenFlow [3], как показано в Таблице 3:

Таблица 3 – Информация о наборе функций

Количество совпадающих пакетов	Байтов передано	Активное время
packet_count	byte_count	duration_sec

Таким образом, может быть сформирован информационный снимок таблицы потоков $S = \{F: (c, d, d)\}$.

Модуль обнаружения аномалий: в основном отвечает за обнаружение аномального трафика в сети на основе информации о моментальных снимках трафика. В этом модуле в основном используется метод обнаружения, основанный на энтропии Реньи, в то же время для сравнения используются традиционная энтропия Шеннона и энтропия Реньи.

Модуль сетевой диагностики: обнаруженное вредоносное поведение маркируется модулем обнаружения аномалий, и информационный снимок таблицы потоков с развитием энтропии. Сначала по вектору меток вредоносного поведения идентифицируется бит, вызывающий энтропийную мутацию, и оценивается тип вредоносного поведения (сканирование портов, распространение вируса-червя, DDoS- атака).

Первое суждение основано на следующем: запись потока, активное время которого меньше, должна быть зарегистрирована, а поток, который вызывает внезапное изменение значения энтропии, должен быть среди вновь выпущенных записей. Затем подсчитывается частота исходного IP-адреса в вредоносных записях потока. IP-адрес или набор IP-адресов с наибольшей частотой — это исходный IP-адрес или набор IP-адресов, которые генерируют вредоносный трафик (если диагностируемое вредоносное поведение представляет собой DDoS- атаку, он соответствует исходному набору IP-адресов). Соответствующие записи потока представляют вредоносный трафик.

Модуль защиты сети: получает отчет о диагностике, отправленный модулем диагностики сети, и извлеките запись потока, соответствующую IP- адресу источника вредоносного ПО и вредоносному трафику, из отчета о диагностике.

Заключение

В данной работе предлагается автономная система защиты SDN на основе энтропии Реньи, которая использует преимущества централизованного управления SDN. Во-первых, система собирает информацию таблицы потоков коммутатора OpenFlow, вычисляет значение энтропии для различных полей в соответствующем поле элемента таблицы потоков и сравнивает его с пороговым значением, чтобы определить, есть ли какое-либо ненормальное поведение сети. Затем система диагностирует исходный IP- адрес, который реализует ненормальное поведение сети, дополнительно анализируя время существования таблицы потоков OpenFlow и подсчитывая частоту появления IP-адреса. Наконец, система реализует защитные меры, такие как блокировка связи от вредоносного трафика. Предлагаемая система может обнаруживать три самых распространенных аномальных поведения сети.

Список литературы

1. BRAGA R, MOTA E, PASSITO A Обнаружение атак с использованием NOX/OpenFlow//The 35th Annual IEEE, Конференция по локальным компьютерным сетям, 2010.
2. BEHAL S, SINGH J. Обнаружение и смягчение последствий DDoS-атак в SDN: всесторонний обзор, исследовательские задачи. Computer Science Review, 2020, 37: C.1-25.

3. МАККОУН Н., АНДЕРСОН Т., БАЛАКРИШНАН Х. и др. OpenFlow: внедрение инноваций в кампусные сети, ACM Computer Communication Review, 2008, 38(2):69-74.
4. ZHAO P, ZHAO W, LIU Q. Многоцелевое разделение каналов. я Международная конференция (MSN), 2019: С.253-258.
5. САЛМАН О., ЭЛЬХАДЖ И.Х., КАЙСИ А. и др. Обзор подходов к классификации интернет-трафика, 2020: С.1-38.
6. УИЛЬЯМС Н., ЗАНДЕР С., АРМИТИДЖ Г. Предварительное сравнение пяти алгоритмов машинного обучения для классификации потоков IP-трафика. ACM SIGCOMM, 2006, 36(5): С.5-16.
7. ЛАХИНА А., КРОВЕЛЛА М., ДИОТ С. Аномалии с использованием распределения характеристик трафика//ACM Sigcomm Conference, 2005: 217с.
8. FIADINO PD, DALCONZO A, SCHIAVONE M, et al. Обнаружение и диагностика аномалий на основе энтропии в сотовой сети, ACM Sigcomm Computer Communication Review, 2015, 45(4): С.87-88.
9. ТИМЧЕНКО В.В., ИБРАГИМ Д., ГАДЖИН С. Поддержка гибридного машинного обучения для обнаружения аномалий сетевого трафика на основе энтропии. //ICIST 2019. 2019: С.144-149
10. ИБРАГИМ Ю., ТИМЧЕНКО В.В., ГАЙИН С. Комплексная архитектура обнаружения аномалий на основе потока с использованием расчета энтропии и классификации машинного обучения //ICIST 2019. 2019: С.138-143.
11. ШУКЛА А.С., МАВРЯ Р. Обнаружение аномалий на основе энтропии. Беспроводная персональная связь, 2018, 99: 1487-1501 гг.
12. SCHAEFFER-FILHO A, MAUTHE A, HUTCHISON D, et al. Набор инструментов для оценки стратегии устойчивости сети. //Международный симпозиум IFIP/IEEE по интегрированной сети. Менеджмент труда, 2013.
13. STONE-GROSS B, COVA M, GILBERT B и др. Захват ботнета, IEEE Security & Privacy, 2011, 9(1): С.64-72.
14. WANG Q, CHEN Z, CHEN C и др. О надежности топологии сети. //Global Telecom, Конференция катионов, 2010.
15. ЧЖОУ ЦЗЯЦЗЮНЬ, ВАН ТИНТИН, Анализ случая использования Agobot на основе контрмер компьютерной сети, Технология и применение сетевой безопасности, 2013, (7): С.86-88.
16. Шаханова М.В., Солоненко Д.Ю., Шаханова Д.С. – «Актуальные проблемы информационной безопасности банков» // BULLETIN ALMANACH SCIENCE ASSOCIATION FRANCE-KAZAKHSTAN, 2022/5. С. 266-276.

