УДК 004

Фирсова А.А.
Магистрант
2 курс, Факультет оптических и квантовых коммуникаций
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»

СОВМЕСТНАЯ СХЕМА ОБНАРУЖЕНИЯ DDOS-АТАК НА ОСНОВЕ ЭНТРОПИИ И КОЛЛЕКТИВНОГО ОБУЧЕНИЯ В SDN

Аннотация: *в статье рассматривается решение проблемы обнаружения распределенных атак типа "отказ в обслуживании" (DDoS) в программно-определяемой сети, предложена схема обнаружения совместной DDoS-атаки на основе энтропии и коллективного обучения. Этот метод настраивает модуль предварительного обнаружения на основе энтропии в пограничном коммутаторе для мониторинга состояния сети в режиме реального времени и сообщения контроллеру при обнаружении каких-либо отклонений. Результаты моделирования двух распространенных методов DDoS-атаки, ICMP и SYN, показывают, что система может эффективно обнаруживать DDoS-атаки и значительно сокращать затраты на связь и нагрузку на контроллер, а также задержку обнаружения атак.*

Ключевые слова: *DDoS-атаки, SDN сети, OpenFlow, ботнет, SYN-Flood.*

Abstract: *the article discusses the solution to the problem of detecting distributed denial of service attacks (DDoS) in a software-defined network, a scheme for detecting a joint DDoS attack based on entropy and collective learning is proposed. This method configures the entropy-based pre-detection module in the edge switch to monitor the network status in real time and report to the controller when any deviations are detected. The simulation results of two common DDoS*

attack methods, ICMP and SYN, show that the system can effectively detect DDoS attacks and significantly reduce communication costs and load on the controller, as well as the delay in detecting attacks.

Keywords: *DDoS attacks, SDN networks, OpenFlow, botnet, SYN-Flood.*

С развитием облачных вычислений, больших данных и других новых технологий сетевой трафик постоянно растет, и традиционной сетевой архитектуре с IP в качестве ядра сложно удовлетворить потребности в масштабируемости, управлении и гибкости сети. Программно-определяемая сеть (SDN), как новая сетевая архитектура, ее основная идея заключается в том, что уровень управления и уровень данных разделены, где состояние сети логически централизовано, а контроллер абстрагирован от базового сетевого объекта. Появление SDN значительно улучшает управляемость, расширяемость, управляемость и динамику сети. Однако с ростом популярности приложений SDN безопасность SDN стала одной из ключевых тем исследований в области SDN [1]. Распределенная атака типа "отказ в обслуживании" (DDoS), как одна из наиболее важных угроз безопасности, с которыми сталкивается Интернет сегодня, особенно опасна в SDN из-за ее сильной разрушительной силы, простой реализации и отсутствия простых и осуществимых контрмер. Чтобы заблокировать атакуемую цель, предоставляющую услуги законным пользователям, злоумышленник создает ботнет через марионеточный хост, запускает сетевую атаку для использования процессора, пропускной способности, памяти и других ресурсов атакуемых целей. Большинство традиционных схем защиты сети от DDoS-атак сосредоточены на очистке трафика и блокировке брандмауэром, что затрудняет достижение унифицированного планирования всей сети и не дает эффективных результатов даже при больших затратах ресурсов. В то время как появление SDN открывает новые возможности для обнаружения DDoS-атаки, которая обеспечивает основу для мониторинга всей сети в режиме реального

времени и ситуации с трафиком каждого узла с его функцией централизованного управления, а также программируемости. Существующие методы варьируются от традиционных статистических методов и современных алгоритмов машинного обучения до комбинации нескольких методов, а затем и сложных методов глубокого обучения. Все они используют преимущества глобального представления и централизованного управления на уровне управления для повышения точности обнаружения DDoS-атак. Однако из-за сбора потоков, статистики, классификации, все это необходимо обрабатывать на контроллере SDN. Когда масштаб сети увеличивается, контроллеру приходится сталкиваться с огромными накладными расходами, что приводит к задержке обнаружения атаки. И худшая ситуация заключается в том, что до обнаружения DDoS-атаки контроллер уже перегружен или даже отключен. Одновременно контроллеру необходимо часто получать таблицу потоков и информацию о пакетах от пограничного коммутатора для обнаружения атаки. Таким образом, когда масштаб сети увеличивается, нагрузка на интерфейс будет тяжелой. Поэтому в процессе обнаружения DDoS-атак важной темой исследования является то, как снизить нагрузку на контроллер и интерфейс, а также повысить скорость обнаружения атак при обеспечении точности обнаружения. Для этой цели и разрабатывается совместная схема обнаружения DDoS-атак на основе SDN. Учитывая программируемые возможности коммутатора OpenFlow, обычно остаются некоторые вычислительные ресурсы, которые используются не полностью [2]. Таким образом, соответствующие задачи статистики и анализа данных расположены на пограничном коммутаторе, который может реализовать часть функции обнаружения атак, чтобы снизить нагрузку на контроллер и повысить скорость реагирования на обнаружение атак.

В данном исследовании все коммутаторы OpenFlow, управляемые одним и тем же контроллером, определены как домен, что показано на Рис. 1. Кроме того, домены соединены друг с другом пограничными коммутаторами.

