УДК 004.822
DOI:10.25729/ESI.2023.30.2.004

Построение цифрового профиля устройств Интернета вещей

Исаева Ольга Сергеевна

Институт вычислительного моделирования СО РАН,
Россия, Красноярск, *isaeva@icm.krasn.ru*

Аннотация. В работе выполнена формализация семантического представления обобщённого цифрового профиля IoT-устройств, содержащая знания об архитектурных решениях сети Интернета вещей, критерии анализа сетевой активности участников информационного обмена в схеме «Издатель-Брокер- Подписчик» и характеристики контролируемых физических явлений. Для выбора понятий, которые легли в основу формализации, рассмотрены актуальные исследования в направлениях кибербезопасности и анализа данных Интернета вещей. Сформирована онтология, содержащая концепты предметной области, отражающие понятия рассматриваемой технологии, их взаимосвязи и экземпляры концептов, описывающие реализацию сети Интернета вещей в Красноярском научном центре. Рассматриваемая сеть предназначена для мониторинга технологических помещений с телекоммуникационным оборудованием и включает измерительные устройства, телекоммуникационную среду, виртуальные и физические сервера и прикладные программные решения. Каждый из экземпляров объектов в онтологии имеет своё цифровое представление в базах данных, содержит результаты измерений, статистические и спектральные характеристики данных и предназначен для решения практических задач.

Ключевые слова: интернет вещей, профилирование устройств IoT, протокол обмена сообщениями, Message Queuing Telemetry Transport (MQTT), онтология, частотный анализ

Цитирование: Исаева О.С. Построение цифрового профиля устройств Интернета вещей / О.С. Исаева // Информационные и математические технологии в науке и управлении. – 2023. – № 2(30). – С. 36-44. – DOI:10.25729/ESI.2023.30.2.004

Введение. В современных направлениях развития информационного общества выделяется тенденция обеспечения передовых сервисов и услуг за счёт организации связи между физическими или виртуальными объектами на основе совместимых информационных и коммуникационных технологий. Концепцией, обеспечивающей такие решения, является технология Интернета вещей (Internet of Things – IoT), поддерживающая информационное взаимодействие распределённых устройств и приложений [1]. Широкая популярность Интернета вещей, мобильность строящихся инфраструктур наряду с неоднородностью сценариев их использования требуют создания специализированных подходов к обеспечению надёжности получения, хранения, обработки и анализа больших объёмов данных. В IoT-сетях используются облегчённые протоколы межсетевого взаимодействия, имеющие ограниченные возможности аутентификации и контроля безопасности, что является причиной развития сетевых атак, направленных на маршрутизацию между их функциональными уровнями. Исследования по обеспечению безопасности вычислительных ресурсов и данных, как правило, ограничиваются анализом сетевого трафика, генерируемого и собираемого устройствами. Ввиду динамичности источников атак и постоянно меняющихся характеристик аномального поведения устройств такого автоматического контроля оказывается недостаточно.

Целью данной работы является создание обобщённого цифрового профиля IoT-устройств, объединяющего как фактические характеристики устройств, сетевых протоколов, архитектурные особенности инфраструктур, так и фактографические данные, журналы сетевого трафика, аномалии контролируемых физических явлений. Новизна подхода заключается в том, что профили устройств, отражающие частоту, периодичность передачи данных, наблюдаемые задержки в сети, размеры пакетов, флаги качества обслуживания, показатели времени установки и удержания соединений и другие параметры, отвечающие за сетевую активность, расширены показателями, построенными в результате анализа и агрегирования собираемых

данных, частотными характеристиками протекающих событий, трендами и критическими значениями, ограничивающими измеряемые показатели.

Исследование проводится на базе сети Интернета вещей, выполняющей мониторинг технологических помещений с телекоммуникационным оборудованием [2] подразделения Красноярского научного центра СО РАН. Построенные цифровые профили позволят выявлять предпосылки аномального поведения элементов сети, выходы из строя или изменения режимов работы оборудования, и строить критерии превентивной защиты в зависимости от настроек политики безопасности серверов.

1. Обзор существующих подходов к исследованию IoT. Несмотря на то, что, по данным аналитических агентств, объем IoT уже оценивается диапазоном от 8 до 30 млрд устройств и прогнозируется их дальнейший существенный рост, универсального определения понятия Интернета вещей не существует [3]. Различаются архитектурные и технологические подходы к организации информационно-телекоммуникационной среды Интернета вещей. Проводимые исследования выполняются совместно специалистами различных областей и включают решения задач сетевого администрирования, кибербезопасности, искусственного интеллекта, анализа больших данных и пр. Для обеспечения семантической связности таких исследований требуется единая информационная платформа, формирующая унифицированный словарь концептов и их взаимосвязей на основе знаний предметной области, отражающий различные аспекты технологии Интернета вещей.

