

ОБЗОР ВОЗМОЖНЫХ ВИДОВ И МЕТОДОВ ТЕСТИРОВАНИЯ ИНТЕРНЕТ ВЕЩЕЙ

Р. А. Долгушев¹, Р. В. Киричек¹, А. Е. Кучерявый¹

¹ СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
Адрес для переписки: kirichek@sut.ru

Информация о статье

УДК 004.7

Язык статьи – русский.

Поступила в редакцию 21.03.16, принята к печати 22.04.16.

Ссылка для цитирования: Долгушев Р. А., Киричек Р. В., Кучерявый А. Е. Обзор возможных видов и методов тестирования Интернет вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 2. С. 1–11.

Аннотация

Предмет исследования. Статья посвящена обзору видов и методов тестирования Интернет Вещей. **Метод.** В качестве метода исследования приводится анализ существующих видов и подходов к тестированию, которые используются в сетях связи в настоящее время. В работе на основе обзора предложен ряд тестовых спецификаций для проведения комплексного тестирования Интернет Вещей. **Основные результаты.** В ходе тестирования возможно оценить различные критерии: вероятностно-временные параметры, связанные с обменом данными между Вещами, а также с использованием сетевых ресурсов, протоколов и т. д. **Практическая значимость.** В качестве апробации предлагаемых тестовых спецификаций приведен натурный эксперимент по тестированию фрагмента сети связи с целью выбора прикладного протокола для типовой Интернет Вещи. Выбор протокола осуществляется на базе определения среднего времени отклика на запрос (RTT) при использовании протоколов MQTT, CoAP и HTTP.

Ключевые слова

Интернет Вещь, ИВ, IoT, Wi-Fi, Bluetooth, ZigBee, MQTT, CoAP, HTTP.



AN OVERVIEW OF POSSIBLE TESTING TYPES AND METHODS FOR THE INTERNET OF THINGS

R. Dolgushev¹, R. Kirichek¹, A. Koucheryavy¹

¹ SPbSUT, St. Petersburg, 193232, Russian Federation
Corresponding author: kirichek@sut.ru

Article info

Article in Russian.

Received 21.03.16, accepted 22.04.16.

For citation: Dolgushev R., Kirichek R., Koucheryavy A.: An Overview of Possible Testing Types and Methods for the Internet of Things // Telecom IT. 2016. Vol. 4. Iss. 2. pp. 1–11 (in Russian).

Abstract

Research subject. The article provides an overview of types and methods of testing various Internet Things. **Method.** Existing testing approaches that are used in communication networks nowadays have been analyzed during the research. In this article, set of test specifications was proposed for the complex testing of Internet Things. **Core results.** During the test it is possible to evaluate various criteria such as probabilistic and time parameters associated with the data exchange between things, as well as with the use of network resources, protocols, etc. **Practical relevance.** As a validation of the proposed test specifications the natural experiment was made to test the fragment of network with the purpose of selecting a standard application protocol for the typical Internet Thing. Protocol selection is based on the determination of the average response time to a request (RTT) using such protocols as MQTT, CoAP and HTTP.

Keywords

Internet Thing, IoT, Wi-Fi, Bluetooth, ZigBee, MQTT, CoAP, HTTP.

Введение

В январе 2016 г. на Всемирном экономическом форуме был отмечен тот факт, что в данный момент времени человечество находится на краю новой четвертой технологической революции (Industry 4.0), которая характеризуется слиянием технологий, стирающей грани между физическим и цифровым миром. Возможности миллиардов людей, связанные с различными мобильными устройствами, имеющими небывалые вычислительные мощности, память и доступ к всевозможной информации, по сути, не ограничены. И эти возможности будут только увеличиваться с приходом таких технологий, как искусственный интеллект, робототехника, 3D-печать, нано- и биотехнологии, технологии хранения энергии, квантовые вычисления, а также Интернет Вещей [1, 2].

