УДК 004.056 DOI:10.31854/1813-324X-2021-7-4-128-137

Обнаружение аномалий в трафике устройств Интернета вещей

И.Н. Муренин[1]*

[1]Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербург, 199178, Российская Федерация
*Адрес для переписки: imurenin@gmail.com

Информация о статье
Поступила в редакцию 06.12.2021
Поступила после рецензирования 20.12.2021
Принята к публикации 21.12.2021

Ссылка для цитирования: Муренин И.Н. Обнаружение аномалий в трафике устройств Интернета вещей // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 128–137. DOI:10.31854/1813-324X-2021-7-4-128-137

Аннотация: *В статье предложено искать аномалии в трафике устройств Интернета вещей на основе анализа временных рядов и оценки нормального и аномального поведения с помощью статистических методов. Основная цель заключается в комбинировании статистических методов для обнаружения аномалий с использованием неразмеченных данных и построении ключевых характеристик профилей устройств. В рамках данного подхода разработаны и реализованы методики построения признаков и границ нормального поведения, а также обнаружения аномалий на основе анализа трафика. Для их оценки использовалась генерация журналов поступающих с устройств событий с аномальной разметкой. Эксперименты показали, что наилучшие результаты по обнаружению аномалий в трафике устройств Интернета вещей дает метод выявления выбросов с помощью GESD-теста.*

Ключевые слова: *обнаружение аномалий, анализ временных рядов, Интернет вещей, сетевой трафик, статистические методы.*

Введение

Технологии Интернета вещей обмениваются данными без необходимости взаимодействия человека с человеком или человека с компьютером. Интернет вещей все чаще используется организациями для оптимизации своих операций и является одной из самых быстрорастущих технологических областей; к концу 2030 г. Интернет вещей будет насчитывать 50 миллиардов устройств. Инновации в области Интернета вещей вносят свой вклад в улучшение реальных интеллектуальных приложений (например, инфраструктур городов, здравоохранения, транспорта и образования).

Одновременное передовое и широкомасштабное внедрение технологии Интернета вещей создало новые проблемы безопасности [1, 2]. Изучением технологий создания безопасных систем и анализа их защищенности занимаются как зарубежные, так и российские ученые [3–5]. Устройства Интернета вещей подключаются в основном через беспроводные сети, в такой среде злоумышленник может легко получить как физический, так и логический доступ к этим устройствам и вызвать критические последствия [6]. Соблюдение требований безопасности Интернета вещей является нетривиальной задачей ввиду разнородности архитектур, большого количества уязвимостей и интеграции новых и нестандартных инфраструктурных и программных решений [7, 8].

Следующим шагом в эволюции систем Интернета вещей, таких как умные дома, системы здравоохранения, автоматизация систем и промышленный Интернет вещей, является их интеграция в социальные сети [9]. Например, интеграция умных домов в социальную сеть формирует более высокий иерархический уровень их взаимодействия, который дает новые возможности и преимущества, в частности, с точки зрения управления, хранения и обработки информации, улучшения обслуживания конечных пользователей, предотвращения и коллективного реагирования на чрезвычайные ситуации и события и т. д. Однако, интеграция умных домов в социальные сети приводит к появлению новых уязвимостей [10].

В данной работе предлагается подход к обнаружению аномалий в трафике устройств Интернета вещей. Под аномалией понимается значение, которое отклоняется от нормы в такой степени, чтобы его можно было рассматривать как редкое исключение. Подход включает формирование при-

знаков поведения устройств на основе агрегации временных рядов и оценку нормального и аномального поведения на основе статистических методов. Для оценки границ нормального поведения были использованы такие методы, как интерквантильный размах, GESD-тест, Grubs-тест и экспоненциальное сглаживание. Новизна подхода состоит в комбинировании нескольких статистических методов для обнаружения аномалий и предложенном механизме генерации журналов трафика устройств, который используется для оценки результатов обнаружения. Для проведения экспериментов с применением различных методов были сгенерированы журналы, содержащие данные, описывающие трафик устройств с всевозможными видами аномальной активности. В работе представлена оценка количества обнаруженных аномалий каждого типа с использованием предложенных статистических методов. Эксперименты показали, что наилучшие результаты по обнаружению аномалий в трафике устройств Интернета вещей дает метод обнаружения аномалий с помощью GESD-теста.

Работа организована следующим образом. Раздел «Анализ существующих решений» содержит обзор релевантных работ по обнаружению аномалий в трафике устройств инфраструктуры Интернета вещей. Раздел «Обнаружение аномалий в трафике» описывает предложенный подход к обнаружению аномалий и особенности используемых методов оценки. В разделе «Генерация журналов активности устройств и оценка предложенного подхода» представлено описание подхода к генерации журналов для проведения экспериментов и полученные результаты обнаружения аномалий.

Анализ существующих решений

Авторы [11] создали испытательный стенд «умный дом» для сбора потребительского трафика Интернета вещей. На основе этих экспериментов был разработан новый инструмент для моделирования и имитации трафика Интернета вещей. Его можно использовать в качестве основы для композиции сценариев для моделирования сред Интернета вещей, например, умных домов. Также были извлечены данные, содержащие аномальную активность из общедоступного набора данных, выполнено сравнение синтетического и реального трафика, а также сгенерирован новый трафик на основе генерации пакетов для каждого устройства с разными временными периодами и вычисления энтропии параметров трафика для оценки зависимых от устройства атрибутов.

