УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2020 Том 20 № 2 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2020 Vol. 20 No 2 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004.054 doi: 10.17586/2226-1494-2020-20-2-223-232

АНАЛИЗ ПРОТОКОЛА MQTT НА АТАКИ «ОТКАЗ В ОБСЛУЖИВАНИИ»

Д.И. Дикий

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: dimandikiy@mail.ru

Информация о статье
Поступила в редакцию 09.01.20, принята к печати 25.02.20
Язык статьи — русский

Ссылка для цитирования: Дикий Д.И. Анализ протокола MQTT на атаки «отказ в обслуживании» // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 2. С. 223–232 doi: 10.17586/2226-1494-2020-20-2-223-232

Аннотация
Исследованы атаки «отказ в обслуживании» при эксплуатации сетей «Интернет вещей» с протоколом MQTT. Протокол предназначен для многоадресной рассылки данных, в том числе телеметрии, поэтому потенциально может быть использован для атак вида «отказ в обслуживании». Представлен обзор исследований по данной проблематике. В отличие от существующих подходов проверена гипотеза о возможности использования для атак не только publish-сообщений, но и сообщений вида connect и subscribe. Проведен анализ влияния обработки множества сообщений на производительность системы. Представлена экспериментальная установка на платформе Raspberry Pi 3 и брокера Moquette. Показано, что сеть «Интернет вещей» в рассмотренной конфигурации подвержена атакам «отказ в обслуживании». Наиболее вероятными сценариями действий потенциального злоумышленника являются: создание большого потока запросов на подключение и на подписку; генерация большого потока сообщений publish при большом количестве получателей. Подобные варианты развития событий являются опасными с точки зрения информационной безопасности и повышают вероятность таких угроз как отсутствие доступа к информации и нарушение порядка передачи сообщений. Традиционно атаки подобного характера относят к виду «отказ в обслуживании». Показано, что актуальной задачей является разработка методов и средств защиты от этого вида атак при использовании сетей «Интернет вещей» с протоколом MQTT в качестве основного прокола передачи данных.

Ключевые слова
интернет вещей, протокол MQTT, отказ в обслуживании, тестирование, сетевые атаки, безопасность

Благодарности
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90051.

doi: 10.17586/2226-1494-2020-20-2-223–232

DENIAL-OF-SERVICE ATTACK ANALYSIS BY MQTT PROTOCOL

D.I. Dikii

ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: dimandikiy@mail.ru

Article info
Received 09.01.20, accepted 25.02.20
Article in Russian

For citation: Dikii D.I. Denial-of-service attack analysis by MQTT protocol. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 2, pp. 223–232 (in Russian). doi: 10.17586/2226-1494-2020-20-2-223-232

Abstract
The paper deals with denial-of-service attacks on the Internet of things networks with the MQTT Protocol. This Protocol is intended for data multicasting, including telemetry, that is why it can be potentially used for denial-of-service attacks. A review of studies already carried out on this issue is presented. In contrast to other approaches, the author has tested a hypothesis about potential application of not only publish messages for attacks, but also other types of messages, such as connect and subscribe. Analysis was carried out for identification of the impact of multiple message processing on system performance. An experimental installation was built on the Raspberry Pi 3 platform and the Moquette broker. The Internet of things network in this configuration is subject to denial-of-service attacks. The most probable scenarios for a potential attacker are: creation of the large stream of connection and subscription requests, and generation of the large stream of publish messages with a wide variety of recipients. These scenarios are dangerous from the information

security point of view and increase the likelihood of the following threats: lack of access to information and message transmission disorder. Traditionally, attacks of this nature are referred to “denial-of-service” attacks. The author has shown that development of protection methods and techniques against this type of attacks when using the Internet of things networks with the MQTT Protocol as the main data transmission channel is the relevant task.

Keywords
Internet of things, MQTT protocol, denial of service, testing, network attack, security, availability

Acknowledgements
The reported study was funded by the RFBR, project number No. 19-37-90051.

Введение

Одним из информационно-технологических прорывов современности является среда «Интернет вещей»[1]. Ее концепция заключается в использовании множества электронных устройств, например, датчиков и оконечных исполнительных устройств для автоматизации процессов в промышленности и быту. Согласно [1], сделан прогноз, что в 2015 году количество устройств, подключенных к сети Интернет, превысит отметку 25 млрд.

Таким образом, актуальной задачей является анализ безопасности применения данной технологии. В работе [2] предложена классификация угроз для сетей «Интернет вещей» по уровням модели OSI[2]. Соколов М.Н. и др. выделили следующие основные угрозы: несанкционированный доступ, перехват данных, нарушение конфиденциальности, целостности, атаки «человек посередине», DoS-атаки, вирусы, эксплойты, сетевые черви, руткиты, уязвимости программного обеспечения. Уделяется внимание и организационно-техническим аспектам безопасности, таким как совместимость аппаратных платформ оконечных устройств по способности обрабатывать, передавать и хранить данные с помощью протоколов и форматов данных, как представлено в работах [3, 4].

Реализация атак на сети «Интернет вещей» зависит от технологий, используемых для коммуникации устройств. В работе [5] перечислены возможные атаки на физическом уровне, атаки на стек протоколов Zig-Bee и протокол передачи данных Z-Wave. Также уделено внимание протоколам транспортного и более высоких уровней: MQTT, CoAP, XMPP и др. Целями атак на протоколы прикладного уровня могут быть как сами передаваемые данные (утечка информации), так и работоспособность физических устройств.

Исходя из вышеперечисленного, можно сделать предварительный вывод о том, что разнообразие угроз информационной безопасности в среде «Интернет вещей» велико. Зачастую информация, циркулирующая в таких сетях, носит критический[3] характер. В таких системах предлагают использовать методы безопасной коммуникации устройств с усиленной аутентификацией и управлением доступом [6, 7]. Одним из основополагающих методов защиты информации при ее передаче является применение криптографических преобразований с помощью симметричных и ассиметричных алгоритмов шифрования. Особое внимание уделяется сетям «Интернет вещей» как потенциальному источнику атак «отказ в обслуживании». Для этого существует несколько предпосылок: огромное количество устройств в сети, отсутствие постоянного мониторинга их поведения, недостатки в системе защиты информации, например, использование стандартных паролей для доступа к учетной записи администратора и др. Одними из наиболее ярких примеров использования устройств сетей «Интернет вещей» для атак «отказ в обслуживании» являются ботнет[4] сети [8].

Как правило, атаки такого типа основаны на транспортном уровне модели OSI и состоят из двух этапов:

1) сканирование сети на наличие потенциально слабого устройства с последующим подбором данных учетной записи администратора;
2) реализация атаки путем отправки большого количества запросов на устройство жертвы.