Традиционно на протяжении долгих лет многие устройства тестировались изолированно, и никто не заботился о таких вещах, как пользовательский интерфейс (если таковой вообще был) или о подключении этих устройств к сети Интернет. Однако, в последние годы так называемый Интернет Вещей приобрел большую популярность, так как количество устройств, подключенных к сети Интернет неуклонно растет. Классический подход к тестированию сетевых устройств и активного сетевого оборудования не всегда может быть использо-



ван для тестирования Интернета Вещей. Нужно выработать новые стратегии, которые помогут добиться стабильной работы всех компонентов сети. Вследствие этого вопрос об их тестировании является на данный момент открытым и актуальным, поэтому появилась необходимость в разработке эффективных методов их тестирования, которые помогли бы решить данную проблему.

Термин Интернет Вещей определяет единую сеть, соединяющую окружающие нас объекты реального и виртуального миров, а также расширенные возможности подключения различных устройств, систем и услуг к сети Интернет^{1,2}. Он включает в себя ряд протоколов, многочисленные и разнообразные устройства, и даже web-приложения. Проще говоря, Интернет Вещей – это будущее технологий, которое расширяет возможности по сбору, анализу и распределению данных, которые человек затем сможет превратить в информацию или знания. В данный момент времени в сети Интернет насчитывается свыше 25 млрд подключенных устройств, и ожидается, что их число превысит отметку в 50 млрд в 2020 г.³

Устройства Интернета Вещей могут быть подключены к сети, а также друг к другу при помощи как проводных, так и беспроводных технологий, например, Wi-Fi, LTE, Bluetooth LE, ZigBee и т. д. В будущем ожидается, что каждая Вещь будет использовать свой уникальный IPv6-адрес. Адресное пространство IPv6 содержит $3,4 \times 10^{38}$ адресов, что отвечает на потребность в пуле адресов для поддержки экспоненциального роста устройств, подключающихся к Интернету. Стоит отметить, что в дальнейшем Интернет Вещей будет генерировать огромный объем данных (*Big Data*), которые к тому же, обладают другими характеристиками, нежели таковые в традиционной модели связи (аудио, видео, данные), что заставляет серьезно задуматься о модернизации уже существующих телекоммуникационных систем, систем обработки и хранения. Важно то, что на передачу данных от IoT-устройств к серверу влияет не только качество соединения, но также и такие параметры, как энергозависимость Вещей, особые протоколы маршрутизации и методы сжатия информации. Наличие этих особенностей влечет за собой новые промежуточные этапы для обработки данных.

Таким образом, IoT-устройства будут разделять вопросы разработки и тестирования во встраиваемых программных системах, также как это происходит и в традиционных IT- и web-системах. С ростом числа устройств Интернета Вещей и программных проектов потребность в тестировщиках и особых подходах к тестированию также возрастет. Специалисты в этой области столкнутся с множеством различных проблем и возможных ошибок.

Необходимые решения для тестирования Интернет Вещей

Количество Интернет Вещей с каждым днем растет, создавая новые возможности для бытовой сферы, сферы бизнеса. Но не всегда новые продукты вписываются в обычные сценарии, используемые разработчиками ПО. Вследствие этого, возникает ряд определенных вопросов, также касающихся и методов тестирования IoT. Кроме того, проблемы в сфере тестирования затрагивают и вопросы относительно безопасности при использовании Вещей.

¹ Y.2060. Обзор Интернета Вещей // Рекомендация МСЭ-T // 06.2012.

² Y.2069. Термины и определения для Интернета Вещей // Рекомендация МСЭ-T // 07.2012.

³ Интернет вещей, IoT, M2M (мировой рынок) // URL: www.tadviser.ru/a/302413



Чтобы гарантировать качество продуктов и услуг Интернета Вещей необходимо выработать такие решения для тестирования, как:

1) Продуманная стратегия тестирования. Нужно сосредоточиться на эффективных методах и практиках тестирования. Четкие требования, детальный план испытаний должны быть частью данной стратегии, что позволит в дальнейшем выпустить качественный продукт или услугу.

2) Новые инструменты и платформы тестирования. Новые платформы будут необходимы для извлечения полезной информации из огромного количества необработанных данных, обеспечивая при этом основу для систем технической поддержки. Также понадобятся дополнительные инструменты, утилиты и симуляторы для тестирования, так как в противном случае данный процесс будет затруднен.

3) Тестирование методом «черного ящика». Для разработки эффективных тестов нужно уметь выявить архитектуру устройства, тип операционной системы, протоколы взаимодействия без знания внутренних механизмов тестируемого объекта (рис. 1).