Атрибуты и свойства трафика существенно различались для разных сценариев и каждого типа устройства Интернета вещей, также можно было наблюдать влияние аномального трафика. Кроме того, авторы представили новый метод идентификации устройств Интернета вещей, основанный на вычислении значений энтропии характеристик трафика. Были использованы алгоритмы машинного обучения, такие как «случайный лес» (*от англ.* Random Forest), для классификации устройств на основе значения энтропии трафика Интернета вещей в различных сценариях. Результаты показали, что предложенный метод позволяет классифицировать устройства с точностью до 94 %.

Основной вклад статьи [12] – это введение функции обнаружения аномалий в трафике устройства с учетом местоположения, которая использует хэш-функцию Nilsimsa. Поскольку предложенный в статье метод LSAD (*аббр. от англ.* Locality Sensitive Anomaly Detection – «локальное чувствительное обнаружение аномалий») не требует извлечения функций из данных, его легче адаптировать, чем аналоги, основанные на использовании методов машинного обучения, и обеспечить аналогичные возможности обнаружения без какой-либо настройки параметров.

LSAD использует Nilsimsa и генерирует набор хэшей из безопасных потоков трафика устройства и вычисляет пороговое значение T. Пороговое значение T определяется путем простого измерения среднего подобия хэшей, сгенерированных из неопасных потоков трафика. Метки неопасного трафика и вычисленное пороговое значение сохраняются в базе данных для обнаружения аномального трафика.

Авторы продемонстрировали эффективность LSAD для обнаружения пятнадцати различных объемных (то есть направленных на превышение пропускной способности канала) атак и провели сравнение с современной системой машинного обучения и популярными одноклассовыми моделями машинного обучения. Результаты показывают, что LSAD достигает среднего истинно-положительного показателя (*от англ.* True-Positive Rate) выше 97 %, используя только 1 мин трафика Интернета вещей.

В работе [13] представлено исследование поведенческой кластеризации устройств инфраструктуры Интернета вещей. Исследование проводилось на реальной базе данных, которая собирает пакеты LoRaWAN (*аббр. от англ.* Low-power Wide-Area Network – «энергоэффективная сеть дальнего радиуса действия»), полученные сетью, развернутой итальянским оператором. Для того, чтобы найти группы пакетов с аналогичным поведением, использовался алгоритм k-средних. Для надежности результатов кластеризации были совместно рассмотрены два внутренних индекса валидации (WCSS и Davies – Bouldin), которые также помогли в решении проблемы поиска наилучшего значения k для разбиения.

Благодаря проведенному исследованию авторы смогли зафиксировать ключевые особенности поведения системы, которые заключались в том, что на одной стороне есть кластеры, которые собирают пакеты, характеризующиеся нормальным поведением, а с другой стороны, некоторые пакеты имеют довольно плохую производительность в системе (в основном из-за условий радиосвязи). Более того, авторы смогли наблюдать, что некоторые устройства генерируют пакеты, которые всегда назначаются одному и тому же кластеру. Эти устройства находятся в стабильном состоянии. Напротив, у некоторых устройств есть пакеты в нескольких кластерах, что означает, что не все их пакеты ведут себя одинаково. Предложенный подход продемонстрировал свою пригодность также для целей обнаружения аномалий.

Следующая работа [14] представляет новую систему обнаружения аномалий для прикладных систем домашней автоматизации HAWatcher (*аббр. от англ.* Home Automation Watcher – «мониторинг домашней автоматизации»). Предлагается метод интеллектуального анализа данных, который использует разнообразную семантическую информацию для построения гипотетических корреляций (когда корреляция описывает, как состояние одного устройства или события коррелирует с другим), и журналы событий в качестве свидетельства для их проверки. Поскольку корреляции объяснимы в соответствии с семантикой, их можно легко интерпретировать для разрешения конфликтов с интеллектуальными приложениями, которые удобно обновлять в соответствии с изменениями. Затем корреляции используются специальным модулем теневого выполнения для моделирования нормального поведения устройств в виртуальной среде. Смоделированные состояния сравниваются с состояниями в реальном мире посредством контекстной и последовательной проверки, а несоответствия во время сравнения определяются как аномалии. Подход оценивался на четырех реальных испытательных стендах с различными случаями аномалий (всего 62), продемонстрировав низкий уровень ложных обнаружений аномалий (0,04 %).

Исследование, описанное в [15], направлено на получение выгоды от интеграции умных домов в социальную сеть с точки зрения повышения безопасности как отдельного умного дома, так и всей социальной сети. Идентификация устройств в каждом из умных домов основана на мониторинге сетевого трафика и создании профилей умных устройств, присутствующих в сети. Профили состоят из набора функций, которые описывают поведение интеллектуальных устройств в сети, включая период активности устройства и период его спящего режима. На основании этого составляется белый список разрешенных профилей работы устройства и формируется кластер; для проверки наличия профиля в его белом списке использовался алгоритм «случайный лес». Если наблюдаемый профиль отсутствует в белом списке, делается запрос на другие кластеры, образующие социальную сеть, для сравнения профиля последовательности пакетов, полученных в кластере, со своими собственными белыми списками. Для оценки эффективности предложенной системы был проведен ряд экспериментальных исследований. Результаты экспериментов показали общую точность системы на уровне 97,21 % при среднем уровне ошибок первого рода – 5,94 %.