В работе [9] рассмотрены три метода проведения атак «отказ в обслуживании» для устройств среды «Интернет вещей». Эксперимент показал, что соединение в процессе проведения атаки между устройствами может быть нарушено. В [10] рассматривались атаки на транспортном уровне для сетей «Интернет вещей», а именно, TCP flood, TCP SYN.

В качестве защитных мер для среды «Интернет вещей» применяются методы, используемые также в других сетях. Это связано с тем, что большинство атак происходит на транспортном уровне по протоколам TCP/UDP [11]. Для выявления ботнет-сетей предлагается использовать методы машинного обучения [12], или статистические методы анализа сетевого трафика [13]. Отдельно стоит выделить атаки, использующие уязвимости в узкоспециализированных протоколах среды «Интернет вещей».

Обзор протокола MQTT

Объектом исследования данной работы является протокол прикладного уровня MQTT[5] v3.1.1 (Message

[1] Ashton K. That ‘Internet of Things’ Thing. RFID Journal. URL: https://www.rfidjournal.com/articles/view?4986 (дата обращения 09.03.2020).

[2] ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. М.: Госстандарт России. 2006.

[3] Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». п. 8 ст. 12.

[4] Официальный сайт Лаборатории Касперского // Что такое ботнет? URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения 02.02.2020).

[5] OASIS Standart MQTT Version 3.1.1 // OASIS. 2014 p. 81. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html (дата обращения 02.02.2020).

Queuing Telemetry Transport). Данный протокол предназначен для межмашинного обмена информацией и построен по принципу «издатель-подписчик». К преимуществам протокола можно отнести высокую плотность полезной информации за счет малого размера служебных заголовков — 2 Б. С точки зрения использования сетей «Интернет вещей» протокол MQTT очень удобен при массовой рассылке информации одновременно большому числу устройств. Так, в клиент-серверной архитектуре сети, чтобы отправить одинаковое сообщение n получателям, необходимо отправить n сообщений. Применяя протокол MQTT, можно сэкономить вычислительные и энергетические затраты в n раз для устройства отправителя за счет того, что шлюз сам ретранслирует сообщения необходимое число раз.

Отдельно стоит отметить поддержку в протоколе MQTT уровней качества передачи (Quality of Service, QoS). Протокол поддерживает три уровня:

— доставка без подтверждения (QoS 0);
— доставка один раз (QoS 1);
— доставка гарантированно только один раз (QoS 2).

Схема обмена сообщениями по протоколу MQTT (рис. 1) состоит из трех элементов:

1) издатель — устройство, которое отправляет сообщения (может быть, как датчиком, так и исполнительным устройством);
2) подписчик — устройство, которое получает и обрабатывает сообщения;
3) шлюз или брокер — устройство, обеспечивающее логистику сообщений от издателей к подписчикам, хранение сообщений при необходимости, а также ответственно за аутентификацию и управление доступом.

В основном критика протокола MQTT сводится к возможности реализации следующих угроз:

— атака «человек посередине» при передаче информации, в том числе для аутентификации, по открытому каналу [14, 15];
— получение несанкционированного доступа к информационным потокам [16, 17];
— атаки «отказ в обслуживании», например, с помощью переполнения очереди буфера на порту [14].

Легкость протокола и возможность массовой рассылки сообщений привлекают злоумышленников для реализации атак «отказ в обслуживании». Протокол MQTT по умолчанию использует порт 1883 для соединения по открытому каналу и порт 8883 для соединения по защищенному каналу (TLS-соединение). На транспортном и сетевом уровне используется TCP/IP. Следовательно, для сети «Интернет вещей», использующей протокол MQTT, свойственны все уязвимости перечисленных протоколов сетевого и транспортного уровней.

Атака «отказ в обслуживании» с помощью протокола MQTT рассмотрена в ряде публикаций. Например, в [18] представлено исследование о влиянии значения QoS передаваемых сообщений на нагрузку шлюза. Согласно результатам, опасность атаки признана высокой.

Работа [19] посвящена широко известным ботнетам Mirai и Bashlite, в которой уделено внимание заключительному этапу атаки, а именно DDoS-атаке. В экспериментальной установке использовалось несколько реальных физических устройств, обменивающихся сообщениями по протоколу MQTT. Авторы сравнивали легальный трафик и трафик во время атаки. На основе полученных данных был извлечен вектор признаков размерностью 115 элементов, и построена модель, способная отличить легитимный трафик от аномального. Здесь анализировались аномалии трафика на транспортном уровне.

Аналогичное исследование представлено в [20], где авторы сгенерировали легитимный трафик, а также трафик, свойственный атаке. Для классификации трафика были рассмотрены такие методы, как коэффициент корреляции Пирсона, одноклассовая машина опорных

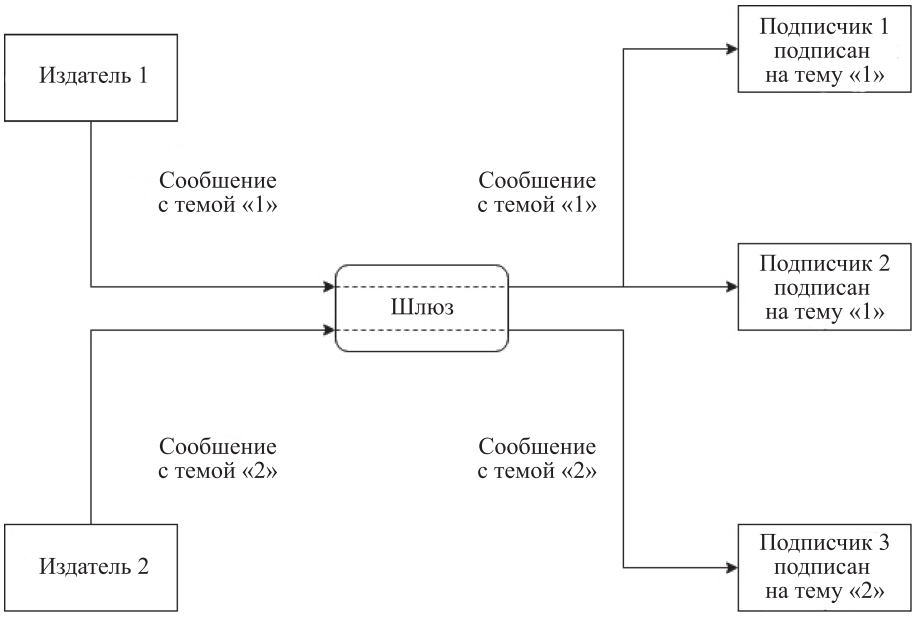

Рис. 1. Схема обмена сообщениями по протоколу MQTT

векторов (SVM), вычисление энтропии, рекуррентные нейронные сети (RNN), рекуррентные нейронные сети с долгой краткосрочной памятью (LSTM RNN). По результатам исследования было показано, что классификация данных методом опорных векторов наиболее точно предсказывает наличие аномалий.