Для выявления понятий, которые бы легли в основу формализации, рассмотрены актуальные исследования в направлениях кибербезопасности и анализа данных Интернета вещей. В качестве основного определения Интернета вещей выбрано его представление как динамической глобальной сетевой инфраструктуры пространственно-распределённых узлов, оснащённых встроенными средствами для взаимодействия друг с другом или с внешней средой, способных измерять, понимать и изменять своё окружение [4]. Сетевая архитектура IoT включает функциональные уровни: сенсорный, транспортный, сервисный и прикладной [5]. В качестве протокола обмена данными в настоящем исследовании выбран Message Queue Telemetry Transport (MQTT) [6], поддерживающий взаимодействие логических сущностей со следующими ролями: Издатель (Publisher) – источник данных, устройство IoT, формирующее сообщение о состоянии наблюдаемых объектов; Брокер (Broker) – программное обеспечение, получающее и распределяющее сообщения (например, Mosquitto MQTT) и Подписчик (Subscriber) – приложение (или устройство), получающее данные по заданным тематическим подпискам [7]. Перечисленные роли распределяются по уровням архитектуры IoT следующим образом: на сенсорном уровне размещаются Издатели (датчики). Транспортный уровень содержит шлюзы и сети передачи данных, через которые от устройств IoT поступают данные. На сервисном уровне устанавливаются Брокеры, которые консолидируют данные, характеризующиеся большим объёмом, разнообразием и частотой генерации [8]. Прикладной уровень формируется Подписчиками – программным обеспечением, решающим задачи предметной области.

Исследование безопасности различных уровней сетевой архитектуры IoT предполагает построение профилей умных устройств. Профили устройств включают статистические характеристики сеансов связи, интенсивность и продолжительность передачи пакетов данных [9, 10]. Особенности протоколов для сети Интернета вещей и проблемы с ограничениями прав доступа к устройствам рассматриваются для информационной схемы «Издатель-Брокер-Подписчик» в [11]. Помимо структурированных данных сеансов связи выполняются исследования журналов обращений [12, 13]. Построены сценарии сетевого поведения при различных видах атак и предложено для обнаружения и смягчения последствий атак выполнять моделирование поведения законных клиентов IoT [14].

Выявление аномального трафика выполняется методами машинного обучения [15, 16], однако большие объёмы данных создают проблемы для их применения. В [17] представлен автоматизированный выбор признаков, необходимых и достаточных для обучения и настройки моделей. Рассмотрены публичные наборы данных для MQTT и показатели, которые они содержат для поиска аномалий методами искусственного интеллекта в контексте IoT [18]. Системы упреждающего поведения при эксплуатации промышленных устройств исследуют временные ряды данных мониторинга и выполняют в них поиск и диагностику аномалий [19, 20]. Такой подход интегрируется в систему безопасности совместно с другими методами анализа.

Из проведённого обзора выделены характеристики, описывающие схему и участников информационного взаимодействия, показатели сетевой активности, настройки политик безопасности, свойства процессов, контролируемых датчиками IoT и прецеденты аномального поведения.

2. Формализация профиля устройств IoT. Для формализации профиля устройств Интернета вещей и интеграции выделенных понятий, свойств и отношений построена онтология. В качестве программных инструментов выбран свободный открытый редактор онтологий и баз знаний Protégé, поддерживающий OWL формат и имеющий web-ресурс для совместной работы группы исследователей. Под онтологией в используемом редакторе понимается формальное явное описание понятий (классов), их свойств (функций и атрибутов), ограничений на свойства и экземпляров классов [21]. Инструмент поддерживает категорированную иерархическую структуру элементов, предоставляет методы контроля зависимостей, восстановления скрытых знаний и построения семантических запросов.

Построенная онтология отражает логические структуры цифрового профиля устройства IoT. На верхнем уровне иерархии выделены классы – участники информационного обмена. Графическое представление классов, показывающее основные характеристики и настройки, приведено на рисунках 1-3.

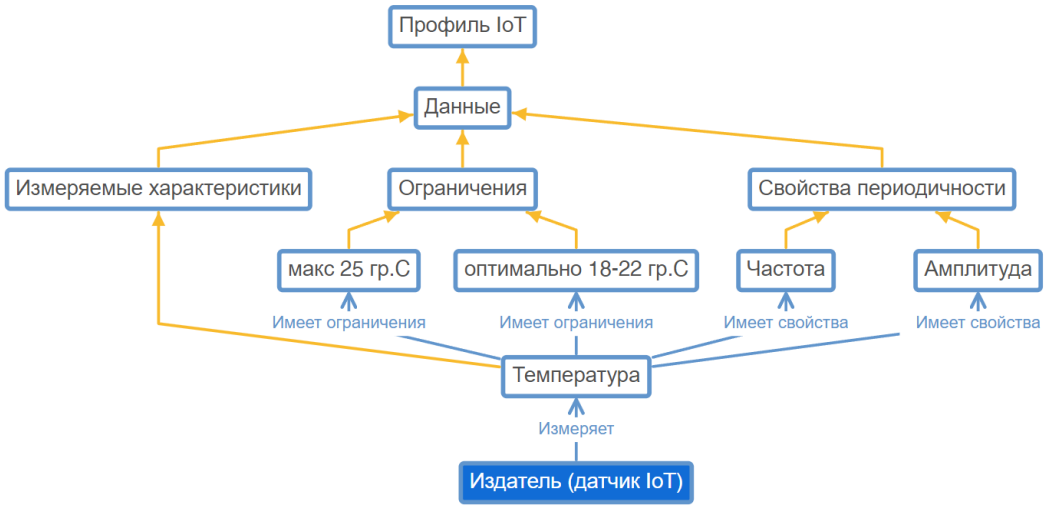

Рис. 1. Графическое представление класса «Издатель»

