DOI 10.37882/2223–2966.2020.04.33

К ВОПРОСУ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ, ОСНОВАННЫХ НА КОНЦЕПЦИИ «ИНТЕРНЕТ ВЕЩЕЙ»

TO THE QUESTION OF TESTING INFORMATION SYSTEMS BASED ON THE CONCEPT OF "INTERNET OF THINGS"

M. Romanova
R. Nabiev

Summary. The article is devoted to testing systems based on the «Internet of Things» (IoT) concept. Discussed situation in the field of testing such systems, application possibilities are shown model-based testing for automatic generation of test cases and testing a model developed on the basis of an IoT system.

Keywords: Internet of things, testing, model-based testing.

Романова Мария Николаевна
Казанский национальный исследовательский технологический университет, г. Казань
mnromanova19@gmail.com
Набиев Рафит Ренатович
К.х.н., доцент, Казанский национальный исследовательский технологический университет, г. Казань
nabievrafit@mail.ru

Аннотация. Статья посвящена тестированию систем, основанных на концепции «Интернет вещей». Рассмотрено положение дел в области тестирования подобных систем, показаны возможности применения модельно-ориентированного тестирования для автоматической генерация тестовых ситуаций и тестирование модели, разработанной на основании системы «Интернет вещей».

Ключевые слова: интернет вещей, тестирование, модельно-ориентированное тестирование.

Введение

«Интернет вещей» (англ. Internet of Things, IoT) — это сеть или ассоциация между подключенными к Интернету объектами (интеллектуальными устройствами). Концепция интернета вещей позволяет объектам среды быть активными участниками жизни — используя Интернет-протокол (IP) они обмениваются информацией и взаимодействуют между собой как через проводные, так и через беспроводные (Wi-Fi, LTE, Bluetooth и т.д.) технологии. По информации Gartner [1], в 2017 году к IoT было подключено около 20 млрд. устройств, к 2025 году ожидается, что данная цифра возрастет до 75 млрд.

Одним из ключевых моментов применения IoT является совместимость между элементами сети. Прежде всего, стоит отметить функциональную совместимость — между объектами сети должен производиться бесперебойный обмен информацией. Также требуется учитывать качество соединения между объектами, протоколы маршрутизации и методы сжатия информации и т.д. К тому же с ростом количества устройств, подключенных к IoT, будет генерироваться все бОльший объем информации, который иметь свойства, которыми характеризуются традиционные виды данных (аудио-видео информация и т.д.). Перечисленные особенности не позволяют разработчикам программного обеспечения применять обычные методы тестирования относительно систем, основанных на концепции Io T.

Таким образом, приобретает актуальность вопрос разработки специфичных методов и средств тестирования систем, основанных на концепции Io T.

Проблемы и основные методы тестирования систем на основании IoT

Тестирование является последней стадией перед вводом системы в эксплуатацию. При этом данный этап подвержен всем задержкам, накопленным в процессе разработки всей системы. На тестирование закладывается 30–50% бюджета проекта. Все эти факты свидетельствуют о важности этапа тестирования, а также показывают, что тестирование — элемент для возможных улучшений.

Перед тестированием систем, основанных на концепции IoT, надо осознавать, что предстоит тестировать не просто Web-сайт, сервер или мобильное приложение. В большинстве случаев разработчики даже не предполагают, с какими тестовыми ситуациями они столкнутся. Все это обусловлено тем, что существует множество аспектов функционирования системы, которые необхо-

димо проверить: функциональная совместимость, безопасность, производительность и т.д.

Среди факторов, которые отличают тестирование классических систем и IoT-тестирование, можно выделить следующие: 1. сложность экосистемы; 2. многоуровневая архитектура, различные типы конечных устройств; 3. большой объем разнообразных данных, которые обрабатываются и передаются с различной скоростью; 4. масштабируемость методов тестирования на подобные системы; 5. безопасность данных.

Тестирование таких составляющих, как конфиденциальность и безопасность IoT-систем нашли широкое освещение в литературе [2–11].

Можно найти несколько исследований, в которых обсуждается производительность систем, основанных на концепции IoT [12]. Как правило, исследования производительности более сфокусированы на функциональной совместимости элементов системы, чем на сквозной производительности с точки зрения пользователя. В качестве отдельной области следует выделить тестирование протокола Io T. Тут используется целый спектр методов, которые описаны: проверка на соответствие [13], проверка на случайность [14], статистическая проверка [15], формальная проверка [16].

Однако гораздо меньше работ в области методологий системного функционального тестирования и обеспечения качества работы разработанной системы. Можно с уверенностью утверждать, что эта область обладает большим потенциалом для будущих исследований.

Для систем, основанных на IoT, требуется новая и специфичная для конкретной предметной области парадигма тестирования, поскольку взаимодействие с датчиками и исполнительными механизмами изменяет способ проведения испытаний. Основная цель заключается в расширении возможностей тестирования благодаря учету аспектов взаимодействия с физической средой. Основная задача заключается в том, чтобы обеспечить автоматизированный процесс разработки и выполнения тестов для упрощения процесса тестирования.

До настоящего времени в области IoT часто применялись ручные подходы к тестированию [17]. Мы предлагаем для IoT-тестирования технологию, которая все больше применяется в промышленности для исключения ошибок, улучшения качества и снижения затрат: модельно-ориентированное тестирование или тестирование на основе моделей (MBT, от англ. model-based testing).