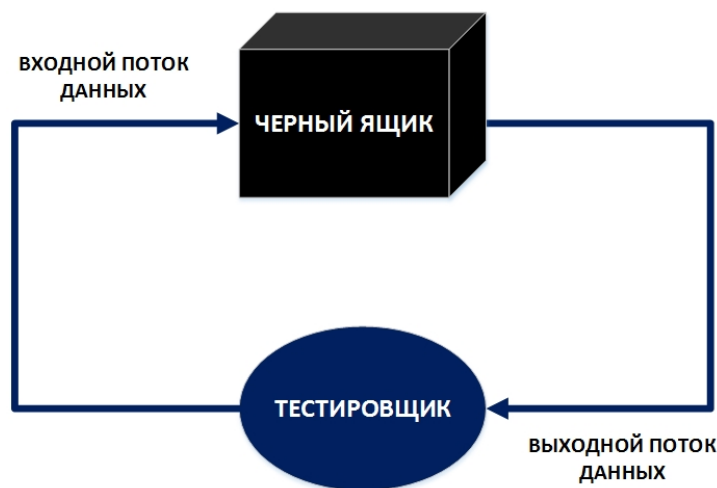


Рис. 1. Тестирование методом «черного ящика»

Анализ методов и видов тестирования Интернет Вещей

Рекомендация МСЭ-Т Q.3900 «Архитектура модельной сети и методы тестирования технических средств сетей связи нового поколения (NGN) для использования в сетях связи общего пользования»⁴, выпущенная в 2006 г., стала основным стандартом для тестирования NGN-сетей [3]. Данную концепцию можно использовать и относительно тестирования Интернет Вещей, однако, рекомендация Q.3900 не определяет структуру IoT-тестирования.

Как уже было сказано, тестирование Интернет Вещей так или иначе относится к проверке различных аспектов, касающихся функционирования самих устройств, их взаимодействия с сетью и безопасности. Проблемы тестирования выходят за рамки устройств и датчиков, так как включают в себя дополнительные сложности, связанные с концепцией больших данных, т. е. большой объем

⁴ Q.3900. Методы тестирования и архитектура модельных сетей для тестирования технических средств СПП, используемых в сетях электросвязи общего пользования // Рекомендация МСЭ-Т // 09.2006.



и разнообразие генерируемой информации. Кроме того, на текущий момент, не существует единого подхода к тестированию устройств Интернета Вещей, которые существуют для узлов сети связи следующего поколения. Таким образом, создание модельной сети и различных методов тестирования поможет решить данную проблему.

На данный момент существует четыре основные области тестирования IoT-устройств, которые должны учитываться при разработке любого продукта, имеющего возможность подключения к сети Интернет. Они приведены далее на рисунке 2.



Рис. 2. Области тестирования Интернет Вещей

Процесс тестирования крайне важен. Вследствие этого необходимо использовать специальные симуляторы, которые могут имитировать работу сетевых узлов и устройств Интернета Вещей, что позволит сократить расходы на оборудование. В целом, вопросы, касающиеся тестирования охватывают большую область, начиная с самих устройств, всевозможных датчиков и заканчивая различными платформами, которые собирают и анализируют данные Интернет Вещей.

Помимо тестирования устройств физического мира, также есть определенные виды тестирования виртуальных Вещей. Виртуальные Вещи существуют в информационном мире, их можно хранить, обрабатывать и получать к ним доступ. Примером таких вещей является прикладное ПО и мультимедийный контент.

Наиболее распространенные методы для тестирования ПО:

1) Модульное тестирование. В данном методе с целью выявления возможных ошибок компоненты программы проверяются в отдельности. При этом необходимо хорошо знать состав программы, следовательно, этот вид тестирования осуществляется программистами, а не тестировщиками.

2) Интеграционное тестирование. В основном выявляет ошибки интерфейса. Компоненты программы, которые были проверены в ходе модульного тестирования, интегрируются друг с другом, а затем тестируются на наличие неполадок.

3) Системное тестирование. На данном этапе анализируется работа всей системы в целом при взаимодействии ее аппаратных и программных составляющих.

Виды тестирования Интернет Вещей

В данном пункте будут рассмотрены некоторые виды тестирования, которые проводятся тестировщиками для обеспечения стабильной работы IoT-систем (рис. 3).

