ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2019 Том 7 № 3 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2019 Vol. 7 Iss. 3 ISSN 2307-1303 http://www.itt.sut.ru

ОБНАРУЖЕНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ УСТРОЙСТВА IOT В СЕТИ НА ОСНОВЕ МОДЕЛИ ТРАФИКА

Д. В. Сахаров*, Д. С. Козлов

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: d.sakharov@rkn.gov.ru

Аннотация
В статье рассматривается протокол CoAP, регламентирующий передачу и прием информационного трафика оконечными устройствами в сетях IoT. Приводится описание модели для выявления аномального трафика в сетях 5G/IoT при помощи алгоритмов машинного обучения, а также основные методы обнаружения аномалий. Актуальность темы статьи обусловлена широким распространением Интернета вещей и грядущего обновления мобильных сетей до поколения 5G.

Ключевые слова
5G-сети, протокол CoAP, Интернет вещей, IDS/IPS, машинное обучение.

Информация о статье
УДК 004.056.53
Язык статьи – русский.
Поступила в редакцию 18.03.2019, принята к печати 30.12.19.

Ссылка для цитирования: Сахаров Д. В., Козлов Д. С. Обнаружение аномального поведения устройства IoT в сети на основе модели трафика // Информационные технологии и телекоммуникации. 2019. Том 7. № 3. С. 50–55. DOI 10.31854/2307-1303-2019-7-3-50-55.

DETECTING ABNORMAL BEHAVIOR OF AN IOT DEVICE IN THE NETWORK BASED ON A TRAFFIC MODEL

D. Saharov*, D. Kozlov

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

*Corresponding author: d.sakharov@rkn.gov.ru

Abstract—The article deals with the CoAP Protocol that regulates the transmission and reception of information traffic by terminal devices in IoT networks. The article describes a model for detecting abnormal traffic in 5G/IoT networks using machine learning algorithms, as well as the main methods for solving this problem. The relevance of the article is due to the wide spread of the Internet of things and the upcoming update of mobile networks to the 5g generation.

Keywords—5G networks, CoAP protocol, Internet of things, IDS/IPS, machine learning.

Article info
Article in Russian.
Received 18.03.2019, accepted 30.12.19.

For citation: Saharov D., Kozlov D.: Detecting Abnormal Behavior of an IoT Device in the Network Based on a Traffic Model // Telecom IT. 2019. Vol. 7. Iss. 3. pp. 50–55 (in Russian). DOI 10.31854/2307-1303-2019-7-3-50-55.

В последние годы Интернет вещей (IoT) превратил объекты повседневной жизни в коммуникационные устройства. Число подключенных устройств к 2021 году составит от 10 до 12 миллиардов. Будущие инфраструктуры должны поддерживать существующие сетевые архитектуры и соответствовать потребностям IoT [1]. Исследователи и специалисты в области кибербезопасности разработали ряд защитных систем для защиты организаций от угроз, таких как вирусы, трояны, черви и ботнеты. Существующие решения, основанные на системах обнаружения вторжений (IDS), включают в себя активные подходы для предупреждения и устранения уязвимостей в системе. Однако эти подходы должны адаптироваться и развиваться в направлении новых технологий и коммуникационных сетей, таких как 5G и IoT. Одним из подходов решения данной проблемы может быть применение машинного обучения для анализа проходящего трафика.

В IoT для передачи данных используется протокол CoAP. Он предназначен для взаимодействия с простыми устройствами. Они обычно имеют ограниченный энергоресурс, небольшой объем памяти и невысокую мощность, поэтому самая главная особенность при работе с ними является обеспечение низких энергозатрат. В качестве примеров таких устройств могут выступать датчики малой мощности, выключатели и клапаны. CoAP разрабатывался по образу и подобию протокола HTTP, но отличается от него тем, что CoAP – это бинарный протокол,

который работает поверх UDP, что значительно уменьшает общий размер передаваемых данных и повышает гибкость взаимодействия. Также он обладает теми же основными типами запросов, что и HTTP: GET, PUT, POST и DELETE.