Более общее исследование протокола MQTT представлено в [21], где рассмотрен эксперимент с одним физическим устройством. В результате исследования определены зависимости размера сообщения, временной задержки и количества потерянных пакетов от значения QoS-сообщения.

В [22] представлены результаты исследования по определению влияния алгоритма шифрования на ресурсы устройств. Авторы показали, что большинство протоколов среды «Интернет вещей» уязвимы к атакам на ресурсоистощение.

Один из основных параметров, по которым можно детектировать атаку, — это время обработки (доставки) сообщения. В [23] представлены результаты нагрузочного тестирования протокола MQTT. Согласно результатам эксперимента, протокол MQTT имеет большее время отклика, чем протокол CoAP, что делает его более уязвимым к атакам «отказ в обслуживании».

В [24] представлен другой подход к оценке безопасности протокола. Так как протокол MQTT не поддерживает криптографические преобразования, то, как правило, на практике дополнительно используют протокол TLS для генерации общего сессионного ключа и последующего симметричного шифрования данных. Авторы измеряли нагрузку на центральный процессор при использовании защищенных и незащищенных соединений. В качестве шлюза использовался микрокомпьютер Raspberry Pi 3. Рассматривались сценарии с последовательной отправкой сообщений с одним из трех видов значений QoS, а также со случайно сгенерированным значением QoS. Авторы сделали вывод о том, что значение QoS незначительно влияет на уровень нагрузки центрального процессора и наиболее успешный сценарий атаки на шлюз — это использование множества сообщений со значением QoS равным нулю по защищенному каналу с TLS-протоколом.

Анализ протокола MQTT также представлен в работе [25], где рассматривались различные сценарии: пошаговое увеличение значения QoS и увеличение числа устройств издателей от десяти до ста с шагом десять. Авторы показали, что увеличение значения QoS влияет на время доставки сообщения. Динамика изменения времени доставки при увеличении числа издателей более сложная. Рост задержки при QoS 0 и увеличении числа издателей носит ступенчатый характер. При QoS 1 резкое увеличение наблюдается, когда количество устройств издателей превышает 70. Аналогичная ситуация происходит при QoS 2, с тем отличием, что резкий рост наблюдается при более чем 90 издателях.

Исследование [26] представляет интерес тем, что учитывает влияние размера полезной нагрузки. Авторам удалось показать, что шлюз не смог обработать моделируемый поток сообщений с большим размером полезной нагрузки спустя 30 с после начала атаки. Для отслеживания состояния шлюза измерялись нагрузка на центральный процессор и размер занимаемой оперативной памяти.

Для среды «Интернет вещей» разрабатываются комплексные инструменты тестирования. В [27] представлен разработанный инструмент, симулирующий три вида атак, одна из которых является атакой на «отказ в обслуживании». В качестве входных данных использовались размер полезной нагрузки и количество сообщений, и измерялись: нагрузка на процессор; объем занимаемой оперативной памяти; использование постоянного запоминающего устройства.

Метод анализа протокола

Целью данной работы является анализ протокола MQTT на возможность реализации атаки «отказ в обслуживании», определение параметров информационного потока, которые необходимо учитывать при разработке средств обнаружения атак этого вида.

Основываясь на [18–21, 23–27], можно сделать вывод, что подходов к моделированию атак «отказ в обслуживании» для сети «Интернет вещей», использующих протокол MQTT, достаточно много. Однако зачастую игнорируется влияние создания защищенного соединения по протоколу TLS (так как протокол MQTT работает поверх протокола TCP, то протокол DTLS не применяется). В большинстве работ в качестве целевых сообщений рассматриваются сообщения вида publish. Так как протокол MQTT поддерживает 14 видов сообщений, то также стоит уделить внимание другим наиболее часто встречающимся видам сообщений, таким как connect (подключение к шлюзу), subscribe (подписка на тему).

Одной из промежуточных задач анализа является получение количественных характеристик о производительности шлюза при различных условиях. Под производительностью шлюза будет подразумеваться количество обработанных сообщений за единицу времени. Введем понятие: вид сообщения – это комбинация следующих характеристик сообщения:

— тип: connect, publish или subscribe;
— защищенное соединение (TLS-протокол): да или нет;
— QoS: 0, 1 или 2 (только для publish-сообщений).

Таким образом, в данной работе рассмотрено множество видов сообщений J, включающее в себя 10 элементов: connect-сообщения по защищенному каналу; connect-сообщения по незащищенному каналу; subscribe-сообщения по защищенному каналу; subscribe-сообщения по незащищенному каналу; publish-сообщения по защищенному каналу QoS 0; publish-сообщения по незащищенному каналу QoS 0; publish-сообщения по защищенному каналу QoS 1; publish-сообщения по незащищенному каналу QoS 1; publish-сообщения по защищенному каналу QoS 2; publish-сообщения по незащищенному каналу QoS 2. Изначально необходимо определить производительность шлюза при обработке каждого вида сообщений без параллельных нагрузок. Для этого выполняется следующая последовательность действий:

1) отправить последовательно большое количество сообщений (далее – поток сообщений) исследуемого вида;

2) измерить время доставки сообщений;
3) рассчитать производительность шлюза при последовательной обработке сообщений только потока исследуемого вида по формуле:

$$E_j = \frac{N_j}{\sum_{k=1}^{N_j} T_{kj}}, \quad (1)$$

где N_j — количество сообщений j-го вида ($j \in J$); T_{kj} — время обработки k-го сообщения j-го вида.

Затем необходимо рассчитать значение E_{ij} — производительность шлюза для потока j-го вида во время параллельной обработки шлюзом нескольких потоков i-го ($i \in J$) вида:

$$E_{ij} = \frac{N_j}{\sum_{k=1}^{N} T_{kj}}. \quad (2)$$

Далее вычисляется процентное соотношение значения производительности, полученное из уравнения (2), к значению производительности, полученному из уравнения (1):

$$F_{ij} = \frac{E_{ij}}{E_j} \times 100\%. \quad (3)$$

Данная величина характеризует, сколько процентов составляет производительность шлюза в отношении потока исследуемого вида сообщений при параллельной обработке еще и других потоков от производительности шлюза при обработке только потока исследуемого вида. Если значение F_{ij} близко к 100 %, то можно сделать вывод об отсутствии влияния параллельной обработки потоков i-го вида на время обработки сообщений одного потока j-го вида и отсутствии предрасположенности к возможности реализации атаки. Если значение F_{ij} близко к нулю, то можно заключить то, что шлюз не справляется с нагрузкой, и имеется потенциал для атаки «отказ в обслуживании». Итоговую оценку можно представить в виде набора количественных параметров, полученных после каждого этапа по формулам (1)–(3).