Модельно-ориентированное тестирование — это автоматическая генерация тестовых ситуаций и тестирование модели, разработанной на основании IoT-системы. Несмотря на сложный этап разработки модели IoT-системы, MBT предлагает существенные преимущества по сравнению с традиционными методами тестирования программного обеспечения: 1. нет необходимости разрабатывать новые тестовые наборы при добавлении дополнительных функций системы; 2. большое тестовое покрытие; 3. разработка различных блоков системы не зависит от текущего тестирования, поэтому эти действия могут выполняться различными членами команды одновременно и т.д.

Тестирование на основе моделей рассматривается как легковесный формализованный (работает на основе машиночитаемой спецификации — модели системы) метод тестирования программного обеспечения. Основное различие между легковесными или тяжеловесными методами тестирования состоит в разнице между «достаточной уверенностью» и «абсолютной уверенностью». В настоящее время цена за «абсолютную уверенность» очень высока — это требует существенные временные и финансовые затраты. Это приводит к тому, что тяжеловесные формализованные методы практически невозможно внедрить в тестирование реальных проектов. Подход MBT считается легковесным, потому что в отличие от других формализованных методов, не ставит своей целью математическое доказательство того, что реализация соответствует спецификациям при всех возможных обстоятельствах. Модельно-ориентированное тестирование обеспечивает систематическую генерацию набора тестов (тестовых случаев), которые при запуске обеспечат достаточное тестовое покрытие IoT-системы.

Обзор литературы показывает, что ни одна из существующих в настоящее время моделей не может быть применена непосредственно к тестированию сервисов на основе Io T.

Резюмируя можно заключить, что для IoT-систем актуальность принимает разработка методологии тестирования, которая будет охватывать аспекты моделирования поведения системы, предоставлять средства для эмуляции их подключенных ресурсов (датчиков и исполнительных механизмов) и обеспечивать возможность преобразования этих моделей в тестовые случаи.

Таким образом, возникает вопрос для исследования, как применять подход тестирования на основе моделей для обеспечения процесса эффективного тестирования IoT, в частности, автоматизации функционального системного тестирования. Решение данной задачи планируется решить в следующем, практическом блоке исследовательской работы.

ЛИТЕРАТУРА

1. Leading the Io T. Gartner Insights on How to Lead in a Connected World [Электронный ресурс] // 2017. URL:
2. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
3. Miroslav Bures, Tomas Cerny, Bestoun S. Ahmed. Internet of Things: Current Challenges in the Quality Assurance and Testing Methods [Электронный ресурс] // 2018. URL:
4. https://arxiv.org/ftp/arxiv/papers/1805/1805.01241.pdf
5. Xu T., Wendt J. B., Potkonjak M. Security of IoT systems: Design challenges and opportunities: сб. научных трудов Международной конференции по автоматизированному дизайну / IEEE, 2014, С. 417–423.
6. Lin H. and Bergmann N. W. IoT privacy and security challenges for smart home environments // Information, 2016, С. 44.
7. Agrawal V. Security and privacy issues in wireless sensor networks for healthcare: сб. научных трудов Международного саммита, посвященного Интернету Вещей IoT360 // In Internet of Things. User-Centric IoT, Springer, 2015, С. 223–228.
8. Bertino E., Choo K. K. R., Georgakopolous D., Nepal, S. Internet of Things (IoT): Smart and secure service delivery // ACM Transactions on Internet Technology (TOIT), 2016, С. 22.
9. Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks, 2015, С. 146–164.
10. Десницкий В., Котенко И. Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge // Journal of Ambient Intelligence and Humanized Computing, Springer, 2016, С. 705–719.
11. Fernández-Caramés T. M., Fraga-Lamas P., Suárez-Albela M., Castedo L. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications // Sensors, 2017, С. 28.
12. Sicari S., Rizzardi A., Miorandi D., Cappiello C., Coen-Porisini A. A secure and quality-aware prototypical architecture for the Internet of Things // Information Systems, 2016, С. 43–55.
13. Ashraf Q. M., Habaebi M. H. Autonomic schemes for threat mitigation in Internet of Things // Journal of Network and Computer Applications, 2015, С. 112–127.
14. Batalla J. M., Gajewski M., Latoszek W., Krawiec, P. Implementation and performance testing of ID layer nodes for hierarchized IoT network: сб. научных трудов Азиатской конференции по интеллектуальным системам и базам данных // Springer, 2015, С. 463–472.
15. Xie H., Wei L., Zhou J., Hua X. Research of conformance testing of low-rate wireless sensor networks based on remote test method: сб. научных трудов 5-й международной конференции по вычислительным и информационным наукам (ICCIS) // IEEE, 2013, С. 1396–1400.
16. Göhring M., Schmitz, R. On randomness testing in physical layer key agreement // IEEE, 2015, С. 733–738.
17. Bae H., Sim S. H., Choi Y., Liu L. Statistical verification of process conformance based on log equality test: сб. научных трудов 2-й международной конференция по сотрудничеству и интернет-вычислениям (CIC) // IEEE, 2016, С. 229–235.
18. Silva D. S., Resner D., de Souza R. L., Martina, J. E. Formal Verification of a Cross-Layer, Trustful Space-Time Protocol for Wireless Sensor Networks // In Information Systems Security, Springer, 2016, С. 426.
19. Dias Neto A. C., Subramanyan R., Vieira M., Travassos G. H. A survey on model-based testing approaches: a systematic review // WEASELTech, 2007, С. 31–36.

Журнал «Современная наука: актуальные проблемы теории и практики»