Авторы [16] построили классификатор с использованием машинного обучения без учителя, используя автокодировщики. Предложенная модель учится эффективно восстанавливать входные данные, которые очень похожи на нормальный сетевой трафик, но плохо восстанавливают аномальный или атакующий. Таким образом, ошибку реконструкции обученной модели машинного обучения можно использовать в качестве классификатора, чтобы отличить нормальный сетевой трафик от известного или неизвестного атакующего трафика. Авторы демонстрируют, что такой подход не менее эффективен, чем использование классификатора на основе машины опорных векторов SVM (*аббр. от англ.* Support Vector Machines), при этом он значительно лучше выявляет новые типы атак.

Как только атака обнаружена, одним из способов смягчения последствий является блокирование атакующего трафика в самом источнике с помощью программно определяемых сетей SDN (*аббр. от англ.* Software-Defined Network). Однако идентификация источников атаки может быть сложной задачей, поскольку злоумышленники могут попытаться замаскировать атаку в сетевом трафике. Для обучения классификаторов нормальному поведению сети использовался общедоступный набор данных о безвредном трафике Интернета вещей. Кроме того, чтобы преодолеть препятствие, связанное с отсутствием общедоступных наборов данных для DDoS-атак (*аббр. от англ.* Distributed Denial of Service – «распределенный отказ в обслуживании») в Интернете вещей, авторы создали большую имитационную локальную сеть, состоящую из виртуальных устройств Интернета вещей и промышленных контроллеров, а также программные инструменты и скрипты, которые позволяют запускать атаки различных типов и интенсивности с выбранного набора виртуальных устройств. Авторы обучили и протестировали предложенные модели классификации для обнаружения атак по данным трафика, а также представили подход, основанный на машинном обучении для выявления скомпрометированных источников при подмене IP-адреса.

В работе [17] показано, что можно создать высокоточную модель неконтролируемого обучения

для обнаружения ботнетов Интернета вещей с ограниченным набором функций. Основным вкладом этого исследования является подробный анализ дискриминационных возможностей функций и сравнение эффективности обнаружения одной общей модели с отдельными моделями. Сокращенный набор функций позволяет потреблять меньше вычислительных ресурсов и может привести к более интерпретируемым результатам. Показано, что одна модель, в которой используются классические методы обучения (такие как SVM или Isolation Forest) с менее, чем десятью функциями, может обеспечить приемлемую скорость обнаружения, что предпочтительно с точки зрения масштабируемости. Другой важный вывод заключается в том, что, хотя одна общая модель обучения для всех устройств Интернета вещей может достичь разумных показателей обнаружения, создание отдельной модели для каждого устройства дает более высокие показатели обнаружения.

В представленных подходах, кроме работы [14], использующей корреляционный анализ для обнаружения аномалий, применяются методы машинного обучения с учителем и без учителя и кластеризация. При этом не используется возможность обнаружения выбросов в данных и построения значений для нормального поведения трафика на основе статистических методов. К преимуществам последних относится простота в использовании, скорость вычислений и возможность работы с неразмеченными данными, а также возможность получать результаты даже в тех случаях, когда неизвестна аналитическая связь между различными параметрами трафика. В данном исследовании предлагается использовать эти преимущества в рамках разрабатываемого подхода к обнаружению аномалий в трафике устройств Интернета вещей.

Обнаружение аномалий в трафике

Разработанный автором подход предполагает, что исходные данные, описывающие трафик устройств Интернета вещей внутри сети, содержатся в журналах, разделенных по дням активности. Обычно каждая строка такого журнала описывает сообщение, полученное от определенного устройства. И может включать следующую информацию: время активности, различные атрибуты текущего пользователя и текущего устройства, сетевые подключения, информацию о приложении, информацию о возможных ошибках подключения и авторизации и т. д.

Предлагаемый подход включает 3 основных этапа: извлечения признаков, оценки нормального поведения и обнаружения аномалий. На этапе извлечения признаков формируются их векторы для данного устройства или пользователя на основе агрегирования шкалы времени. На этапе оценки поведения вычисляется нормальный диапазон для различных значений признаков для всех устройств или пользователей. Этап обнаружения аномалий отвечает за проверку активности пользователя или устройства и ищет значительные отклонения, известные как аномалии.

Для реализации каждого этапа была разработана соответствующая методика. Выходными данными методики извлечения признаков являются признаки устройств, созданные на основе агрегированного по времени количества сообщений из различных столбцов журнала, сохраненные в словаре. Входными данными методики извлечения признаков являются журналы, описывающие трафик устройств в сети.

Функциональность методики извлечения признаков позволяет загружать журналы трафика устройств, объединять несколько журналов в один, фильтровать активные устройства, создавать и сохранять признаки устройств. Методика предназначена для извлечения сущностей, описывающих ключевые характеристики поведения устройств, для оценки нормального и аномального поведения устройств. Для этого был проведен ряд экспериментов. Направление экспериментов в первую очередь связано с поиском аномальной активности устройств, поскольку их необычное поведение может указывать на мошенническую деятельность и в меньшей степени влиять на человеческий фактор. Рассматриваются только активные устройства, которые имеют как минимум несколько сообщений (5–10), порог фильтрации для общего количества сообщений определяется как входной параметр. Затем для целевых устройств создается несколько признаков (их имена также определяются как входной параметр) на основе агрегированного по времени количества сообщений из определенных столбцов исходных журналов. Эти признаки представляют ключевые характеристики поведения устройства и могут указывать на наличие аномальной активности. Размер временного окна для агрегирования определяется как входной параметр. Его значение зависит от свойств случайного процесса, т. е. характера активности устройств, и определяет размерность каждого признака. Данный интервал должен обеспечивать возможность отследить некоторые незначительные изменения в активности устройства и в то же время обобщить паттерны его активности. В ходе экспериментов использовалось значение временного окна, равное 60 с, для трафика, который включал в себя сообщения от устройств, поступающих на протяжении нескольких дней.