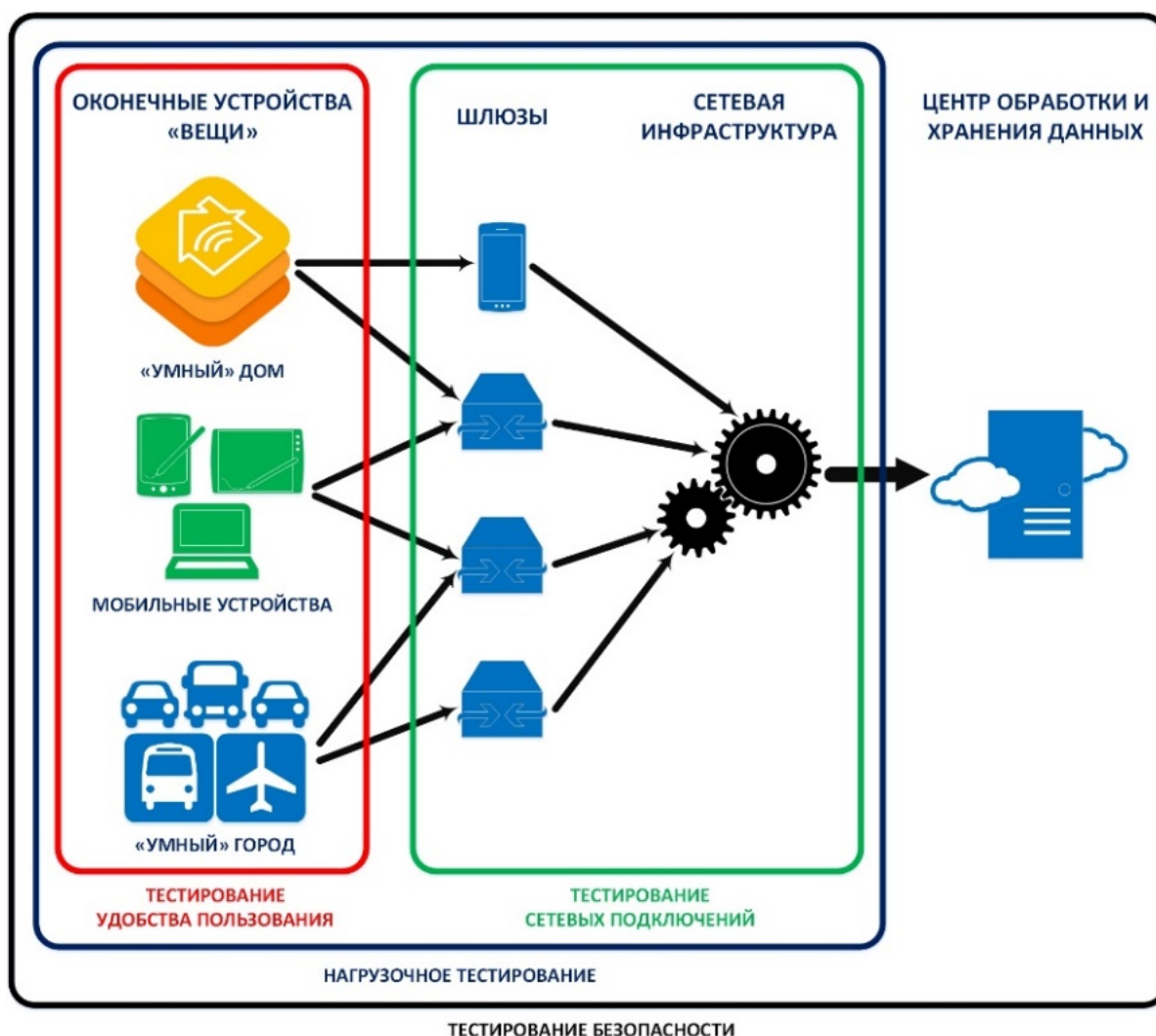


Рис. 3. Виды тестирования Интернет Вещей

Тестирование удобства пользования (Usability Testing)

Прежде всего, функциональные возможности Интернет Вещей должны отвечать требованиям пользователя. Наиболее важным моментом является то, что потребитель смог бы выявить все свойства и особенности продукта без каких-либо проблем. Этот метод тестирования направлен на установление степени удобства использования, обучаемости, понятности и привлекательности разрабатываемого продукта для пользователей.