Онтология «Профиль IoT» содержит сущности и атрибуты, связанные с реализацией сети Интернета вещей в Красноярском научном центре. Издатели в текущей схеме представлены измерительными устройствами CL-210-E (производства ICP DAS), выполняющими мониторинг показателей температуры, влажности, точки росы и концентрации мелкодисперсной пыли (PM2.5). Они размещены в специализированных технологических помещениях с телекоммуникационным оборудованием. В онтологии описаны характеристики: размещение, точность измерения, периодичность передачи данных, даты ввода в эксплуатацию

и поверки (при необходимости), граничные условия на измеряемые параметры и частотные характеристики данных.

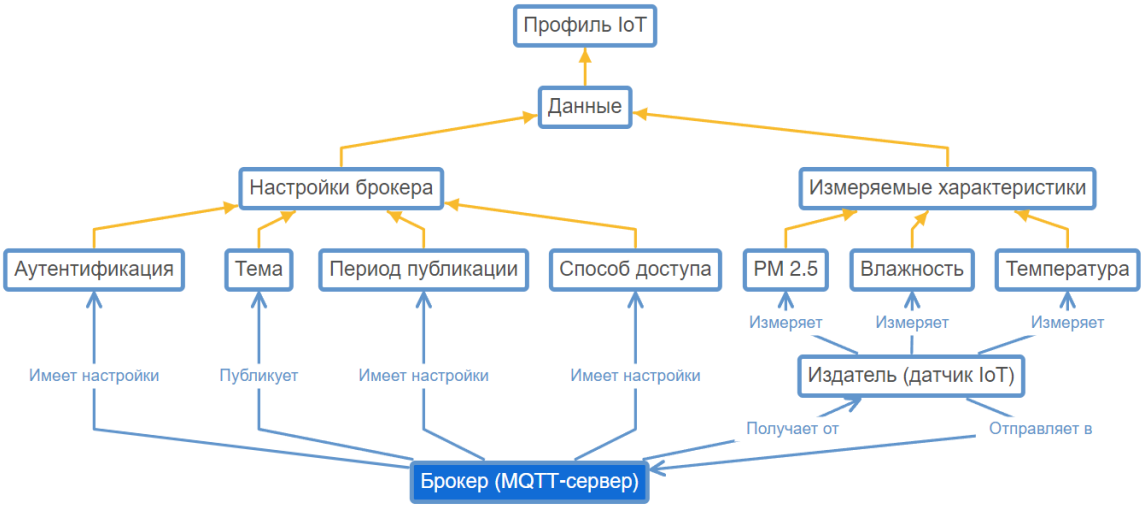

Рис. 2. Графическое представление класса «Брокер»

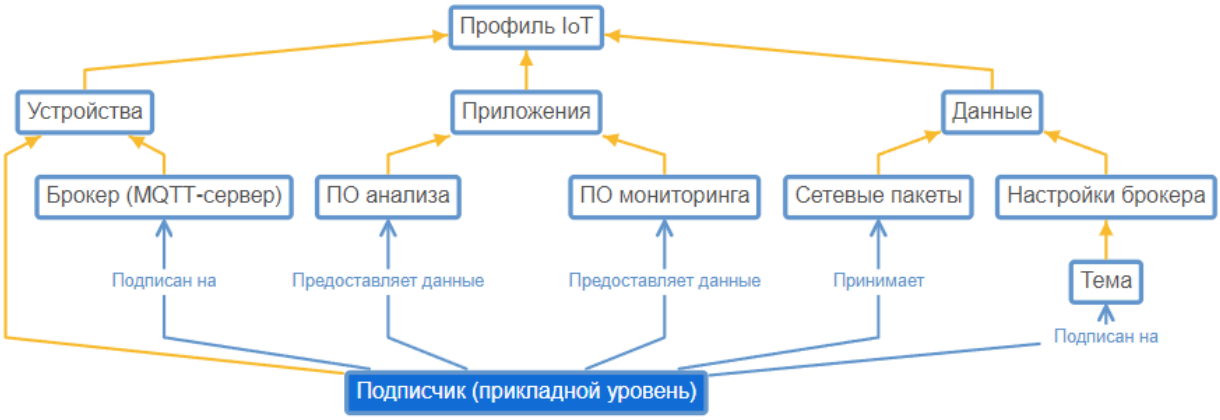

Рис. 3. Графическое представление класса «Подписчик»