Схема работы протокола CoAP представлен на рис. 1. В данном сценарии рассматривается ситуация, когда. в большом помещении расположены несколько датчиков CoAP, которые осуществляют измерение температуры. Управлять этими датчиками можно посредством HTTP-клиента, который подключается к серверу. Подразумевается, что сервер не поддерживает протокол CoAP, и в этом случае пакеты с датчиков должны передаваться через CoAP-прокси, который и осуществляет конвертацию CoAP-пакетов в HTTP-пакеты. Также возможен сценарий, когда датчики подключаются непосредственно к серверу и он в свою очередь осуществляет преобразование пакеты в другой формат [2].

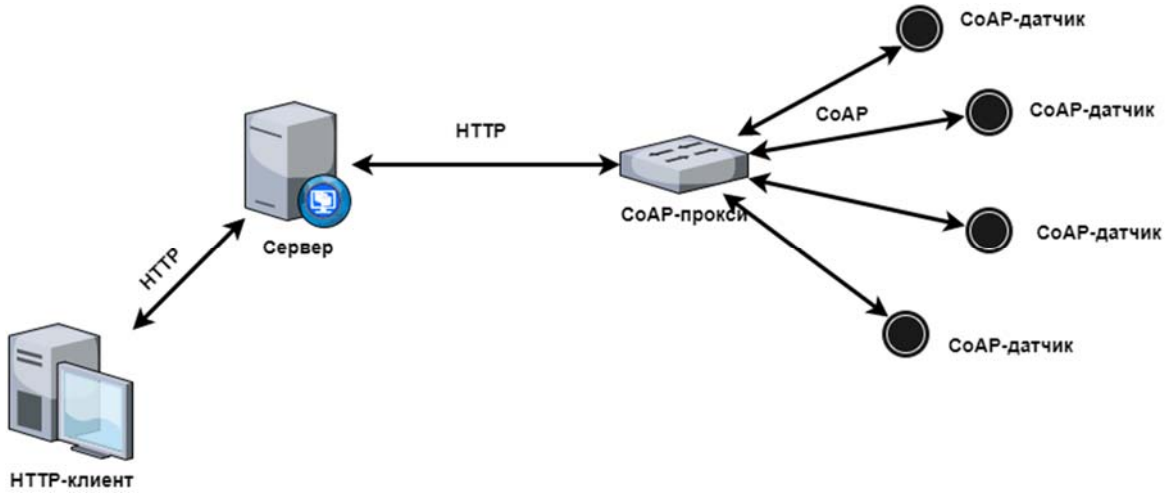

Рис. 1. Схема работы протокола CoAP через прокси

Тема безопасности для «Интернета вещей» является особенно актуальной. В CoAP поддерживается шифрование, но без TCP, так как стандартный TLS (*Transport Layer Security*) не может быть использован для обеспечения безопасности связи. По этой причине в CoAP используется DTLS (*Datagram Transport Layer Security*), который позволяет приложениям, основанным на коммуникациях посредством датаграмм, обмениваться данными безопасным способом, предотвращающим перехват, прослушивание, вмешательство, не нарушая защиты целостности данных или подделку содержимого сообщения.

Для анализа трафика принято использовать модель, которая отражает его предполагаемые особенности. Обычно модель состоит из трех компонент:

- Тренд – общее поведение ряда в плане возрастания или убывания значений.
- Сезонность – периодичные колебания значений, связанные, например, с днем недели или месяца.
- Случайное значение – результат, оставшийся после исключения из ряда других компонент. Именно здесь необходимо осуществлять поиск аномалий.

В первую очередь после выбора модели необходимо приступить к разложению ее на компоненты. Затем выделить тренд, сгладив исходные данные (скользящее окно, экспоненциальное сглаживание, регрессия). Для определения сезонной составляющей из исходных данных следует вычесть тренд или разделить

на него, в зависимости от типа выбранной модели. В свою очередь усредненный сезон определяется путем деления полученного результата на конкретный период (например, неделю). Затем путем удаления из исходного ряда тренда и сезонного фактора Удалив из исходного ряда тренд и сезонный фактор можно получить искомую случайную компоненту. В качестве примеров аномалий могут выступать выброс, сдвиг, изменение характера (распределения) значений, отклонение от «повседневного» и совместные аномалии.

Ниже рассмотрен обзор того, как с помощью методов машинного обучения можно усовершенствовать анализ аномального трафика. Пример архитектуры такого подхода представлен на рис. 2.