Для того, чтобы провести такое тестирование, нужно отобрать группу людей, соответствующих определенным критериям (пол, возраст, род деятельности), и провести среди них небольшой опрос. Это позволит получить оценки и отзывы относительно использования какого-либо продукта, что в дальнейшем поможет повысить его качество.

Тестирование сетевых подключений (Connectivity Testing)

Интернет Вещи должны взаимодействовать друг с другом, поэтому необходимо обратить внимание на различные способы связи, а также на обмен информацией между устройствами и пользователями [4, 5]. В ходе тестирования сетевых подключений важно учитывать среду, в которой будет использоваться устройство (тип сети, мощность сигнала, погодные условия и т. д.), и проверять то, как оно функционирует при заданных условиях.

Нагрузочное тестирование (Benchmark Testing)

Нагрузочное тестирование Интернета Вещей по сути сводится к проверке взаимодействия между IoT-устройствами и сетевой инфраструктурой. Основная задача такого типа тестирования – тщательный учет проблем, связанных с сетью, которые привели или могут привести к разрыву соединения, а также проверка маршрутизаторов и коммутаторов на предмет устойчивости к трафику Интернета Вещей. Необходимость в создании методики для такого типа тестирования связано с тем, что IoT-трафик отличается от классического трафика конвергентных сетей связи, в связи с чем возникает вопрос устойчивости существующего оборудования сетей связи к трафику подобного типа [6].

При таком подходе инженеры контроля качества должны учитывать такие особенности, как пропускная способность сети, задержки, нагрузку, иные законы распределения, потери пакетов, большое количество одновременно работающих пользователей и т. д. Также важно учитывать системные показатели устройств, например, потребляемая мощность, температура, использование памяти, загрузка процессора. Влияние всех этих факторов в Интернете Вещей может быть гораздо более серьезным. Другими словами, такие устройства, как автомобиль, могут перестать отвечать на посылаемые команды, что может привести к печальным последствиям. Во избежание возможных проблем, которые могут повлиять на производительность, необходимо проводить тестирование разных типов сетей и потоков данных. Тестировщики должны всесторонне анализировать сетевую активность, учитывая то, насколько быстро данные могут быть переданы от одного узла сети к другому. Модель нагрузочного тестирования представлена на рисунке 4.



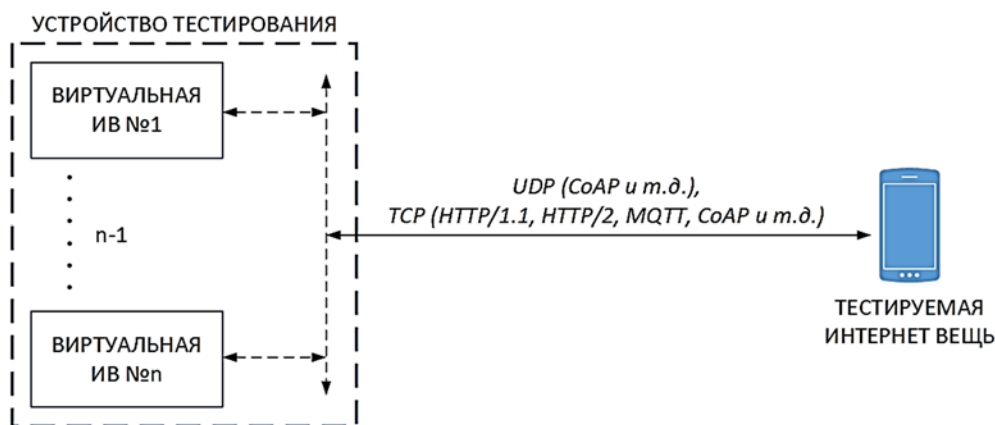


Рис. 4. Модель нагрузочного тестирования IoT-устройств

Тестирование безопасности (Security Testing)

При разработке Интернет Вещей также нужно заботиться об их безопасности, для того, чтобы избежать несанкционированного доступа к устройствам или данным со стороны злоумышленников. Этот вид тестирования зачастую упускается из внимания по причине рыночного давления на компании, что заставляет их как можно быстрее выпускать новые продукты. Также сказывается отсутствие общих стандартов сетевой безопасности для Интернет Вещей и их ограниченная вычислительная мощность.