Транспортный уровень сети IoT реализуется на основе существующей инфраструктуры корпоративной сети Красноярского научного центра. Для реализации функций брокеров данных развёрнут кластер Kubernetes (K8s) на 10 узлов, включающий несколько физических серверов и виртуальных машин с системой виртуализации Hyper-V. На всех узлах использована ОС Ubuntu Server 20.04. Централизованное управление жизненными циклами контейнеров выполняется на платформе оркестрации Rancher. Брокеры получают результаты измерений от источников данных, обрабатывают их и размещают в базах, а также ведут сетевые журналы, содержащие сведения об обращениях к данным. В настоящий момент происходит наполнение онтологии атрибутами, отражающими особенности сетевой активности, характеристики политик безопасности и данные журналов [22].

Построенная онтология консолидирует знания специалистов предметной области и позволяет решать практические задачи. Например, одной из задач, для которых предназначен профиль устройств IoT, является выбор настроек Брокера данных.

3. Выбор настроек брокера данных IoT. Изменение развёрнутой структуры сети IoT требует выбора настроек безопасности и параметров выдачи данных. Графическое представление классов, экземпляров и отношений, описывающее решение этой задачи, приведено на рисунке 4.

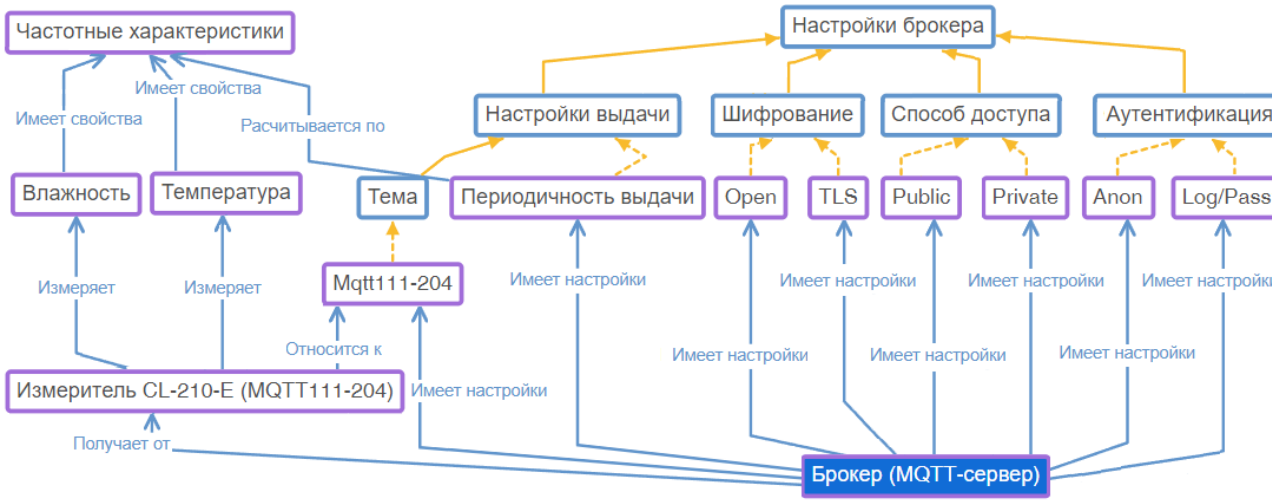

Рис. 4. Графическое представление класса «Настройки брокера»

Варианты настройки Брокеров включают способы доступа (видимость только из внутренней корпоративной сети – Private или из сети Internet – Public), аутентификации (с авторизацией – Log/Pass или без авторизации – Anon), шифрования (протокол Transport Layer Security – TLS или без шифрования – Open).

Кроме того, в онтологии описан способ выбора периодичности публикации Брокером данных, получаемых от издателей [23]. Издатели собирают данные в технологических помещениях со сложным коммуникационным и вычислительным оборудованием, обладающим повышенной теплоотдачей, снабжённых системами кондиционирования. Требуется обеспечить этими данными Подписчиков, в том числе и мобильных, имеющих ограниченные ресурсы на обработку и хранение информации. Для этого необходимо сократить объем рассылок и уменьшить загрузку каналов связи при сохранении адекватности представления протекающих процессов. Исследование показало, что процессы имеют периодический характер и для создания режима выдачи данных, при котором частота их обновления соответствует скорости протекания событий, предложено выполнять анализ частотных характеристик, собираемых Издателями данных.

Для пояснения подхода возьмём набор измерений температуры в N отсчётах (рисунок 5). Для определения частотных характеристик данных рассчитаем параметры гармонического ряда методом дискретного преобразования Фурье [24]. В общем случае свойство периодичности достигается путём повторения рассматриваемых данных с периодом NT, где $T = (t_{n+1} - t_n)$ – период дискретизации, $n = [0, N\text{-}1]$, N – количество отсчётов.