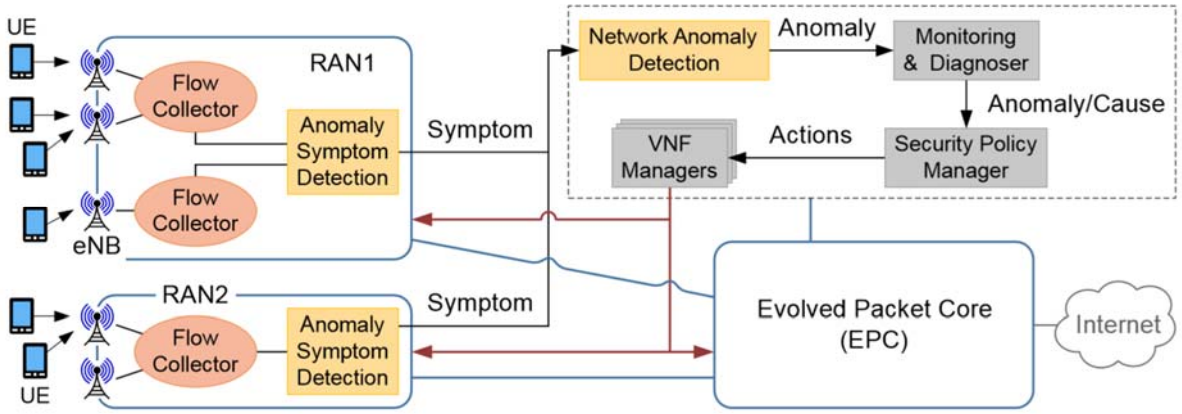

Рис. 2. Пример архитектуры, направленной на обнаружения аномального трафика

Данная архитектура состоит из 2-х основных виртуализированных компонент: обнаружение симптомов аномалий (ASD) и обнаружения сетевых аномалий (NAD). Первый расположен в инфраструктуре сети радиодоступа (RAN), и ориентирован на быстрый поиск симптома аномалии, то есть любого следа или признака аномалии в сетевом трафике, генерируемом оборудованием пользователя, подключенного к RAN. С другой стороны, NAD собирает временные метки и симптомы, а затем центральный процесс осуществляет анализ этих данных и пытается выявить закономерности, которые можно отнести к аномальному (вредоносному) трафику. Как только аномалия будет обнаружена, сообщение об инциденте немедленно отправляется к модулю контроля и диагностирования.

Данный подход очень гибок, поскольку позволяет динамически развертывать новые виртуализированные ресурсы для обнаружения симптомов аномалий в конкретном RAN при увеличении сетевого трафика; а также расширяем, поскольку обнаружение симптомов, которое является самым дорогостоящим процессом анализа, распределено между RAN, в то время как обнаружение аномалий централизовано в основной сети, известной как Evolved Packet Core (EPC), которой необходимы только симптомы в качестве входных данных.

В рассматриваемой архитектуре обнаружение аномалий организовано на двух уровнях. На нижнем уровне коллектор потока получает все различные потоки в течение заданного периода времени, вычисляет вектор признаков, которые модуль ASD классифицирует как аномальные или нормальные. Эта первоначальная классификация должна быть сделана как можно быстрее, даже если

приходится жертвовать точностью для более низкого времени отклика. При подозрении на аномалию пакет симптомов, состоящий из вектора признаков, метки времени и типа обнаруженной аномалии, отправляется на следующий уровень, модуль NAD. NAD получает несколько потоков симптомов от всех ASDs, сортирует их по меткам времени и собирает временную последовательность симптомов.

При таком подходе необходимо учитывать, что каждый RAN должен поддерживать огромное количество трафика, именно поэтому крайне важна возможность обрабатывать достаточное количество потоков в секунду, даже если обнаружение не столь точно, как это могло бы быть. Учитывая все выше описанное необходимо, чтобы выбранный метод машинного обучения отвечал следующим требованиям [3]:

- должен быть пригоден для эффективного выполнения на графическом процессоре;
- должен быть вычислен за конечное число шагов для заданного размера вектора признаков;
- должен иметь одинаковые требования к памяти независимо от количества выборок, используемых в обучении;
- должен достигать хорошей точности в классификации, но при этом его точность не должна резко ухудшаться при работе с реальным трафиком.