В зависимости от полей автор выделяет 5 типов признаков:

1) частота сообщений – строятся временные ряды для всех сообщений от уникального устройства

за определенный интервал времени с шагом H с: например, H = 60 с;

2) количество входов – строятся временные ряды для сообщений входа в систему с уникального устройства за определенный интервал времени с шагом H с: например, H = 60 с;

3) количество повторяющихся сообщений – строится временной ряд для сообщений с одинаковыми атрибутами, идущих подряд друг за другом, от уникального устройства за определенный интервал времени с шагом H с: например, H = 60 с;

4) интервалы между сообщениями – строится последовательность значений интервалов времени между подряд идущими сообщениями, полученными от уникального устройства;

5) количество ошибок – строятся временные ряды для сообщений с ошибками устройства от уникального устройства за определенный интервал времени с шагом H с: например, H = 60 с.

Пример общей активности устройства в определенный интервал времени и образец активности для текущего устройства для H = 60 с показаны на рисунке 1.

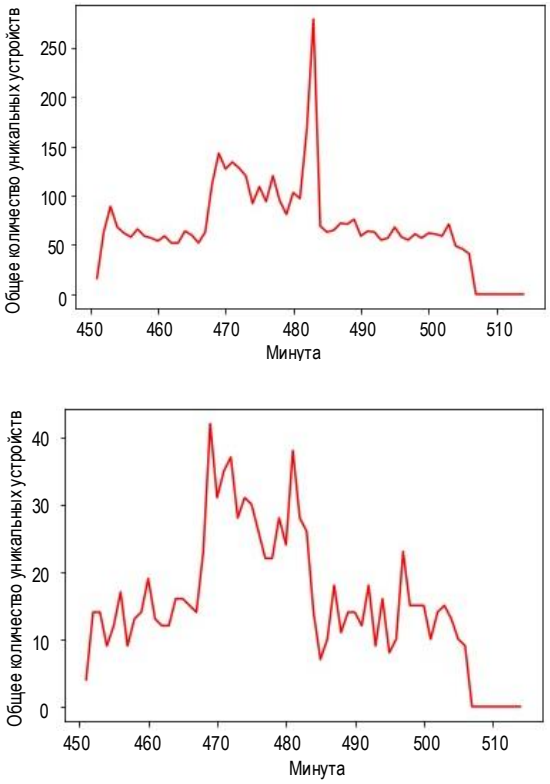

Рис. 1. Примеры паттернов активности устройств

Fig. 1. Examples of Device Activity Patterns

Следующим шагом предложенного подхода является оценка нормальной активности устройств для различных признаков с помощью методики оценки нормального поведения. Ее входными данными является словарь признаков активных устройств, а выходными – границы нормального поведения устройств для каждого признака.

Цель данного этапа – вычислить диапазон нормальных значений для каждого признака каждого устройства. Для этого используются 4 статистических метода оценки: интерквантильный размах (iqr), Grubs-тест, GESD-тест и экспоненциальное сглаживание.

Интерквантильный размах представляет собой разницу между первой ($Q1$) и третьей ($Q3$) квартилями, при его вычислении границы нормального поведения для значения признака f вычисляются согласно формуле:

$$\begin{aligned} \text{iqr} &= Q3(f) - Q1(f); \\ \text{left} &= Q1(f) - \text{scale} * \text{iqr}; \\ \text{right} &= Q3(f) + \text{scale} * \text{iqr}. \end{aligned} \quad (1)$$

где параметр scale = 1,5 может использоваться для поиска незначительных выбросов, не попадающих в пределы внутренних границ набора данных, а scale = 3 используется для поиска значительных выбросов, вышедших за внешние границы.

Критерий Граббса (Grubs-тест) – статистический тест, используемый для определения выбросов. Критерий Граббса определяет один выброс за одну итерацию. Этот выброс исключается из набора данных и тест повторяется до тех пор, пока не будут обнаружены все выбросы. Он рассчитывается на основе среднего и среднеквадратичного отклонения наблюдаемых значений:

$$G = \frac{\max |Y_i - \bar{Y}|}{s}, \quad (2)$$

где s – среднеквадратическое отклонение.

Критерий Граббса определяется для гипотез: в наборе данных нет выбросов (основной) и в наборе данных присутствует как минимум один выброс (альтернативной).

GESD (*аббр. от англ.* Generalized Extreme Studentized Deviate Test) – тест используется для обнаружения одного или нескольких выбросов в одномерном наборе данных. Он проверяет нулевую гипотезу «В данных нет выбросов» против конкурирующих «В данных есть i выбросов», $i = 1, .., n$. Тестовая статистика рассчитывается в виде:

$$\begin{aligned} \alpha_i &= \frac{(n-i)t_{p,n-t-1}}{\sqrt{(n-i+t^2_{p,n-t-1})}};\ i = 1, 2, .., r; \\ p &= 1 - \frac{\alpha}{2(n-i+1)}, \end{aligned} \quad (3)$$

где n – размер вектора признаков; $t_{p,v}$ – 100p-процентная точка t-распределения с ν степенями свободы.

После поиска и исключения выбросов из набора данных с помощью двух описанных выше статистических тестов диапазон нормальных значений наблюдаемого признака определяется, исходя из

значений минимального и максимального элемента в полученном наборе данных.