Тестирование безопасности в Интернете Вещей имеет очень важное значение, так как поведение IoT-устройств влияет на повседневную жизнь людей. Если не уделить должного внимания на степень защищенности устройств, то у злоумышленников будет возможность получить к ним доступ дистанционно через беспроводное соединение. Таким образом, разработчикам необходимо проверять безопасность IoT-систем, чтобы гарантировать, что доступ к ней осуществляется только авторизованными пользователями, и передаваемые данные не смогут быть перехвачены вследствие хакерской атаки.

Существует два основных вида тестирования безопасности:

1) Статические тесты. Проводятся либо вручную, либо при помощи средств проверки кода. Главная задача такого тестирования состоит в том, чтобы проанализировать программный код, написанный для устройства, и определить возможные бреши в безопасности.

2) Динамические тесты. Заключаются в использовании специальных инструментов, которые проверяют устройство в процессе его нормальной работы и выявляют наличие проблем, связанных с аутентификацией, перехватывают и анализируют сетевой трафик, отмечают недопустимое использование памяти устройства, имитируют хакерские атаки и т. д.

Виды взаимодействия Интернет Вещей и возможные тестовые спецификации

Согласно рекомендации МСЭ Y.2060⁵ возможны следующие виды взаимодействия различных типов Интернет Вещей (рис. 5):

1. Обмен данными с использованием сети связи через шлюз.

⁵ Y.2060. Обзор Интернета Вещей // Рекомендация МСЭ-T // 06.2012.



2. Обмен данными с использованием сети связи без шлюза.
3. Обмен данными напрямую, т. е. без использования сети связи.
4. Сочетание первого и третьего сценариев.
5. Сочетание второго и третьего сценариев.

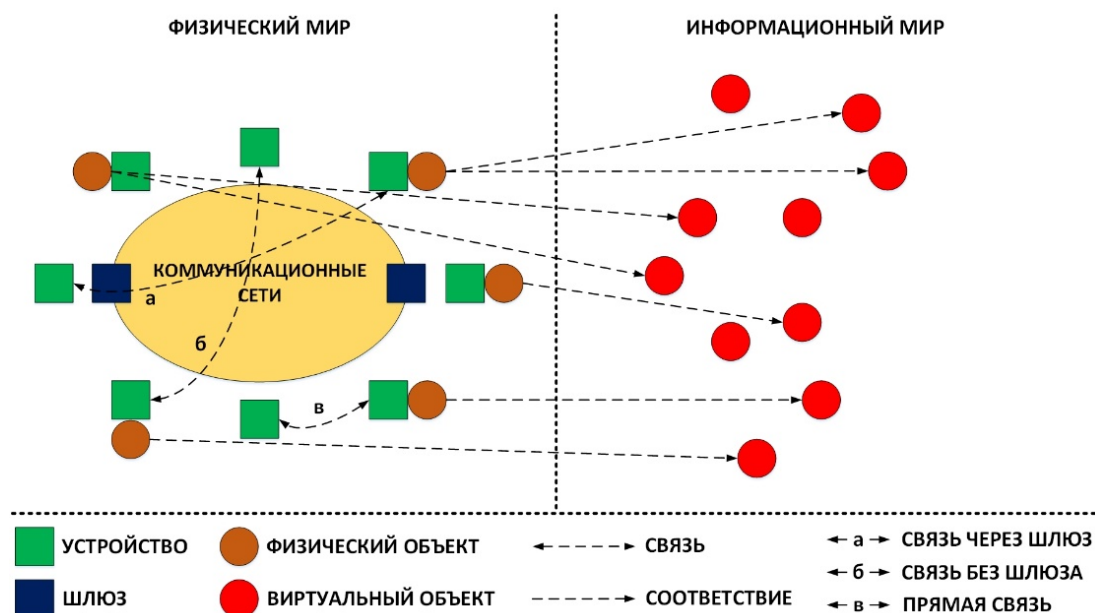


Рис. 5. Виды взаимодействия Интернет Вещей

Следует отметить тот факт, что, хотя на данной схеме показаны взаимодействия между объектами физического мира (обмен данными между устройствами), они также происходят и в информационном мире (взаимодействие виртуальных вещей), а также между физическим и информационным миром.