Для измерения среднего времени обработки connect- и subscribe-сообщений учитывается время, затраченное с момента отправки до момента получения подтверждения о получении от шлюза в виде connack- и suback-сообщений, соответственно. В случае publish-сообщений фиксируется время между моментом отправки и моментом получения его получателем.

Для проведения анализа была собрана экспериментальная установка (рис. 2). В качестве шлюза использовался проект с открытым исходным кодом Moquette, развернутый на микрокомпьютере Raspberry Pi 3 model B[1]. Моделирование клиентов производилось на двух отдельных персональных компьютерах (ПК 1 и ПК 2), один из которых отвечал за моделирование большого числа клиентов, другой — за имитацию всего

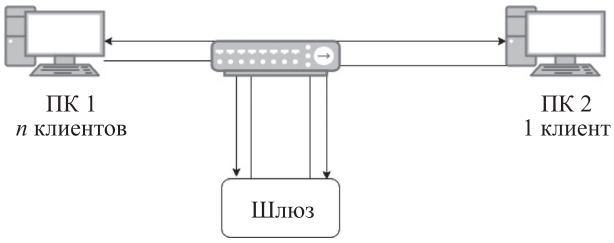

Рис. 2. Схема экспериментальной установки

лишь одного клиента. Программный модуль для моделирования клиентов основан на библиотеке paho-mqtt[2].

Результаты

При определении производительности шлюза для каждого вида сообщений без параллельных нагрузок на шлюзе были получены следующие результаты (рис. 3, 4). Процесс соединения устройства со шлюзом оказался самым затратным по времени. Так, обычное подключение по открытому каналу в среднем занимает 0,02 с, в то время как соединение по защищенному

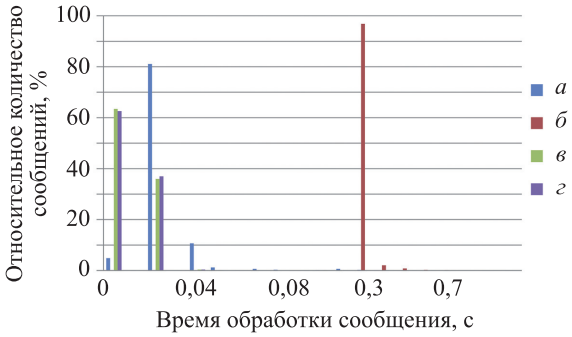

Рис. 3. Количество сообщений в процентном соотношении к их общему числу в зависимости от времени их обработки: connect (*а*) и subscribe (*в*) сообщения по открытому каналу; connect (*б*) и subscribe (*г*) сообщения по защищенному каналу

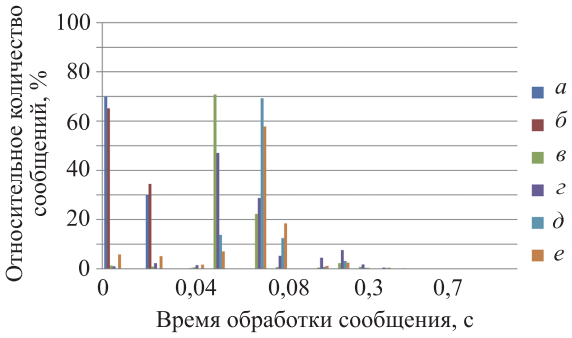

Рис. 4. Количество publish-сообщений в процентном соотношении к их общему числу в зависимости от времени их обработки: QoS 0 (*а*); QoS 1 (*в*); QoS 2 (*д*) по открытому каналу QoS 0 (*б*); QoS 1 (*г*); QoS 2 (*е*) по защищенному каналу

[1] Официальный сайт Raspberry. URL: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/ (дата обращения 02.02.2020).

[2] Официальный сайт клиента paho-mqtt. URL: https://pypi.org/project/paho-mqtt/1.3.0/ (дата обращения 02.02.2020).

Таблица 1. Значение параметра F_{ij} при условии $i = j$, %

Тип	Connect		Subscribe		Publish					
Параметры	без TLS	с TLS	без TLS	с TLS	без TLS			с TLS		
					QoS 0	QoS 1	QoS 2	QoS 0	QoS 1	QoS 2
F_{ij}	2,26	7,39	0,63	1,12	97,79	99,3	88,97	91,09	99,23	96,57

каналу через TLS-протокол занимает в среднем 0,24 с. Самыми быстрыми операциями являются подписка на тему и отправка-получение сообщения со значением QoS 0 (при одном получателе): 0,006 и 0,004 с соответственно. Среди других закономерностей можно выделить то, что с повышением значения QoS, время необходимое для доставки сообщения увеличивается (0,06 с при QoS 2). Причем наибольшая разница наблюдается между QoS 0 и остальными значениями QoS. Наличие защищенного канала незначительно влияет на обработку subscribe- и publish-сообщений. Обратная ситуация наблюдается при подключении устройства к шлюзу. Таким образом, наиболее подходящими сценариями для реализации атаки «отказ в обслуживании» являются:

1) множественные подключения к шлюзу с созданием защищенного канала;
2) отправка-получение сообщения со значением QoS ≥ 1, вне зависимости от защищенности канала.

Было определено влияние параллельной обработки множества потоков сообщений на производительность шлюза, вычисленную в отношении одного потока в рамках одного вида. В табл. 1 приведены сведения о значениях F_{ij} при $i = j$ для всех рассматриваемых видов сообщений.

Отчетливо прослеживается негативная динамика во всех сценариях, кроме массовой отправки publish-сообщений. Производительность шлюза при таком сценарии существенно снижается. Время на подключение устройства к шлюзу в тот момент, когда запросы на подключение отправлены многими другими устройствами, увеличивается (рис. 5). Для удобства графики на рис. 5 с результатами измерений, происходящих в одно и то же время, расположены друг под другом. В то же время, по умолчанию, шлюз поддерживает соединение в течение 30 с. Также существует ограничение на ожидание ответа при установлении TLS-соединения. Таким образом, в связи с превышением установленных временных пределов, соединение зачастую не устанавливается. Аналогичная ситуация происходит при попытке подписаться на тему с тем лишь отличием, что защищенность канала не играет большой роли. Отдельно стоит отметить сценарии с publish-сообщениями. В данном сценарии было всего одно устройство, подписанное на публикуемую тему. Вне зависимости от значения QoS и защищенности канала шлюз справлялся с нагрузкой, значение F_{ij} близко к 100 %.

