УДК 004.42

Лавлов А.Ю.
студент магистратуры
2 курс, институт информатики и кибернетики
Самарский национальный исследовательский университет имени академика С.П. Королева
Россия, г. Самара

Lavlov A Yu
graduate student
2 year, Institute of lnformatics and Cybernetics
Samara National Research University
Russia, Samara

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА В ПРОГРАММНО КОНФИГУРИРУЕМЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

A SYSTEM FOR DETECTING ABNORMAL TRAFFIC IN SOFTWARE DEFINED NETWORKS USING MACHINE LEARNING TECHNOLOGIES

Аннотация:

Статья посвящена актуальной на сегодняшний день задаче обнаружения аномального трафика в программно конфигурируемых сетях. Рассматриваются особенности реализации системы с помощью технологий машинного обучения.

Ключевые слова: *интернет вещей, атака распределённого отказа в обслуживании, метод опорных векторов*

Abstract:

The article is devoted to the current problem of detecting abnormal traffic in software defined networks. The features of the system implementation using machine learning technologies are considered.
Keywords: *IoT, DDoS, SVM*

Технология интернета вещей (IoT) объединяет различные устройства: датчики, ПО и оборудование в единую сеть, обеспечивая предприятиям возможность отслеживать рабочие процессы и собирать данные в режиме реально времени. Это позволяет принимать обоснованные решения, а также автоматизировать процессы, в которых присутствие человека может быть опасным для его здоровья. Основные проблемы реализации сети IoT заключается в широком спектре устройств участников этой сети. Эти устройства должны поддерживаться в состоянии автономной работы и не нарушать принципы доверия, безопасности и конфиденциальности сети, в которой они находятся. Открытость технологии IoT делает её уязвимой к атакам. Эти атаки могут быть направлены на выведения компонентов сети из стабильного рабочего состояния путём атаки типа распределённый отказ в обслуживании DDoS. Такая атака перегружает сеть большим объемом пакетов ложных запросов с задачей деградации системы производства. Такие типы атак, при успешном для злоумышленника исходе, приводят к отказу обслуживания легитимных пользователей сети.

Достижения в области программно-конфигурируемых сетей (SDN) и их распространение привело к росту интереса в исследовании разработок SDN-основанных решений в области сетевой безопасности.

Структура SDN-сети обладает преимуществами, в сравнении с обычными сетями, которые являются критически важными для выявления и уменьшения последствий DDoS-атак. Одной из особенностей является отделение плоскости управления от плоскости данных в централизованный программный контроллер. Такое существенное отличие

от обычной сети даёт возможности: изменять параметры сети при помощи внешних приложений, анализировать трафик сети с помощью программ, динамически изменять правила маршрутизации. Ряд работ [1], [2], [3] посвящён также моделированию сетей.

OpenDaylight — это открытая программная платформа для программно-конфигурируемых сетей. Контроллер ODL разработан на языке Java и работает на виртуальной машине JVM. Такая особенность позволяет установить его на любом оборудовании и операционную систему, в которой можно запустить Java-машину.

OpenDaylight состоит из нескольких уровней. Уровень приложений – здесь располагаются прикладные программы. Здесь запускаются политики маршрутизации и системы анализа трафика. Уровень управления – слой, где реализованы северные и южные API взаимодействие с которыми управляет программно-конфигурируемой сетью. Контроллер предоставляет открытые северные API, которыми могут пользоваться приложения. Инфраструктура сети – уровень, где располагаются физические и виртуальные устройства. OpenDaylight поддерживает протокол OpenFlow необходимый для конфигурации сети.

Разработка системы обнаружения DDoS-атак

Существуют различные методы обнаружения DDoS-атак. Программно-конфигурируемые сети позволяют быстрее и эффективнее обнаруживать такие атаки. Алгоритм основан на модели обучения методом опорных векторов (SVM). Разрабатываемый алгоритм обнаруживает узел с аномальным трафиком, сравнивая параметры с выявленными при обучении модели пороговыми показателями. Ключевым элементом исследования стало использование открытого набора данных «IoT-DH Dataset», специально подготовленного для задач сетевой безопасности [4]. Эти данные были собраны в ходе развертывания сети-приманки, которая представляет собой искусственную уязвимую сеть, намеренно открывающую порты и сервисы для привлечения злоумышленников. Такая

сеть действует как пассивный наблюдатель, собирающий данные о стратегиях и типах атак, инициированных извне. Задача обученной модели – определить аномальный трафик.

В машинном обучении используется большое количество метрик, помогающих определить точность и эффективность работы обученной модели. В рамках работы параметрами оценки эффективности исследуемого метода обучения выбраны accuracy, error, hinge loss.

Метод опорных векторов (SVM, от англ. Support Vector Machine) является одним из наиболее популярных алгоритмов машинного обучения, особенно для задач бинарной классификации. Он находит оптимальную разделяющую гиперплоскость между двумя классами, максимизируя отступ (margin) от ближайших точек данных. Это свойство обеспечивает высокую способность обобщения и устойчивость модели при работе с реальными данными, что делает SVM эффективным инструментом в различных областях.

Алгоритм SVM может использовать различные типы ядер (kernels) — функций, которые преобразуют входное пространство в более высокое измерение, где классы могут быть разделены линейно. В данном исследовании применялись радиально-базисное ядро (RBF) и линейное ядро. Эти ядра позволяют охватывать как линейные, так и нелинейные зависимости в данных, что значительно расширяет возможности алгоритма и повышает его адаптивность к различным типам задач.

Одним из главных достоинств «IoT-DH Dataset» является его реалистичность: он отражает поведение злоумышленников в реальной сетевой среде и включает широкий спектр атак — от простого сканирования портов до сложных DDoS-атак, направленных на истощение ресурсов. Это делает набор данных ценным источником для обучения алгоритмов обнаружения угроз, особенно в контексте IoT и SDN-сетей.

Набор данных содержит как нормальный, так и атакующий трафик, который был размечен как вручную, так и автоматически.

Дополнительно, набор данных был расширен за счет информации, собранной в сети с использованием OpenFlow-коммутатора Aruba 2930F. В рамках этого процесса были проведены серии пингов для генерации нормального трафика, а также эксперименты по созданию UDP-трафика с передачей больших пакетов данных, что позволило получить аномальный трафик. Эти дополнительные данные способствуют улучшению качества и точности моделей, направленных на обнаружение аномалий в сетевом трафике.

Использованные источники:

1. Стуликова К.А., Полукаров Д.Ю. Проблемы отображения автономных систем с помощью графов //Известия Самарского научного центра Российской академии наук. – 2014. – Т. 16. – No. 4-2.

2. Капустин И.В., Полукаров Д.Ю. Реализация графовых структур данных с помощью библиотек JAVASCRIPT //IT & Transport/ИТ & Транспорт: сб. науч. статей – Самара, 2016. – С. 81-88.

3. Никулин С. А., Полукаров Д. Ю. НЕКОТОРЫЕ ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ СЕТЕЙ С ЯЧЕИСТОЙ ТОПОЛОГИЕЙ //Перспективные информационные технологии (ПИТ 2019). – 2019. – С.79-81.

4. IoT-DH Dataset. [Электронный ресурс]//Mendeley Data. – URL: https://data.mendeley.com/datasets/8dns3xbckv/1 (дата обращения 12.05.2025).