Далее приведены некоторые виды возможных тестов для Интернет Вещей, относительно используемых сетевых технологий:

- 1) Тестирование конфигурации сети, построенной по технологии Ethernet (стандарты 10Base-T, 100Base-T, 1000Base-T, 10GBase-T).
- 2) Комплексное тестирование WLAN на базе стандарта IEEE 802.11 (Wi-Fi).
- 3) Определение коэффициента битовых ошибок при передаче данных по стандарту IEEE 802.15.1 (Bluetooth, Bluetooth LE).
- 4) Определение среднего значения скорости передачи данных к приемному терминалу при использовании технологий мобильной связи.
- 5) Тест с целью выбора прикладного протокола для Интернет Вещи относительно среднего времени отклика на запрос (RTT) при использовании протоколов MQTT, CoAP и HTTP.

Проведение натурного эксперимента

Для апробации предлагаемых тестовых спецификаций был проведен натурный эксперимент на базе модельной сети лаборатории Интернета Вещей СПбГУТ [7, 8], посвященный тестированию протоколов MQTT, CoAP и HTTP относительно времени отклика сервера на запрос. Следовательно, в ходе теста нужно отправлять запросы на сервер и отслеживать значения RTT, которые в дальнейшем необходимо проанализировать, и выявить наиболее подходящий



протокол для использования в данной Интернет Вещи. Результаты проведенного эксперимента отражены на рисунке 6, который показывает, что наименьшее время отклика наблюдается при использовании протокола CoAP.

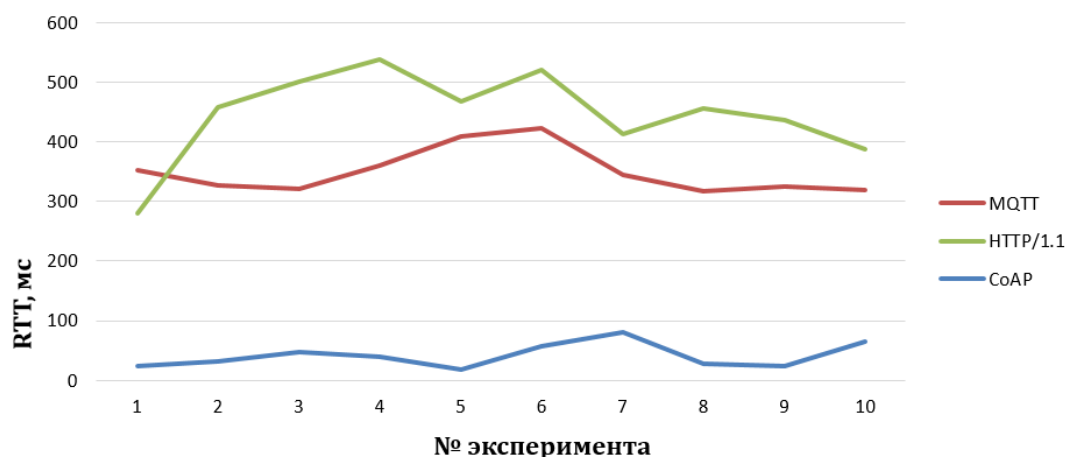


Рис. 6. Результаты проведенного эксперимента

CoAP действительно является хорошим решением для M2M-коммуникаций в Интернете Вещей. Данный протокол достаточно легковесный и быстрый, к тому же имеет различные опции. Но к сожалению, клиентская часть в CoAP не может быть реализована при помощи обычных web-страниц, написанных на языке JavaScript, вследствие чего приходится использовать дополнительные инструменты, например, Corper. Также программная реализация CoAP-сервера намного сложнее, чем у MQTT и HTTP.

Заключение

В статье были рассмотрены различные виды и методы тестирования Интернет Вещей. Данные методы и тестовые спецификации могут быть использованы при проведении тестирования Интернет Вещей для обеспечения их стабильной работы. На базе одной из тестовых спецификаций проведен натурный эксперимент и представлены его результаты.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта N15-07-09431a «Разработка принципов построения и методов самоорганизации для летающих сенсорных сетей».