Экспоненциальное сглаживание – это практический метод выравнивания временных рядов с использованием экспоненциальной оконной функции. В то время как в простом скользящем среднем прошлые наблюдения имеют одинаковый вес, экспоненциальные функции используются для назначения экспоненциально убывающих весов с течением времени. Последовательность необработанных данных $\{x_i\}$ начинается с момента времени $t = 0$, а результат алгоритма экспоненциального сглаживания обычно записывается как $\{s_t\}$. Процесс экспоненциального сглаживания может быть описан следующим образом:

$$s_0 = x_0; \quad s_t = \alpha x_t + (1 - \alpha) s_{t-1}, \; t > 0, \qquad (4)$$

где $0 < \alpha < 1$ – параметр сглаживания.

Для расчета границ нормального поведения на основе экспоненциального сглаживания используют нормированную разницу между исходным и восстановленным временным рядом, а также ее среднее и среднеквадратичное отклонение, на основе которых вычисляется доверительный интервал:

$$d = |x - s|; d_{scaled} = \frac{d - d_{min}}{d_{max} - d_{min}}; \qquad (5)$$
$$left = \overline{d_{scaled}} - t_{\alpha/2} s,$$

где $t_{\alpha/2}$ – уровень построения доверительного интервала (используется значение 1,96: доверительный интервал – 95 %).

Устройства, имеющие недостаточные показатели активности (всего несколько сообщений), могут быть отфильтрованы с помощью порога, заранее заданного вручную, затем выполняется вычисление границ с указанной последовательностью методов, по умолчанию вначале используется GESD-метод, затем тест Граббса, затем интерквантильный размах, затем экспоненциальное сглаживание. На протестированных журналах GESD-метод показывает наилучшие результаты, соответственно для каждого метода были получены 113, 6, 3 и 53 устройства с ненулевыми границами нормальной активности для исходных данных. Исходя из результатов применения GESD-метода, вычисляются границы только для оставшихся устройств для каждого следующего метода. Это также сокращает время вычислений и дает возможность использовать различные методы для оценки нормального поведения одновременно, что позволяет определить границы нормального поведения для большего количества устройств.

После определения нормальных диапазонов признаков методика проверяет информацию о ранее рассчитанном диапазоне и по возможности использует их (объединяя со значениями в словаре границ нормального поведения). Если для анализируемого устройства нет информации о ранее рассчитанном диапазоне нормальных значений или имеются неопределенные или нулевые нормальные значения признаков, то эта информация сохраняется и соответствующие значения обновляются.

Заключительный этап предложенного подхода представляет собой обнаружение аномалий с помощью методики обнаружения аномалий. В качестве входных данных для обнаружения аномалий используются нормальные значения признаков и характеристики устройства. Выходными данными методики обнаружения аномалий являются: их количество для каждого признака каждого устройства, атрибуты времени начала для аномалий, некоторые статистики устройства на основе его аномальных временных атрибутов.

Процесс обнаружения аномалии состоит из следующих шагов.

Шаг 1. Обнаружение аномалии в значениях каждого признака для каждого устройства. Данный шаг реализуется путем сравнения значений каждого признака для каждого устройства с диапазонами нормальных значений.

Шаг 2. Определение атрибутов аномалий, таких как идентификатор устройства, название признака, интенсивность аномалии и время аномалии. Интенсивность аномалии определяется как отношение расстояния между значением признака и ближайшей границей диапазона к значению признака, в случае, когда значение признака равно нулю, интенсивность равна отношению целевого расстояния к расстоянию между правой и левой границами нормального диапазона. Время аномалии определяет временной интервал аномальной активности, продолжительность которого определяется параметром H, рассматривается только время начала аномалии.

Шаг 3. Фильтрация аномалий. Аномалии фильтруются по порогам интенсивности, указанным для каждого признака в заранее определенном параметре, который представляет собой последовательность весов интенсивностей для каждого признака. Это необходимо для того, чтобы была возможность исключить из рассмотрения незначительные отклонения от нормального поведения, не представляющие интереса. Данные веса задаются вручную и позволяют сократить количество ложно-положительных обнаружений в случаях, когда потенциально аномальные значения отклоняются от нормальных всего на несколько процентов.

Шаг 4. Вычисление итоговых значений. На данном шаге вычисляется количество аномалий для каждого признака каждого устройства, определяются атрибуты времени начала для аномалий и вычисляются следующие статистики устройства на основе его аномальных временных атрибутов, а

именно – количество дней общей активности, аномальной активности и последних последовательных дней нормальной активности. После этого вычисляются веса аномалий на основе отношения интервалов времени аномалии ко всем интервалам активности для всех признаков (или их целевого подмножества) с целью последующего применения для обнаружения атак и анализа рисков информационной безопасности.

Для проведения экспериментов был реализован подход в рамках программного прототипа на языке Python, каждая методика вместе со своими входными и выходными параметрами составляла отдельный модуль, в том числе и методика генерации журналов активности устройств, описанная в следующем разделе.

Генерация журналов активности устройств и оценка предложенного подхода

Для оценки предложенного подхода для обнаружения аномалий в трафике устройств использовался механизм генерации журналов на основе использования распределений исходных атрибутов устройства, таких как временные метки, входы с устройства, сетевые адреса, возникшие ошибки и т. д. В процессе генерации в журнал добавлялись аномалии для каждого из признаков для некоторых случайных устройств с заданной вероятностью, затем итоговая разметка сравнивалась с результатами обнаружения на журнале, полученном в процессе генерации.