References

1. BRAGA R, MOTA E, PASSITO A Detection of attacks using NOX/OpenFlow//The 35th Annual IEEE, Conference on Local Computer Networks, 2010.
2. BEHAL S, SINGH J. Detection and mitigation of DDoS attacks in SDN: a comprehensive overview, research tasks. Computer Science Review, 2020, 37:pp.1-25.

3. MCCONE N., ANDERSON T., BALAKRISHNAN H. and others . OpenFlow: Introducing Innovation to Campus Networks, ACM Computer Communication Review, 2008, 38(2):pp.69-74.
4. ZHAO P, ZHAO W, LIU Q. Multi-purpose channel separation. I International Conference (MSN), 2019: pp.253-258.
5. SALMAN O., ELHAJ I.H., KAYSI A. et al. Review of approaches to the classification of Internet traffic, 2020:pp. 1-38.
6. WILLIAMS N., ZANDER S., ARMITAGE G. A preliminary comparison of five machine learning algorithms for classifying IP traffic flows. ACM SIGCOMM, 2006, 36(5): pp.5-16.
7. LAKHINA A., KROVELLA M., DIOT S. Anomalies using the distribution of traffic characteristics//ACM Sigcomm Conference, 2005: 217.
8. FIADINO PD, DALCONZO A, SCHIAVONE M, et al. Entropy-based Anomaly Detection and Diagnosis in Cellular Networks, ACM Sigcomm Computer Communication Review, 2015, 45(4): pp.87-88.
9. TIMCHENKO V.V., IBRAHIM D., GADZHIN S. Support for hybrid machine learning to detect network traffic anomalies based on entropy. //ICIST 2019. 2019: pp.144-149
10. IBRAHIM Yu., TIMCHENKO V.V., GAYIN S. Complex architecture of anomaly detection based on flow using entropy calculation and machine learning classification //ICIST 2019. 2019: pp.138-143.
11. SHUKLA A.S., MAVRYA R. Detection of anomalies based on entropy. Wireless Personal Communication, 2018, 99:pp.1487-1501.
12. SCHAEFFER-FILHO A, MAUTHE A, HUTCHISON D, et al. A set of tools for evaluating network resilience strategies. //IFIP/IEEE International Symposium on Integrated Networking. Labor Management, 2013.
13. STONE-GROSS B, COVA M, GILBERT B, etc. Botnet Hijacking, IEEE Security & Privacy, 2011, 9(1): pp.64-72.
14. WANG Q, CHEN Z, CHEN C, etc. About the reliability of the network topology. //Global Telecom, Cation Conference, 2010.
15. ZHOU JIAJUN, WANG TINGTING, Agobot use case analysis based on computer network countermeasures, Network Security Technology and Application, 2013, (7): pp.86-88.
16. Shakhanova M.V., Solonenko D.Yu., Shakhanova D.S. – "Actual problems of information security of banks" // BULLETIN ALMANACH SCIENCE ASSOCIATION FRANCE-KAZAKHSTAN, 2022/5. pp. 266-276.