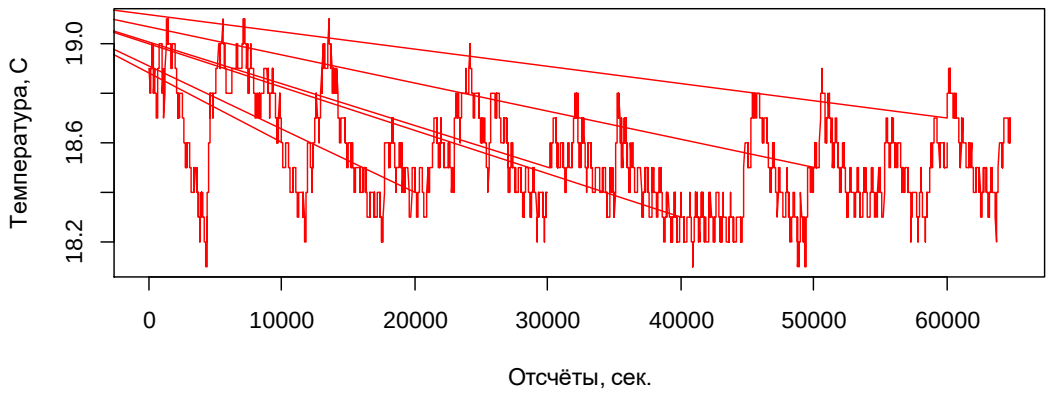

Рис. 5. График измерений температуры помещения в наблюдаемых отсчётах

Результат разложения приведён на рисунке 6, полученные весовые коэффициенты являются комплексным спектром периодического сигнала.

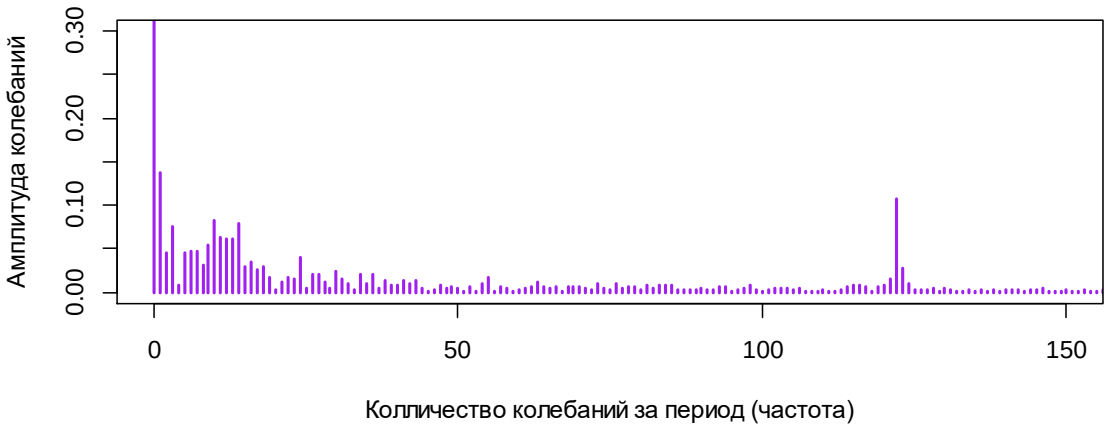

Рис. 6. Частотный спектр анализируемых данных

Если рассмотреть полученный частотный спектр, то его первая гармоника отражает постоянную составляющую данных, остальные характеризуют периодичность сигнала. Выберем максимальную амплитуду среди значений, превышающих порог точности измерений, рассчитаем соответствующую частоту колебаний. Воспользовавшись теоремой Котельникова [25], определим, при каких условиях сигнал может быть однозначно восстановлен по его дискретным отсчётам. На каждое колебание сигнала должно приходится как минимум 2 отсчёта. Затем рассчитаем период дискретизации. Выдача брокером данных должна происходить с полученным периодом.

Такая настройка выполняется по каждому Издателю для каждого Брокера и позволяет обеспечить Подписчиков результатами наблюдений за протекающими в технологических помещениях событиями в соответствии с динамикой изменения данных. Кроме того, изучение частотного спектра позволяет выявлять аномалии в наблюдаемых процессах.

Заключение. Проведённое исследование по формализации знаний и выделению значимых факторов, определяющих цифровые профили IoT-устройств, является основой для описания сети Интернета вещей, функционирующей в Красноярском научном центре. Структура цифрового профиля задана с помощью онтологии, которая содержит объекты, описывающие понятия предметной области, связи, экземпляры объектов, свойства данных, в том числе: диапазоны изменения и критические значения, ограничивающие атрибуты элементов онтологии, настройки архитектуры сети и устройств, выполняющих сбор, передачу данных, их хранение, обработку и пр.