Также была произведена оценка влияния параллельной обработки потоков сообщений одного вида на производительность шлюза, вычисленную в отношении потока другого вида ($i \neq j$). Функционирование шлюза нарушалось во всех случаях, кроме массовой отправки publish-сообщений при одном подписчике

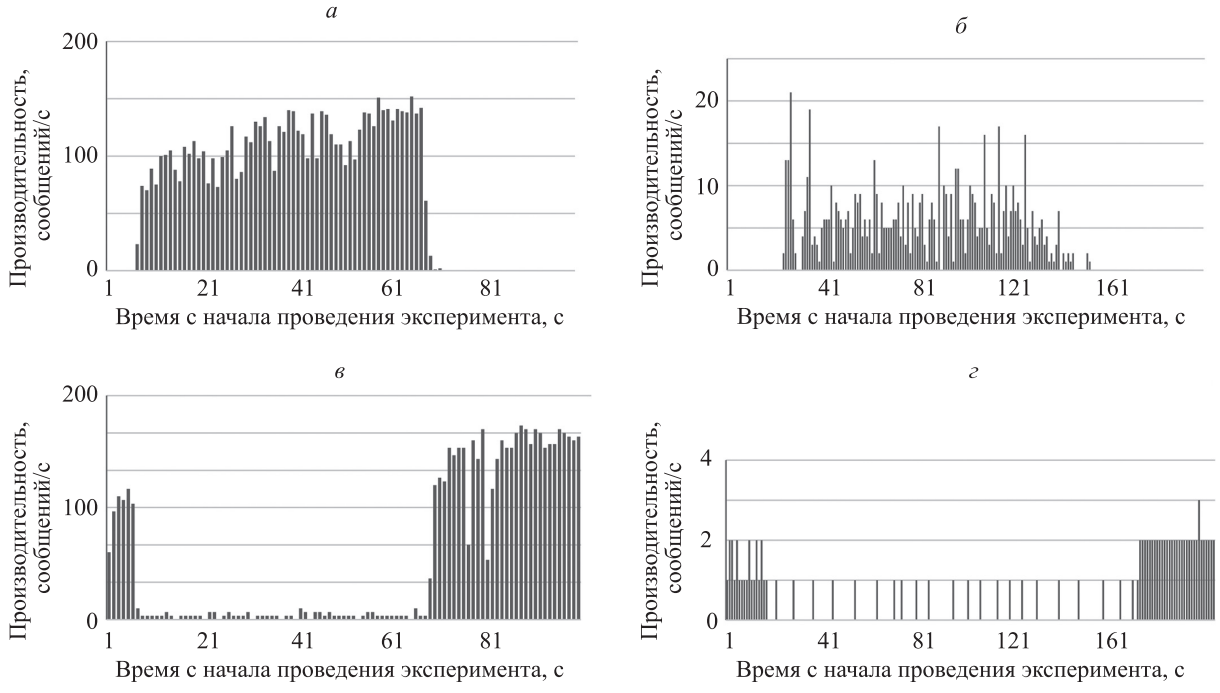

Рис. 5. Изменение производительности шлюза для сообщений: при потоке подключений от множества устройств (*а*) и одного устройства (*б*) по открытому каналу; при потоке подключений от множества устройств (*в*) и одного устройства (*г*) по защищенному каналу

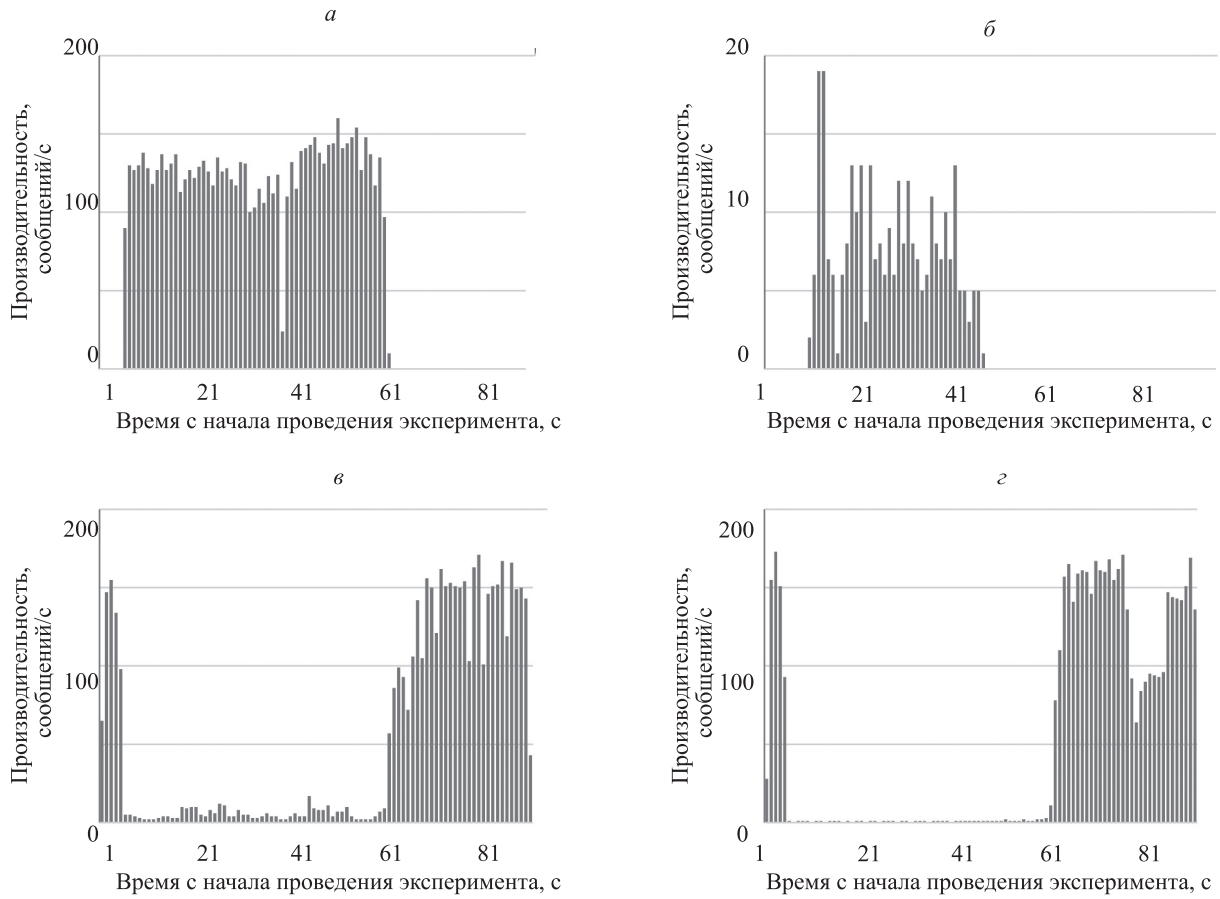

Рис. 6. Изменение производительности шлюза для сообщений: при потоке connect-сообщений от множества устройств (*а*) и subscribe-сообщений от одного устройства (*б*) по открытому каналу; при потоке connect-сообщений от множества устройств (*в*) и publish-сообщений от одного устройства QoS 0 (*г*) по защищенному каналу