На основе входных данных определялось частотное распределение сообщений с устройств и на его основе осуществлялась генерация идентификатора устройства и его профиля, который содержал всевозможные значения атрибутов для данного устройства. На основе этого профиля осуществлялась генерация аномальной активности путем изменения целевых атрибутов устройства с заданной вероятностью, которая затем добавлялась в генерируемый журнал. Оценка на основе корреляций с использованием коэффициента корреляции Спирмена применялась для формирования множества зависимых и независимых атрибутов устройства, зависимые атрибуты (например, версия программного обеспечения, идентификатор пользователя) генерировались на основе их распределений относительно текущего устройства, независимые (например, адреса сетевых шлюзов, IP-адреса) – на основе общего распределения атрибута по журналу, либо на основе других атрибутов. На рисунке 2 представлена общая схема похода к генерации журнала активности устройств.

Ниже перечислены основные шаги для генерации журнала активности устройств.

Шаг 1. Выбираем устройство из общего множества устройств в соответствии с исходным распределением частот входов.

Шаг 2. Определяем и генерируем для устройства время входа на основе выбора исходных временных интервалов с небольшим фиксированным случайным отклонением.

Шаг 3. Определяем для устройства множество его атрибутов, таких как попытки логина, сетевые адреса, ошибки и т. д. Для этого необходимо проверить, какие атрибуты зависят от конкретного устройства.

Шаг 4. Генерируем для устройства необходимые атрибуты.

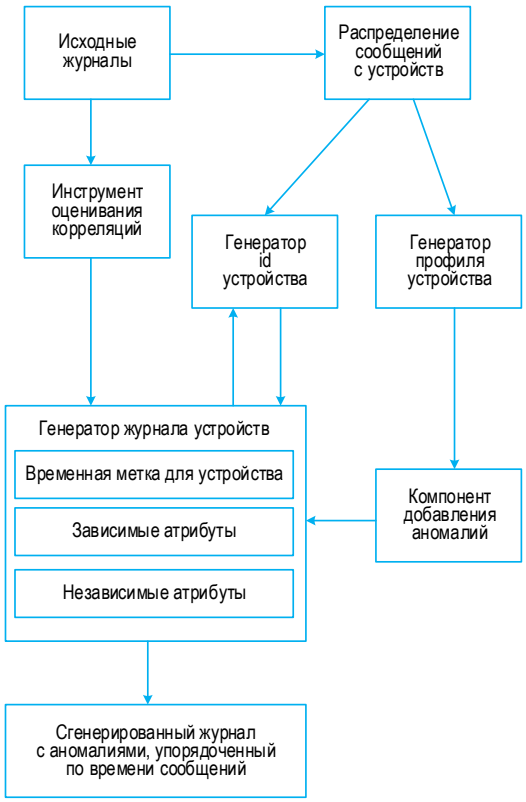

Рис. 2. Общая схема похода к генерации журнала активности устройств

Fig. 2. General Scheme of Approach to Generating a Device Activity Log

Выполняем шаги 1–4 нужное число раз, в зависимости от требуемого количества строк в журнале; в конце – упорядочиваем все по времени.

После генерации в журнал были добавлены аномалии для каждого признака, которые включали:

– нетипичное (большее или меньшее) количество сообщений от устройства;

– нетипичное количество попыток авторизации устройства;

– нетипичное количество подряд идущих сообщений от устройства;

– нетипичные интервалы отклика устройства (промежутки между отдельными сообщениями);

– нетипичное количество ошибок, возникших при соединении с устройством.

После генерации журнала были построены признаки устройств, определены значения, соответ-

ствующие нормальному поведению и обнаружены различные аномалии. Общее количество уникальных устройств в сгенерированном логе составило 4804. Количественная оценка обнаруженных аномалий в сгенерированном журнале приведена в таблице 1. Точность обнаружения аномалий представляет собой отношение количества найденных аномалий к общему количеству аномалий для данного признака.

Таким образом, средняя точность обнаружения аномалий в сгенерированном журнале по всем видам характеристик устройств составила 79 %. Лучше всего обнаруживаются аномалии, связанные с изменением временных интервалов между сообщениями от устройства, хуже всего – аномалии, связанные с количеством повторяющихся сообщений. Это может быть связано с незначительным изменением частоты сообщений при генерации, которое могло попасть в рамки диапазона нормальных значений. Возможно, требуется более чувствительная настройка методов определения границ нормального поведения конкретно для данной характеристики.

ТАБЛИЦА 1. Количественная оценка обнаруженных аномалий в сгенерированном журнале

TABLE 1. Quantification of Detected Anomalies in the Generated Log

Признак	Количество аномалий		Из них:			Точность
	в сгенерированном логе	обнаруженных	истинно-положительные	ложно-отрицательные	ложно-положительные	
Частота сообщений	82	73	68	9	5	83 %
Количество входов	31	45	25	1	19	80 %
Количество повторяющихся сообщений	41	29	25	12	3	61 %
Интервалы между сообщениями	81	86	72	7	7	89 %
Количество ошибок	47	40	34	9	4	72 %
Общее количество	282	273	224	38	38	79 %