В завершение рассматриваются основополагающие методы к обнаружению аномалий в трафике с использованием машинного обучения. Они могут работать в одном из следующих трех режимов:

- обнаружение с учителем: доступен обучающий набор с трафиком, помеченным как нормальный или аномальный;
- частично-контролируемое обнаружение: обучающий набор содержит только обычный трафик, и все, что не относится к этому виду трафика, считается аномальным;
- обнаружение без учителя: нет необходимости в маркированном обучающем наборе [4].

В обнаружении с учителем основной вопрос заключается в том, как построить действительно полный набор обучения со всеми аномальными трафиками, правильно помеченными. Это может быть трудно достичь и труднее поддерживать. В этом случае каждый фрагмент трафика, относящийся к одной из определенных категорий, будет правильно классифицирован, но, если появится новый тип аномалии трафика, он будет классифицирован неправильно.

При частично-контролируемом обнаружении весь алгоритм не привязан к конкретным типам аномального трафика, и может сам определять аномалии нового типа, но обладает меньшей точностью на известной выборке по сравнению с обнаружением с учителем.

Обнаружение же без учителя имеет худшую точность по сравнению с предыдущими подходами, но не требует обучающей выборки [5].

В заключение можно сказать, что большой рост количества устройств, подключаемых к Интернету, а также высокие требования к пропускной способности сетей 5G приводят к новым проблемам информационной безопасности, которые могут быть решены путем усовершенствования средств обнаружения вторжения алгоритмами машинного обучения [6].

Литература

1. Santos J. et al. Fog computing: Enabling the management and orchestration of smart city applications in 5g networks // Entropy. 2018. V. 20. No 1. p. 4.
2. Гойхман В., Савельева А. Аналитический обзор протоколов Интернета вещей // Технологии и средства связи. 2016. № 4. С. 32–37.
3. Maimó L. F. et al. On the performance of a deep learning-based anomaly detection system for 5G networks // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017. pp. 1–8.
4. Дешевых Е. А., Ушаков И. А., Котенко И. В. Обзор средств и платформ обработки больших данных для задач мониторинга информационной безопасности // Информационная безопасность регионов России (ИБРР-2015). 2015. С. 67–67.
5. Донской Д. М., Рябова О. Н., Сахаров Д. В., Виткова Л. А. Некоторые аспекты модели нарушителя информационной безопасности в интернете вещей // Интернет вещей и 5G. 2-я Международная научно-техническая конференция студентов, аспирантов и молодых ученых, Санкт-Петербург, 07 декабря 2016 г. СПб.: СПбГУТ, 2016. С. 47–50.
6. Аникевич Е. А., Виткова Л. А., Сацук Е. Н., Сергеева И. Ю. Предотвращение утечек конфиденциальной информации в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2017. Т. 2. С. 46–51.

References

1. Santos J. et al. Fog computing: Enabling the management and orchestration of smart city applications in 5g networks // Entropy. 2018. V. 20. No 1. p. 4.
2. Goikhman V., Saveleva A. Analytical Review of the Internet of Things Protocols // Communication Technologies & Equipment. 2016. No 4. pp. 32–37.
3. Maimó L. F. et al. On the performance of a deep learning-based anomaly detection system for 5G networks // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017. pp. 1–8.
4. Deshevih E. A., Ushakov I. A., Kotenko I. V. Overview of Big Data Tools and Platforms for Information Security Monitoring // Informatsionnaya bezopasnost regionov Rossii (IBRR-2015). 2015. s. 67–67.
5. Donskoy D. M., Ryabova O. N., Sakharov D. V., Vitkova L. A. Some aspects of the information security intruder model in the Internet of things // INTHITEN 2016. St. Petersburg, 07 December 2016. pp. 47–50.
6. Anikevich E., Vitkova L., Satsuk E., Sergeeva I. Leak Prevention Confidential Data in Information Systems // 6th International Conference on Advanced Infotelecommunications (ICAIT 2020). 2017. V. 2. pp. 46–51.

Сахаров Дмитрий Владимирович – кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, d.sakharov@rkn.gov.ru

Козлов Дмитрий Сергеевич – студент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, dmitriy.kozlov.97@mail.ru

Sakharov Dmitry – Candidate of Engineering Sciences, Associate Professor, SUT, St. Petersburg, 193232, Russian Federation, d.sakharov@rkn.gov.ru

Kozlov Dmitry – Student, SUT, St. Petersburg, 193232, Russian Federation, dmitriy.kozlov.97@mail.ru