(сценарии 3, 4, 7, 8 в табл. 2). После начала массовой отправки connect- и subscribe-сообщений, время, необходимое на обработку наблюдаемого потока, резко возрастало (рис. 6, табл. 2). Это свидетельствует о том, что потенциальному злоумышленнику достаточно сгенерировать большой поток сообщений любого из connect или subscribe видов, чтобы реализовать атаку, способную значительно увеличить время обработки любых других сообщений на шлюзе. Значение QoS для потоков publish-сообщений, как и ранее не имело большого влияния. Таким образом, атаку при использовании publish-сообщений для одного подписчика

Таблица 2. Сравнение параметра F_{ij} для некоторых сценариев при условии $i \neq j$

Исследуемый поток				Атакующие потоки			F_{ij}, %
Номер	Тип	TLS	QoS	Тип	TLS	QoS	
1	connect	—	—	subscribe	—	—	6,8
2	connect	—	—	subscribe	+	—	3,5
3	connect	—	—	publish	—	2	96,0
4	connect	—	—	publish	+	2	88,0
5	connect	—	—	connect	—	—	3,5
6	connect	—	—	connect	+	—	0,48
7	connect	—	—	publish	—	2	96,81
8	connect	—	—	publish	+	2	93,63
9	publish	—	0	connect	—	—	13,01
10	publish	—	0	connect	+	—	0,79
11	publish	—	0	subscribe	—	—	12,52
12	publish	—	0	subscribe	+	—	1,15

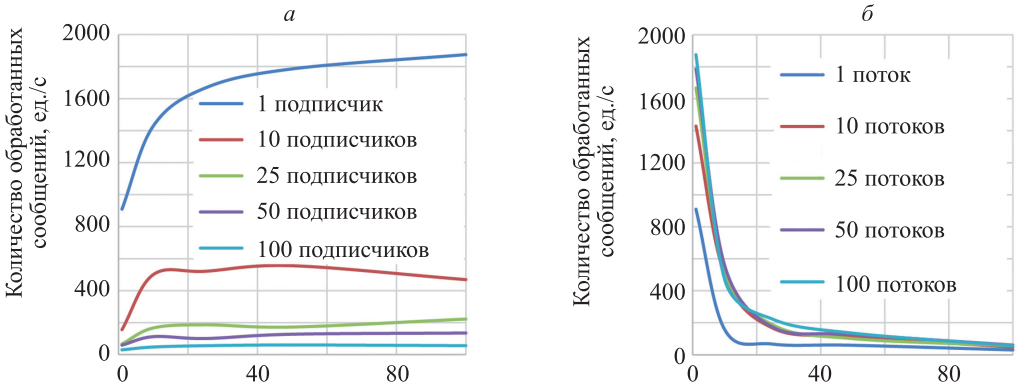

Рис. 7. Графики производительности шлюза при обработке publish-сообщений в зависимости от количества: одновременных потоков сообщений (*а*); подписчиков (*б*)

средствами экспериментальной установки смоделировать не удалось.

Также была исследована зависимость производительности шлюза при массовой рассылке publish-сообщений с разным значением QoS по защищенному и открытому каналам с большим числом подписчиков. В ходе проведения этой части исследования обособленное устройство теряло связь со шлюзом, следовательно, устройство не могло ни отправлять, ни принимать сообщения. Таким образом, атака «отказ в обслуживании» была воспроизведена в модельных условиях. После окончания атаки шлюз вновь обрабатывал сообщения в обычном режиме. Злоумышленник может временно повлиять на стабильность работы шлюза путем генерации большого потока publish-сообщений при большом числе подписчиков на публикуемую тему. Зависимость от значения QoS и защищенности канала не играла решающей роли.

Для publish-сообщений важно понять зависимость загрузки шлюза от количества издателей и получателей, а также оценить эту зависимость. Были смоделированы сценарии с различным количеством издателей и получателей (от 1 до 100), использовался QoS 0. Оцениваемым параметром являлось количество обработанных сообщений за единицу времени. Согласно полученным результатам (рис. 7), при небольшом количестве получателей зависимость производительности шлюза от числа одновременно обрабатываемых потоков publish-сообщений имеет вид логарифмической функции. Однако при увеличении количества получателей более чем 25 единиц производительность шлюза резко сокращается. Дальнейшее увеличение числа получателей незначительно сокращает производительность шлюза (рис. 7, *а*). На рис. 7, *б* изображена зависимость числа обработанных сообщений от количества подписчиков при одновременной обработке нескольких потоков сообщений. Большее число подписчиков (от 1 до 20) приводит к резкому сокращению производительности, при дальнейшем увеличении подписчиков скорость сокращения производительности уменьшается. Как было показано ранее, оба параметра оказывают влияние на итоговое время обработки сообщения. Чтобы определить, что имеет большее влияние на производительность: увеличение числа одновременно обрабатываемых сообщений или увеличение числа издателей, были рассчитаны скорости сокращения производительности шлюза в зависимости от того или иного параметра.

По результатам исследования выяснилось, что большее сокращение производительности наблюдается при увеличении количества подписчиков от 1 до 10, чем при изменении числа одновременно обрабатываемых потоков в тех же пределах. Дальнейшее увеличение числа подписчиков и потоков незначительно, но отрицательно влияет на производительность шлюза.

Заключение

В данной работе рассмотрен протокол MQTT с точки зрения его использования для атак «отказ в обслуживании». Рассмотрены существующие подходы к моделированию атак, произведен анализ сети на примере экспериментальной установки на базе микрокомпьютера Raspberry pi 3 — аппаратно и MQTT шлюза — программно. Основной подход, используемый в работе, — моделирование максимальной нагрузки на шлюз при различных исходных данных: количество устройств, максимальное число получателей и сообщений за единицу времени. Анализ состоял из четырех этапов, три из которых реализовывали нагрузочное тестирование по трем типам сообщений connect, publish, subscribe, учитывая значение QoS, наличие криптографических преобразований по протоколу TLS и количество устройств.