Каждый из экземпляров объектов в онтологии имеет своё цифровое представление в базах данных, включая результаты измерений, статистические и спектральные характеристики данных. В обобщённый цифровой профиль входят дополнительные характеристики: площадь и объем помещений, настройки циклов работы систем кондиционирования, пиковые значения тепловыделения оборудования, факторы цикличности нагрузки (сезонность, время суток) и пр. Профиль наполняется расчётными показателями, отвечающими за сетевую активность элементов IoT в схеме «Издатель-Брокер-Подписчик» при различных настройках политик безопасности и флагах качества обслуживания, в том числе статистикой размеров пакетов, временем установки и удержания соединений и др.

Построенные цифровые профили позволят выявлять предпосылки аномального поведения элементов сети, выходы из строя или изменения режимов работы оборудования и строить критерии реагирования и превентивной защиты, что является одним из аспектов обеспечения надёжности инфраструктуры Интернета вещей.

Благодарности. Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (Соглашение 075-02-2023-912).

Список источников

1. Дикий Д.И. Протокол передачи данных MQTT в модели удалённого управления правами доступа для сетей Интернета / Д.И. Дикий, В.Д. Артемьева // Научно-технический вестник информационных технологий, механики и оптики, 2019. – Т. 19(1). – С. 109-117.
2. Исаева О.С. Создание инструментов сбора данных для анализа аспектов безопасности Интернета вещей / О.С. Исаева, Н.В. Кулясов, С.В. Исаев // Информационные и математические технологии в науке и управлении, 2022. – № 3(27). – С. 113-125. – DOI: 10.38028/ESI.2022.27.3.011.
3. Alam T. A reliable communication framework and its use in Internet of Things (IoT). International journal of scientific research in computer science, engineering and information technology, 2018, no. 3(5), pp. 450-456.
4. Rozik A.S., Tolba A.S., El-Dosuky M.A. Design and implementation of the sense Egypt platform for real-time analysis of IoT Data Streams. Advances in Internet of Things, 2016, no. 6(4), pp. 66-91.
5. Javed A., Heljanko K., Buda A., Främling K. CEFIoT: A fault-tolerant IoT architecture for edge and cloud. IEEE World forum on Internet of things, 2018, pp. 813-818, DOI:10.1109/WF-IoT.2018.8355149.
6. Patel C., Doshi N. A Novel MQTT security framework in generic IoT model. Procedia Computer Science, 2020, no. 171, pp. 1399-1408, DOI:10.1016/j.procs.2020.04.150.
7. Dizdarević J., Carpio F., Jukan A., Masip-Bruin X. A Survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. ACM Computing Surveys, 2019, no. 1(1).
8. Azad P., Navimipour N.J., Rahmani A.M. The role of structured and unstructured data managing mechanisms in the Internet of things. Cluster Computing, 2020, no. 23, pp. 1185-1198, DOI:10.1007/s10586-019-02986-2.
9. Татарникова Т.М. Обнаружение атак в сетях интернета вещей методами машинного обучения. / Т.М. Татарникова, П.Ю. Богданов // Информационно-управляющие системы, 2021. – № 6. – С. 42-52. – DOI:10.31799/1684-8853-2021-6-42-52.
10. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Breitenbacher D., Shabtai A., Elovici Y.N. BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing. Special Issue – Securing the IoT, 2018, no. 17(3), pp. 12-22.
11. Munshi A. Improved MQTT secure transmission flags in smart homes. Sensors, 2022, no. 22(6), p. 2-15.
12. Isaev S.V., Kononov D.D. Analysis of the dynamics of Internet threats for corporate network web services. CEUR Workshop Proceedings, 2021, no. 3047, pp. 71-78, DOI:10.47813/sibdata-2-2021-10.
13. Kononov D.D., Isaev S.V. Development of secure automated management systems based on web technologies. IOP Conference Series: Materials Science and Engineering, 2019, no. 537(5), DOI: 10.1088/1757–899X/537/5/052024.
14. Haripriya A., Kulothungan K. Secure-MQTT: An efficient fuzzy logic-based approach to detect dos attack in MQTT protocol for Internet of Things. J. Wirel. Commun. Netw, 2019.
15. Bhattacharyya D.K., Kalita J.K. Network anomaly detection: A machine learning perspective. CRC Press, 2014.
16. Nassif A.B., Talib M.A., Nasir Q., Dakalbab F.M. Machine learning for anomaly detection: A systematic review. IEEE Access, 2021, no. 9, pp. 78658-78700.
17. Omar S., Ngadi A., Jebur H. Machine learning techniques for anomaly detection: an overview. International Journal of Computer Applications, 2013, no. 79(2), pp. 32-41.
18. Dissanayake M.B. Feature engineering for cyber-attack detection in Internet of Things. International Journal of wireless and microwave technologies, 2021, no 6, pp. 46-54.
19. Vaccari I., Chiola G., Aiello M., Mongelli M. MQTTset, a New dataset for machine learning techniques on MQTT. Sensors, 2020, no. 20, pp. 6578, DOI:10.3390/s20226578.
20. Cook A.A., Mısırlı G., Fan Z. Anomaly detection for IoT time-series data: a survey. IEEE Internet of Things Journal, 2020, no. 7(7). pp. 6481-6494.
21. Musen M.A. The Protégé project: A look back and a look forward. AI Matters. Association of Computing Machinery Specific Interest Group in Artificial Intelligence, 2015, no. 1(4), DOI: 10.1145/2557001.25757003.
22. Isaeva O.S., Kulyasov N.V., Isaev S.V. Creation of a simulation stand for studying of the internet of things' technologies. AIP Conference Proceedings, 2022, no. 2647, pp. 040030-1-040030-5, DOI:10.1063/5.0104342.
23. Исаева О.С. Формирование адаптивных рассылок брокера данных интернета вещей / О.С. Исаева, С.В. Исаев, Н.В. Кулясов // Информационно-управляющие системы, 2022. – № 5(120). – С. 23-31. – DOI:10.31799/1684-8853-2022-5-23-31.
24. Duhamel P., Vetterli M. Fast Fourier transforms: a tutorial review and a state of the art. Signal Processing, 1990, no. 19, pp. 259-299.
25. Зиатдинов С.И. Восстановление сигнала по его выборкам на основе теоремы отсчётов Котельникова / С.И. Зиатдинов // Известия вузов. Приборостроение, 2010. – №. 53(5). – С. 44-47.