В отличие от традиционного метода обнаружения DDoS-атак, который полагается только на контроллер, создана новая система обнаружения DDoS-атак на основе SDN, в которой весь процесс обнаружения разделен на два разных этапа: один на уровне данных, а другой на уровне управления.

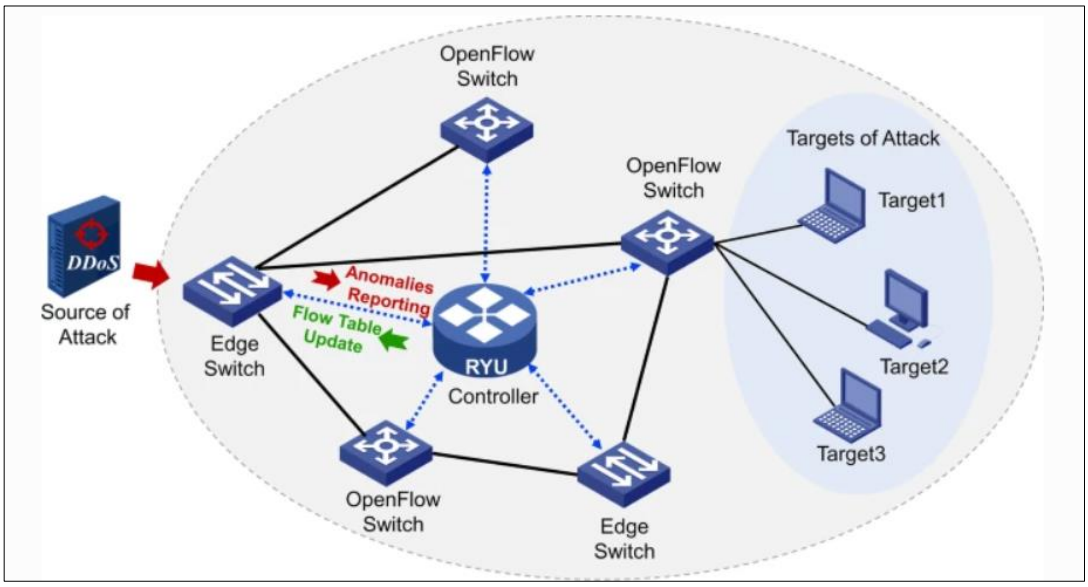

Рисунок 1. Модель системы обнаружения DDoS-атак

В данной статье предлагается совместная схема обнаружения DDOS-атак, основанная на обучении энтропии, которая практично использует вычислительные мощности пограничного коммутатора для переноса части задач обнаружения с уровня управления на уровень данных. Облегченный алгоритм в пограничном коммутаторе и точный метод в контроллере совместно выполняют полное обнаружение, что значительно снижает нагрузку на контроллер и накладные расходы на связь в южном направлении.

В пограничном коммутаторе на уровне данных разработан алгоритм быстрого обнаружения аномалий, основанный на информационной энтропии. Ее низкая сложность обеспечивает низкую нагрузку на ресурсы пограничного коммутатора при одновременном мониторинге трафика в режиме реального времени.

В контроллере на плоскости управления создается набор из 5 функций, охватывающий типичные базовые характеристики сетевого трафика, и используем алгоритм случайного леса для дальнейшего точного обнаружения трафика во всем домене, чтобы гарантировать, что аномальный трафик может быть идентифицирован быстро и эффективно, затем команда отбрасывания пакета может быть своевременно передана соответствующим коммутаторам путем обновления таблицы потоков для устранения угрозы атаки.

В этой статье предлагается метод обнаружения совместной DDoS-атаки на основе энтропии и коллективного обучения в SDN. На уровне данных модуль предварительной проверки устанавливается на пограничном коммутаторе для сбора статистики сетевого трафика в режиме реального времени, и контроллер будет замечен при обнаружении отклонений с помощью разработанного алгоритма быстрого обнаружения. А на уровне управления на контроллере разрабатывается модуль точного обнаружения атак, в котором создается группа из пяти элементов, нацеленная на характеристики DDoS-атаки, и алгоритм случайного леса используется для дальнейшей идентификации аномального трафика. Наконец, как только трафик атаки подтвержден, контроллер немедленно отправляет команду на удаление пакета на пограничный коммутатор через обновление таблицы потоков, таким образом, атака будет заблокирована. Эта совместная схема практически использует простаивающие вычислительные мощности пограничного коммутатора для переноса некоторых задач обнаружения с уровня управления на уровень данных.

Список литературы:

1. Q. Ян, Ф.Р. Ю, К. Гун, Дж. Ли, программно-определяемые сетевые (SDN) и распределенные атаки типа "отказ в обслуживании" (DDoS) в средах облачных вычислений: обзор, некоторые вопросы и проблемы исследования. IEEE Communun. Обзор. Преподаватель. 18(1). С 602–622.

2. С. Лим, С. Янг, Ю. Ким, С. Янг, Х. Ким, Планирование контроллера для продолжения работы SDN при DDoS-атаках. Электрон. Lett. 51(16). С 1259–1261.