Заключение

В данной работе предложен подход к обнаружению аномалий в трафике устройств Интернета вещей, основанный на построении численных характеристик профилей устройств, определении их нормальных значений и поиску отклонений от нормы на основе статистических методов, а именно интерквантильного размаха, Grubs-теста, GESD-теста и экспоненциального сглаживания. Описаны методики анализа трафика устройств Интернета вещей, входящие в разработанный подход, предложенные признаки выявления аномалий, механизм генерации журналов событий для устройств, а также численная оценка обнаруженных аномалий в сгенерированном журнале с помощью предложенного подхода. Эксперименты показали, что в сгенерированном журнале средняя точность обнаружения аномалий по всем признакам составила 79 %, лучшие результаты в 89 % были получены для признака, измеряющего частоту сообщений, полученных от устройства. В данном исследовании использовались различные статистические методы для обнаружения аномалий в трафике устройств Интернета вещей, которые имеют такие преимущества, как гибкость, универсальность, скорость вычислений и возможность работы с неразмеченными данными. К недостаткам предложенного подхода можно отнести отсутствие оценки предложенных методик, на основе размеченных данных с аномалиями.

Дальнейшие улучшения предложенного подхода связаны с анализом большего количества признаков и сравнении эффективности предложенных методов с методами, основанными на использовании машинного обучения.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа подготовлена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Список используемых источников

1. Tariqa N., Khan F.A., Asimc M. Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis // Procedia Computer Science. 2021. Vol. 191. PP. 425–430. DOI:10.1016/j.procs.2021.07.053
2. Sengupta J., Ruj S., Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT // Journal of Network and Computer Applications. 2019. Vol. 149. DOI:10.1016/j.jnca.2019.102481
3. Котенко И.В., Степашкин М.В., Богданов В.С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
4. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3(39). С. 68–75.
5. Enoch S.Y., Ge M., Hong J.B., Kim D.S. Model-based Cybersecurity Analysis: Past Work and Future Directions. Cornell University, 2021. URL: https://arxiv.org/abs/2105.08459 (дата обращения 21.12.2021)
6. Torres N., Pinto P., Lopes S.I. Security Vulnerabilities in LPWANs – An Attack Vector Analysis for the IoT Ecosystem // Applied Sciences. 2021. Vol. 11. Iss. 7. DOI:10.3390/app11073176
7. Alansari Z., Anuar N.B., Kamsin A., Belgaum M.R., Alshaer J., Soomro S., et al. Internet of Things: Infrastructure, Architecture, Security and Privacy // Proceedings of the International Conference on Computing, Electronics & Communications Engineering (iCCECE, Southend, UK, 6–17 August 2018). IEEE, 2018. DOI:10.1109/iCCECOME.2018.8658516
8. Hamza A., Gharakheili H.H., Sivaraman V. IoT Network Security: Requirements, Threats, and Countermeasures. Cornell University, 2020. URL: https://arxiv.org/abs/2008.09339 (дата обращения 21.12.2021)
9. Bouazza H., Zohra L.F., Said B. Integration of Internet of Things and Social Network: Social IoT General Review // Proceedings of the First International Conference on Computing (ICC 2019, Riyadh, Saudi Arabia, 10–12 December 2019) on Advances in Data Science, Cyber Security and IT Applications. Communications in Computer and Information Science. Vol. 1098. Cham: Springer, 2019. PP. 312–324. DOI:10.1007/978-3-030-36368-0_26
10. Ali O., Ishak M.K., Bhatti M.K.L. Emerging IoT domains, current standings and open research challenges: a review // PeerJ Computer Science. 2021. DOI:10.7717/peerj-cs.659
11. Nguyen-An H., Silverston T., Yamazaki T., Miyoshi T. IoT Traffic: Modeling and Measurement Experiments // IoT. 2021. Vol 2(1). PP. 140–162. DOI:10.3390/iot2010008
12. Charyyev B., Gunes M.H. Detecting Anomalous IoT Traffic Flow with Locality Sensitive Hashes // Proceedings of the Global Communications Conference (GLOBECOM, Taipei, Taiwan, 7–11 December 2020). IEEE, 2020. DOI:10.1109/GLOBECOM42002.2020.9322559
13. Garlisi D., Martino A., Zouwayhed J., Pourrahim J., Cuomo F. Exploratory approach for network behavior clustering in LoRaWAN // Journal of Ambient Intelligence and Humanized Computing. 2021. DOI:10.1007/s12652-021-03121-z
14. Fu C., Zeng Q., Du X. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes // Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, 2021. PP. 4223–4240. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong (дата обращения 21.12.2021)
15. Nicheporuk A., Nicheporuk A., Sachenko A., Sachenko O., Kazantsev A. A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication // Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS (IntelITSIS, 2021, Khmelnytskyi, Ukraine, 24–26 March 2021). URL: http://ceur-ws.org/Vol-2853/paper44.pdf (дата обращения 21.12.2021)
16. Bhatia R., Benno S., Esteban J., Lakshman T.V., Grogan J. Unsupervised machine learning for network-centric anomaly detection in IoT // Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19). New York: Association for Computing Machinery, 2019. PP. 42–28. doi:10.1145/3359992.3366641
17. Nõmm S., Bahşi H. Unsupervised Anomaly Based Botnet Detection in IoT Networks // Proceedings of the 17th International Conference on Machine Learning and Applications (ICMLA, Orlando, USA, 17–20 December 2018). IEEE, 2018. DOI:10.1109/ICMLA.2018.00171

* * *

Detection of IoT Device Traffic Anomalies

I. Murenin[1]*

[1]Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
St. Petersburg, 199178, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-4-128-137
Received 6th December 2021
Revised 20th December 2021
Accepted 21th December 2021