Исаева Ольга Сергеевна. *Старший научный сотрудник отдела Красноярского математического центра Института вычислительного моделирования СО РАН, доктор технических наук. Область научных интересов:*

методы искусственного интеллекта, анализ данных, цифровые двойники. SPIN-код: 8412-5807, ORCID: 0000-0002-5061-6765, Researcher ID: A-8905-2018, isaeva@icm.krasn.ru, г. Красноярск, ул. Академгородок, д. 50, стр. 44, каб. 209.

UDC 004.822
DOI:10.25729/ESI.2023.30.2.004

Building a digital profile of IoT devices

Olga S. Isaeva

Institute of Computational Modeling of SB RAS, Russia, Krasnoyarsk, *isaeva@icm.krasn.ru*

Abstract. The paper formalizes the semantic representation of the common digital profile of IoT devices, containing knowledge about the architectural solutions of the Internet of Things, the criteria for analyzing the network activity of information exchange participants in the Publisher-Broker-Subscriber scheme and the characteristics of controlled physical processes. In order to select the concepts underlying the formalization, current research in the areas of cybersecurity and data analysis of the Internet of Things are considered. The author has formed an ontology containing the concepts of the subject area and their relationships, reflecting IoT-technology and instances of concepts that describe the implementation of the Internet of Things network in the Krasnoyarsk Scientific Center. The described network is used to monitor technological rooms with telecommunications equipment and includes measuring devices, telecommunications environment, virtual and physical servers, and application software. The instances of objects in the ontology have its own digital representation in databases, contains measurement results, statistical and spectral characteristics of data, and is used to solve practical problems.

Keywords: Internet of Things, IoT device profiling, Message Queuing Telemetry Transport (MQTT), messaging protocol, ontology, frequency analysis

Acknowledgements: This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation in the framework of the establishment and development of regional Centers for Mathematics Research and Education (Agreement No. 075-02-2023-912).

References

1. Dikii D.I., Artemeva V.D. Protokol peredachi dannyh MQTT v modeli udalyonnogo upravleniya pravami dostupa dlya setej Interneta [MQTT data protocol in remote access control management model for Internet networks]. Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki [Scientific and technical journal of information technologies, Mechanics and Optics], 2019, no. 19(1), pp. 109-117, DOI: 10.17586/2226-1494-2019-19-1-109-117.
2. Isaeva O.S., Kulyasov N.V. Isaev S.V. Sozdanie instrumentov sbora dannyh dlya analiza aspektov bezopasnosti Interneta veshchej [Creating data collection tools to analyze security aspects Internet of Things]. Informacionnye i matematičeskie tehnologii v nauke i upravlenii [Informational and mathematical technologies in science and management], 2022, no. 3(27), pp. 113-125, DOI: 10.38028/ESI.2022.27.3.011.
3. Alam T. A reliable communication framework and its use in Internet of Things (IoT). International journal of scientific research in computer science, engineering and information technology, 2018, no. 3(5), pp. 450-456.
4. Rozik A.S., Tolba A.S., El-Dosuky M.A. Design and implementation of the sense Egypt platform for real-time analysis of IoT Data Streams. Advances in Internet of Things, 2016, no. 6(4), pp. 66-91.
5. Javed A., Heljanko K., Buda A., Främling K. CEFIoT: A fault-tolerant IoT architecture for edge and cloud. IEEE World forum on Internet of things, 2018, pp. 813-818, DOI:10.1109/WF-IoT.2018.8355149.
6. Patel C., Doshi N. A Novel MQTT security framework in generic IoT model. Procedia Computer Science, 2020, no. 171, pp. 1399-1408, DOI:10.1016/j.procs.2020.04.150.
7. Dizdarević J., Carpio F., Jukan A., Masip-Bruin X. A Survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. ACM Computing Surveys, 2019, no. 1(1).
8. Azad P., Navimipour N.J., Rahmani A.M. The role of structured and unstructured data managing mechanisms in the Internet of things. Cluster Computing, 2020, no. 23, pp. 1185-1198, DOI:10.1007/s10586-019-02986-2.