Согласно результатам эксперимента, можно выделить следующие основные выводы:

— сети «Интернет вещей», использующие протокол MQTT, подвержены атакам «отказ в обслуживании», не только из-за массовых рассылок publish-сообщений, как показано во многих других работах, но и массовых рассылок других видов сообщений: connect, subscribe;

— после прекращения атаки работоспособность шлюза через некоторое время восстанавливается, если не превышены максимальные значения занимаемой оперативной памяти;

— создание защищенного канала по протоколу TLS с помощью connect-сообщений требует наибольших временных затрат, что может быть использовано злоумышленниками для увеличения нагрузки на

шлюз, и, как следствие, может способствовать возникновению ошибки подключения;
— большой поток сообщений любого из рассмотренных видов сообщений влияет на производительность шлюза. При этом для publish-сообщений большое влияние в первую очередь имеет количество получателей;
— определена зависимость производительности шлюза для publish-сообщений при различном числе одновременных потоков сообщений и количестве получателей.

Литература

1. Эванс Д. Интернет вещей. Как изменится вся наша жизнь на очередном витке развития Всемирной сети. Cisco IBSG, 2011. 14 с.
2. Соколов М.Н., Смолянинова К.А., Якушева Н.А. Проблемы безопасности Интернет вещей: обзор // Вопросы кибербезопасности. 2015. № 5(13). С. 32–35.
3. Гришенцев А.Ю., Коробейников А.Г. Проектирование и технологическая подготовка сетей станций вертикального зондирования ионосферы // Научно-технический вестник информационных технологий, механики и оптики. 2013. Т. 13. № 3(85). С. 61–66.
4. Гришенцев А.Ю., Коробейников А.Г. Средства интероперабельности в распределенных геоинформационных системах // Журнал радиоэлектроники. 2015. № 3. С. 19.
5. Kliarsky A. Detecting Attacks Against The “Internet of Things”. SANS Institute Information Security Reading Room, 2017. 36 p.
6. Albalawi U., Joshi S. Secure and trusted telemedicine in Internet of Things IoT // Proc. 4th IEEE World Forum on Internet of Things (WF-IoT). 2018. P. 30–34. doi: 10.1109/WF-IoT.2018.8355206
7. Wazid M., Das A.K., Khan M.K., Al-Ghaiheb A.A.-D., Kumar N., Vasilakos A.V. Secure authentication scheme for medicine anti-counterfeiting system in IoT environment // IEEE Internet of Things Journal. 2017. V. 4. N 5. P. 1634–1646. doi: 10.1109/JIOT.2017.2706752
8. Коновалова С.В., Миронов А.Н. Вопросы информационной безопасности интернета вещей // ИТ-СТАНДАРТ. 2016. № 4(9). С. 37–39.
9. Liang L., Zheng K., Sheng Q., Huang X. A Denial of service attack method for an IoT system // Proc. 8th International Conference on Information Technology in Medicine and Education (ITME 2016). 2016. P. 360–364. doi: 10.1109/ITME.2016.0087
10. Chen Q., Chen H., Cai Y., Zhang Y., Huang X. Denial of service attack on IoT system // Proc. 9th International Conference on Information Technology in Medicine and Education (ITME 2018). 2018. P. 755–758. doi: 10.1109/ITME.2018.00171
11. Fuchs P. DoS Detection in NodeRED. Bachelor Thesis University of Passau, 2015. 81 p.
12. McDermott C., Majdani F., Petrovski A.V. Botnet detection in the Internet of Things using deep learning approaches // Proc. of the International Joint Conference on Neural Networks (IJCNN 2018). 2018. P. 8489489. doi: 10.1109/IJCNN.2018.8489489
13. Moustafa N., Turnbull B., Choo K-K.R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things // IEEE Internet of Things Journal. 2019. V. 6. N 3. P. 4815–4830. doi: 10.1109/JIOT.2018.2871719
14. Abdul-Ghani H.A., Konstantas D., Mahyoub M. A Comprehensive IoT attacks survey based on a building-blocked reference model // International Journal of Advanced Computer Science and Applications. 2018. V. 9. N 3. P. 355–373. doi: 10.14569/IJACSA.2018.090349
15. Andy S., Rahardjo B., Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system // Proc. 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). 2017. P. 600–604. doi: 10.11591/eecsi.4.1064
16. Дикий Д.И., Артемьева В.Д. Протокол передачи данных MQTT в модели удаленного управления правами доступа для сетей Интернета // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 1. С. 109–117. doi: 10.17586/2226-1494-2019-19-1-109-117
17. Perrone G., Vecchio M., Pecori R., Giaffreda R. The day after mirai: a survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices // Proc. 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017). 2017. P. 246–253. doi: 10.5220/0006287302460253

References

1. Evans D. *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*. Cisco IBSG, 2011, 14 p.
2. Sokolov M., Smolyaninova Ch., Yakusheva N. Security problems Internet of Things: Survey. *Voprosy kiberbezopasnosti*, 2015, no. 5(13), pp. 32–35. (in Russian)
3. Grishentcev A., Korobeynikov A. Design and engineering background for station networks of vertical ionosphere sounding. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, vol. 13, no. 3(85), pp. 61–66. (in Russian)
4. Grishentcev A., Korobeynikov A. Interoperability facilities in distributed geographic information systems. *Zhurnal Radioelektroniki*, 2015, no. 3, pp. 19. (in Russian)
5. Kliarsky A. Detecting Attacks Against The “Internet of Things”. SANS Institute Information Security Reading Room, 2017, 36 p.
6. Albalawi U., Joshi S. Secure and trusted telemedicine in Internet of Things IoT. *Proc. 4th IEEE World Forum on Internet of Things (WF-IoT)*, 2018, pp. 30–34. doi: 10.1109/WF-IoT.2018.8355206
7. Wazid M., Das A.K., Khan M.K., Al-Ghaiheb A.A.-D., Kumar N., Vasilakos A.V. Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. *IEEE Internet of Things Journal*, 2017, vol. 4, no. 5, pp. 1634–1646. doi: 10.1109/JIOT.2017.2706752
8. Konovalova S.V., Mironov A.N. Questions of the information security of the Internet of Things. *IT-STANDARD*, 2016, no. 4(9), pp. 37–39. (in Russian)
9. Liang L., Zheng K., Sheng Q., Huang X. A Denial of service attack method for an IoT system. *Proc. 8th International Conference on Information Technology in Medicine and Education (ITME 2016)*, 2016, pp. 360–364. doi: 10.1109/ITME.2016.0087
10. Chen Q., Chen H., Cai Y., Zhang Y., Huang X. Denial of service attack on IoT system. *Proc. 9th International Conference on Information Technology in Medicine and Education (ITME 2018)*, 2018, pp. 755–758. doi: 10.1109/ITME.2018.00171
11. Fuchs P. DoS Detection in NodeRED. Bachelor Thesis University of Passau, 2015, 81 p.
12. McDermott C., Majdani F., Petrovski A.V. Botnet detection in the Internet of Things using deep learning approaches. *Proc. of the International Joint Conference on Neural Networks (IJCNN 2018)*, 2018, pp. 8489489. doi: 10.1109/IJCNN.2018.8489489
13. Moustafa N., Turnbull B., Choo K-K.R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal*, 2019, vol. 6, no. 3, pp. 4815–4830. doi: 10.1109/JIOT.2018.2871719
14. Abdul-Ghani H.A., Konstantas D., Mahyoub M. A Comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*, 2018, vol. 9, no. 3, pp. 355–373. doi: 10.14569/IJACSA.2018.090349
15. Andy S., Rahardjo B., Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. *Proc. 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017, pp. 600–604. doi: 10.11591/eecsi.4.1064
16. Dikii D.I., Artemeva V.D. MQTT data protocol in remote access control management model for Internet networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 1, pp. 109–117. (in Russian). doi: 10.17586/2226-1494-2019-19-1-109-117
17. Perrone G., Vecchio M., Pecori R., Giaffreda R. The day after mirai: a survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices. *Proc. 2nd International*