Литература

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с. ISBN 978-5-86983-318-1.
2. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
3. Васильев А. Б., Тарасов Д. В., Андреев Д. В., Кучерявый А. Е. Тестирование сетей связи следующего поколения. М. : ФГУП ЦНИИС, 2008. 144 с.
4. Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering. 2016. Vol. 348. PP. 485–494.
5. Кулик В. А., Киричек Р. В., Кучерявый А. Е. Программно-аппаратный комплекс для тестирования устройств Интернета Вещей // Информационные технологии и телекоммуникации. 2015. № 4 (12). С. 67–76. URL: <https://www.sut.ru/doci/nauka/review/4-15.pdf>



6. Кулик В. А., Киричек Р. В., Бондарев А. Н. Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы // Информационные технологии и телекоммуникации. 2015. № 1. С. 106–114. URL: <https://www.sut.ru/doci/nauka/review/1-15.pdf>

7. Киричек Р. В., Владыко А. Г., Захаров М. В., Кучерявый А. Е. Модельные сети для Интернета Вещей и программируемых сетей // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 17–26. URL: <https://www.sut.ru/doci/nauka/review/3-15.pdf>

8. Kirichek, R., Vladyko, A., Zakharov, M., Koucheryavy, A. Model Networks for Internet of Things and SDN // 18th International Conference on Advanced Communication Technology (ICTACT). 2016. pp. 76–79. URL: http://icact.org/upload/2016/0186/20160186_finalpaper.pdf

References

1. Koucheryavy, A. E., Prokopiev, A. V., Koucheryavy, E. A. Self-Organizing Networks. SPb. : Lubavich, 2011. 312 p. ISBN 978-5-86983-318-1.

2. Koucheryavy, A. E. The Internet o Things // *Electrosvyaz*, 2013. No. 1. pp. 21–24.

3. Vasiliev, A. B., Tarasov, D. V., Andreev, D. V., Koucheryavy, A. E. Testing of Next Generation Networks. M. : FGUP ZNIIS, 2008. 144 p. ISBN 5-00-000834-0.

4. Kirichek, R., Koucheryavy, A. Internet of things laboratory test bed // *Lecture Notes in Electrical Engineering*, 2016. Vol. 348. pp. 485–494.

5. Kulik, V. A., Kirichek, R. V., Koucheryavy, A. E. Hardware-Software Complex for Testing Internet of Things Devices // *Telecom IT*. 2015. No. 4 (12). pp. 67–76. URL: <https://www.sut.ru/doci/nauka/review/4-15.pdf>

6. Kulik, V. A., Kirichek, R. V., Bondarev, A. N. Research Methods Wireless Channel of Internet of Things in other Networks Interference // *Telecom IT*. 2015. No. 1. pp. 106–114. URL: <https://www.sut.ru/doci/nauka/review/1-15.pdf>

7. Kirichek, R. V., Vladyko, A. G., Zakharov, M. V., Koucheryavy, A. E. Model Networks for Internet of Things and SDN // *Telecom IT*. 2015. No. 3 (11). pp. 17–26. URL: <https://www.sut.ru/doci/nauka/review/3-15.pdf>

8. Kirichek, R., Vladyko, A., Zakharov, M., Koucheryavy, A. Model Networks for Internet of Things and SDN // 18th International Conference on Advanced Communication Technology (ICTACT). 2016. pp. 76–79.

Долгушев Роман Андреевич

– магистрант, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, dexter.m.1969@gmail.com

Киричек Руслан Валентинович

– кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, kirichek@sut.ru

Кучерявый Андрей Евгеньевич

– доктор технических наук, профессор, заведующий кафедрой, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, akouch@mail.ru

Dolgushev Roman

– undergraduate, SPbSUT, St. Petersburg, 193232, Russian Federation, dexter.m.1969@gmail.com

Kirichek Ruslan

– Ph.D., assistant professor, SPbSUT, St. Petersburg, 193232, Russian Federation, kirichek@sut.ru

Koucheryavy Andrey

– D.Sc., professor, head of the Department, SPbSUT, St. Petersburg, 193232, Russian Federation, akouch@mail.ru