9. Tatarnikova T.M., Bogdanov P.Yu. Obnaruzhenie atak v setyah interneta veshchej metodami mashinnogo obucheniya [Intrusion detection in internet of things networks based on machine learning methods]. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2021, no. 6, pp. 42–52, DOI:10.31799/1684-8853-2021-6-42-52.
10. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Breitenbacher D., Shabtai A., Elovici Y.N. BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing. Special Issue – Securing the IoT, 2018, no. 17(3), pp. 12-22.
11. Munshi A. Improved MQTT secure transmission flags in smart homes. Sensors, 2022, no. 22(6), pp. 2-15.
12. Isaev S.V., Kononov D.D. Analysis of the dynamics of Internet threats for corporate network web services. CEUR Workshop Proceedings, 2021, no. 3047, pp. 71-78, DOI:10.47813/sibdata-2-2021-10.
13. Kononov D.D., Isaev S.V. Development of secure automated management systems based on web technologies. IOP Conference Series: Materials Science and Engineering, 2019, no. 537(5), DOI: 10.1088/1757–899X/537/5/052024.
14. Haripriya A., Kulothungan K. Secure-MQTT: An efficient fuzzy logic-based approach to detect dos attack in MQTT protocol for Internet of Things. J. Wirel. Commun. Netw, 2019.
15. Bhattacharyya D.K., Kalita J.K. Network anomaly detection: A machine learning perspective. CRC Press, 2014.
16. Nassif A.B., Talib M.A., Nasir Q., Dakalbab F.M. Machine learning for anomaly detection: A systematic review. IEEE Access, 2021, no. 9, pp. 78658-78700.
17. Omar S., Ngadi A., Jebur H. Machine learning techniques for anomaly detection: an overview. International Journal of Computer Applications, 2013, no. 79(2), pp. 32-41.
18. Dissanayake M.B. Feature engineering for cyber-attack detection in Internet of Things. International Journal of wireless and microwave technologies, 2021, no 6, pp. 46-54.
19. Vaccari I., Chiola G., Aiello M., Mongelli M. MQTTset, a New dataset for machine learning techniques on MQTT. Sensors, 2020, no. 20, pp. 6578, DOI:10.3390/s20226578.
20. Cook A.A., Mısırlı G., Fan Z. Anomaly detection for IoT time-series data: a survey. IEEE Internet of Things Journal, 2020, no. 7(7), pp. 6481-6494.
21. Musen M.A. The Protégé project: A look back and a look forward. AI Matters. Association of Computing Machinery Specific Interest Group in Artificial Intelligence, 2015, no. 1(4), DOI: 10.1145/2557001.25757003.
22. Isaeva O.S., Kulyasov N.V., Isaev S.V. Creation of a simulation stand for studying of the internet of things' technologies. AIP Conference Proceedings, 2022, no. 2647, pp. 040030-1-040030-5, DOI:10.1063/5.0104342.
23. Isaeva O.S., Kulyasov N.V., Isaev S.V. Formirovanie adaptivnyh rassylok brokera dannyh interneta veshchej [Formation of adaptive publications from the Internet of things data broker]. Informatsionno-upravlyayushchiye sistemy [Information and Control Systems], 2022, no. 5(120), pp. 23-31, DOI: 10.31799/1684-8853-2022-5-23-31.
24. Duhamel P., Vetterli M. Fast Fourier transforms: a tutorial review and a state of the art. Signal Processing, 1990, no. 19, pp. 259-299.
25. Ziatdinov S.I. Vosstanovlenie signala po ego vyborkam na osnove teoremy otschyotov Kotel'nikova [Reconstruction of signal by its samples on the base of Kotelnikov counts theorem]. Izvestiya vuzov. Priborostroyeniye [Journal of Instrument Engineering], 2010, no. 53(5), pp. 44-47.

Isaeva Olga Sergeevna. *Senior researcher of the Department of the Krasnoyarsk Mathematical Center of the Institute of Computational Modeling SB RAS, doctor of technical sciences. Research interests: artificial intelligence, data analysis, digital twins. SPIN code: 8412-5807, ORCID: 0000-0002-5061-6765, Researcher ID: A-8905-2018, isaeva@icm.krasn.ru, Krasnoyarsk, Akademgorodok, 50/44.*

Статья поступила в редакцию 10.05.2023; одобрена после рецензирования 08.06.2023; принята к публикации 16.06.2023.

The article was submitted 05/10/2023; approved after reviewing 06/08/2023; accepted for publication 06/16/2023.