18. Chifor B., Bica I., Patriciu V. Mitigating DoS attacks in publish-subscribe IoT networks // Proc. 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2017). 2017. P. 1–6. doi: 10.1109/ECAI.2017.8166463
19. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT – Network-based detection of IoT botnet attacks using deep autoencoders // IEEE Pervasive Computing. 2018. V. 17. N 3. P. 12–22. doi: 10.1109/MPRV.2018.03367731
20. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset // Future Generation Computer Systems. 2019. V. 100. P. 779–796. doi: 10.1016/j.future.2019.05.041
21. Фам В.Д., Юльчиева Л.О., Киричек Р.В. Исследование протоколов взаимодействия интернета вещей на базе лабораторного стенда // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 55–67.
22. Kim J.Y., Holz R., Hu W., Jha S. Automated analysis of secure Internet of Things protocols // Proc. 33rd Annual Computer Security Applications Conference (ACSAC 2017). 2017. P. 238–249. doi: 10.1145/3134600.3134624
23. Долгушев Р.А., Киричек Р.В., Кучерявый А.Е. Обзор возможных видов и методов тестирования Интернет вещей // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 1–11.
24. Fehrenbach P. Messaging Queues in the IoT under pressure // Computational Science and Its Applications, ICCSA. 2018. P. 1–9.
25. Handosa M., Gračanin D., Performance evaluation of MQTT-based internet of things systems // Proc. 2017 Winter Simulation Conference (WSC 2017). 2017. P. 4544–4545. doi: 10.1109/WSC.2017.8248196
26. Firdous S.N., Baig Z., Valli C., Ibrahim A. Modelling and evaluation of malicious attacks against the IoT MQTT protocol // Proc. 10th IEEE International Conference on Internet of Things, iThings 2017, 13th IEEE International Conference on Green Computing and Communications, GreenCom 2017, 10th IEEE International Conference on Cyber, Physical and Social Computing, CPSCom 2017 and the 3rd IEEE International Conference on Smart Data, Smart Data. 2017. P. 748–755. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115
27. Bao C., Guan X., Sheng Q., Zheng K., Huang X. A Tool for Denial of Service Attack Testing in IoT // Proc. 8th International Conference on Information Technology in Medicine and Education (ITME). 2016. P. 1–6.

Conference on Internet of Things, Big Data and Security (IoTBDS 2017), 2017, pp. 246–253. doi: 10.5220/0006287302460253
18. Chifor B., Bica I., Patriciu V. Mitigating DoS attacks in publish-subscribe IoT networks. *Proc. 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI 2017)*, 2017, pp. 1–6. doi: 10.1109/ECAI.2017.8166463
19. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT — Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 2018, vol. 17, no. 3, pp. 12–22. doi: 10.1109/MPRV.2018.03367731
20. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, 2019, vol. 100, pp. 779–796. doi: 10.1016/j.future.2019.05.041
21. Pham V., Yulchieva L., Kirichek R. Research of Protocols of interaction of the Internet of Things on the basis of the laboratory bench. *Telecom IT*, 2016, vol. 4, no. 1, pp. 55–67. (in Russian)
22. Kim J.Y., Holz R., Hu W., Jha S. Automated analysis of secure Internet of Things protocols. *Proc. 33rd Annual Computer Security Applications Conference (ACSAC 2017)*, 2017, pp. 238–249. doi: 10.1145/3134600.3134624
23. Dolgushev R., Kirichek R., Koucheryavy A. An overview of possible testing types and methods for the Internet of Things. *Telecom IT*, 2016, vol. 4, no. 2, pp. 1–11. (in Russian)
24. Fehrenbach P. Messaging Queues in the IoT under pressure. *Computational Science and Its Applications, ICCSA*, 2018, pp. 1–9.
25. Handosa M., Gračanin D., Performance evaluation of MQTT-based internet of things systems. *Proc. 2017 Winter Simulation Conference (WSC 2017)*, 2017, pp. 4544–4545. doi: 10.1109/WSC.2017.8248196
26. Firdous S.N., Baig Z., Valli C., Ibrahim A. Modelling and evaluation of malicious attacks against the IoT MQTT protocol. *Proc. 10th IEEE International Conference on Internet of Things, iThings 2017, 13th IEEE International Conference on Green Computing and Communications, GreenCom 2017, 10th IEEE International Conference on Cyber, Physical and Social Computing, CPSCom 2017 and the 3rd IEEE International Conference on Smart Data, Smart Data*, 2017, pp. 748–755. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115
27. Bao C., Guan X., Sheng Q., Zheng K., Huang X. A Tool for Denial of Service Attack Testing in IoT. *Proc. 8th International Conference on Information Technology in Medicine and Education (ITME)*, 2016. pp. 1–6.

Авторы

Дикий Дмитрий Игоревич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56998707400, ORCID ID: 0000-0002-8819-8423, dimandikiy@mail.ru

Authors

Dmitry I. Dikii — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56998707400, ORCID ID: 0000-0002-8819-8423, dimandikiy@mail.ru