For citation: Murenin I. Detection of Anomalies in the Traffic of IoT Devices. *Proc. of Telecom. Universities.* 2021;7(4): 128–137. (in Russ.) DOI:10.31854/ 1813-324X-2021-7-4-128-137

Abstract: *The article proposes an approach to finding anomalies in the traffic of IoT devices based on time series analysis and assessing normal and abnormal behavior using statistical methods. The main goal of the proposed approach is to combine statistical methods for detecting anomalies using unlabeled data and plotting key characteristics of device profiles. Within this approach the following techniques for traffic analysis has been developed and implemented: a technique for a feature extraction, a normal behavior boundary building technique and an anomaly detection technique. To evaluate the proposed approach, we used a technique for generating event logs from devices with the generation of anomalous markup. The experiments shown that the GESD-test gives the best results for anomaly detection in IoT traffic.*

Keywords: *anomaly detection, time series analysis, IoT, network traffic, statistical methods.*

References

1. Tariqa N., Khan F.A., Asimc M. Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis. *Procedia Computer Science*. 2021;191:425–430. DOI:10.1016/j.procs.2021.07.053
2. Sengupta J., Ruj S., Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*. 2019;149. DOI:10.1016/j.jnca.2019.102481
3. Kotenko I.V., Stepashkin M.V., Bogdanov V.S. Architectures and Models of Active Vulnerabilities Analysis Based on Simulation of Malefactors' Actions. *Information Security Problems. Computer Systems*. 2006;2:7–24 (in Russ.)
4. Kotenko I.V., Desnitskiy V.A., Chechulin A.A. Research of technology for designing safe embedded systems in the project of the European Community SecFutur. *Zaŝita informacii. Inside*. 2011;3(39):68–75.
5. Enoch S.Y., Ge M., Hong J.B., Kim D.S. *Model-based Cybersecurity Analysis: Past Work and Future Directions*. Cornell University; 2021. Available from: https://arxiv.org/abs/2105.08459 [Accessed 21th December 2021]
6. Torres N., Pinto P., Lopes S.I. Security Vulnerabilities in LPWANs – An Attack Vector Analysis for the IoT Ecosystem. *Applied Sciences*. 2021;11(7). DOI:10.3390/app11073176
7. Alansari Z., Anuar N.B., Kamsin A., Belgaum M.R., Alshaer J., Soomro S., et al. Internet of Things: Infrastructure, Architecture, Security and Privacy. *Proceedings of the International Conference on Computing, Electronics & Communications Engineering, iCCECE, 6–17 August 2018, Southend, UK*. IEEE; 2018. DOI:10.1109/iCCECOME.2018.8658516
8. Hamza A., Gharakheili H.H., Sivaraman V. *IoT Network Security: Requirements, Threats, and Countermeasures*. Cornell University, 2020. Available from: https://arxiv.org/abs/2008.09339 [Accessed 21th December 2021]
9. Bouazza H., Zohra L.F., Said B. Integration of Internet of Things and Social Network: Social IoT General Review. *Proceedings of the First International Conference on Computing, ICC 2019, 10–12 December 2019, Riyadh, Saudi Arabia on Advances in Data Science, Cyber Security and IT Applications. Communications in Computer and Information Science*. Cham: Springer; 2019. vol.1098. p.312–324. DOI:10.1007/978-3-030-36368-0_26
10. Ali O., Ishak M.K., Bhatti M.K.L. Emerging IoT domains, current standings and open research challenges: a review. *PeerJ Computer Science*. 2021. DOI:10.7717/peerj-cs.659
11. Nguyen-An H., Silverston T., Yamazaki T., Miyoshi T. IoT Traffic: Modeling and Measurement Experiments. *IoT*. 2021;2(1):140–162. DOI:10.3390/iot2010008
12. Charyyev B., Gunes M.H. Detecting Anomalous IoT Traffic Flow with Locality Sensitive Hashes. *Proceedings of the Global Communications Conference, GLOBECOM, 7–11 December 2020, Taipei, Taiwan*. IEEE; 2020. DOI:10.1109/GLOBECOM 42002.2020.9322559
13. Garlisi D., Martino A., Zouwayhed J., Pourrahim J., Cuomo F. Exploratory approach for network behavior clustering in LoRaWAN. *Journal of Ambient Intelligence and Humanized Computing*. 2021. DOI:10.1007/s12652-021-03121-z
14. Fu C., Zeng Q., Du X. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes. *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association; 2021. p.4223–4240. Available from: https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong [Accessed 21th December 2021]
15. Nicheporuk A., Nicheporuk A., Sachenko A., Sachenko O., Kazantsev A. A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication. *Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, IntelITSIS, 2021, 24–26 March 2021, Khmelnytskyi, Ukraine*. Available from: http://ceur-ws.org/Vol-2853/paper44.pdf [Accessed 21th December 2021]
16. Bhatia R., Benno S., Esteban J., Lakshman T.V., Grogan J. Unsupervised machine learning for network-centric anomaly detection in IoT // Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19). New York: Association for Computing Machinery, 2019. PP. 42–28. doi:10.1145/3359992.3366641
17. Nõmm S., Bahşi H. Unsupervised Anomaly Based Botnet Detection in IoT Networks // Proceedings of the 17th International Conference on Machine Learning and Applications, ICMLA, 17–20 December 2018, Orlando, USA. IEEE, 2018. DOI:10.1109/ICMLA.2018.00171

Сведения об авторе:

МУРЕНИН Иван Николаевич | младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, imurenin@gmail.com
https://orcid.org/0000-0002-2263-2426