

О ЗАДАЧАХ В ОБЛАСТИ РЕАЛИЗАЦИИ КОНЦЕПЦИИ «ИНТЕРНЕТА ВЕЩЕЙ»

Р.Р. Кадыров

kadyrov9634@gmail.com
SPIN-код: 6133-2755

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

«Интернет вещей» — это стремительно развивающаяся комплексная концепция, включающая в себя исследования в области информатики, сетевых технологий, микроэлектроники и сенсорной техники. Данная парадигма представляет собой основное направление развития сетевых технологий в будущем и позволит решить многие рутинные задачи человечества, начиная от измерения экологических показателей и заканчивая увеличением эффективности производства. Настоящая работа посвящена анализу ключевых научных задач, возникающих на пути реализации концепции «Интернета вещей». Перечислены основные критические задачи области, приведены их описания и возможные способы их решения, проанализированы существующие средства решения этих задач.

Ключевые слова

Концепция «Интернет вещей», сетевые технологии, анализ проблемной области, проблемы реализации, обработка информации, архитектура IoT, электропитание, масштабируемость, защита данных

Поступила в редакцию 21.01.2019

© МГТУ им. Н.Э. Баумана, 2019

Введение. «Интернет вещей» (Internet of Things, IoT) определяется как концепция, в которой бóльшая часть устройств, используемых людьми, снабжена микроконтроллерами для управления и сетевыми интерфейсами для цифровой передачи данных и общения [1]. Группа RFID определяет IoT как всемирную сеть доступных объектов, чья уникальная адресация основана на стандартных протоколах связи [2]. Можно выделить следующие сферы использования «Интернета вещей»: промышленность и производство; транспорт и перевозки; контроль технического состояния конструкций зданий, качества воздуха, шумового фона и потребляемой энергии; управление отходами; организация «умных» парковок и предоставление данных о дорожных пробках; организация «умного» уличного освещения и использование в быту [1–5].

С технической точки зрения IoT является не новой технологией, а совокупностью существующих средств, предоставляющих следующие возможности [6]:

– связь и взаимодействие — объекты могут создавать соединение с интернет-ресурсами или друг с другом и обновлять свое состояние. Первостепенное значение имеют беспроводные технологии, такие как GSM и UMTS, Wi-Fi, Bluetooth, ZigBee и другие разрабатываемые в настоящее время стандарты беспроводной сети;

– адресуемость — в «интернете вещей» объекты распределены в пространстве и должны иметь однозначную адресацию;

– идентификация позволяет однозначно ассоциировать данные с конкретным объектом и извлекать их. Стандарты RFID и NFC являются примерами технологий, с помощью которых можно идентифицировать даже пассивные объекты, не имеющие встроенных энергетических ресурсов [7];

– зондирование — IoT-устройства собирают информацию об окружающей среде с помощью датчиков, обмениваются ею или изменяют свое состояние под ее воздействием;

– встроенная обработка информации — объекты могут быть оснащены процессором или микроконтроллером для мгновенного анализа и обработки информации;

– локализация — устройства знают о своем физическом местоположении, что достигается благодаря использованию GPS или сети мобильной связи, а также радиомаяков (например, WLAN или RFID-ридеров с известными координатами) [7].

Приложения IoT подразделяют на две общие категории. К первой категории относят приложения, в которых собранные данные обычно проверяются не сразу, а обрабатываются и анализируются позже, ко второй — приложения реального времени, в которых важным является значение задержки [5].

Основные проблемы и задачи. Концепция «Интернета вещей» является комплексной и подразумевает объединение таких областей, как аппаратные средства, коммуникации и сети, потоки данных и программное обеспечение [3]. В результате возникает множество проблем и задач, которые являются как технологическими, так и социально-правовыми.

Архитектура системы. Основополагающими задачами IoT являются разработка и выбор правильной архитектуры системы, поскольку от решений на начальных этапах исследований зависит весь дальнейший процесс разработки [2]. На данный момент не существует конкретного соглашения по архитектуре IoT, которое было бы утверждено и использовалось повсеместно. Наиболее распространенными являются трех- и пятиуровневые модели архитектур. Первая из них служит базовой и включает уровень восприятия, сетевой и прикладной уровни. Данная модель определяет основную идею IoT, но она недостаточно детализирована, что необходимо для более глубоких исследований. Поэтому в литературе предлагаются архитектуры с большим числом уровней, например, пятиуровневая модель, которая дополнительно включает в себя уровни обработки и транспортный уровень [4].

Другой пример — облачная и туманная архитектуры. Первая ориентирована на облачные инфраструктуры, которые находятся в центре, приложения располагаются над ними, а сеть из «умных вещей» располагаются на уровне ниже. «Облакам» придается первостепенное значение, поскольку они обеспечивают большую гибкость и масштабируемость и предоставляют необходимые услуги (инфраструктура и платформа для программного обеспечения и хранения данных) [4].

По мнению исследователей, в последнее время появилась тенденция развития туманных вычислений, в которых датчики и сетевые шлюзы выполняют часть задач по обработке и анализу данных. Туманные и облачные вычисления зачастую используют совместно, поскольку это необходимо для оптимальной производительности IoT-приложений. Для реализации туманных вычислений шлюз может быть встроен между локальными сетями и «облаком» [4]. Здесь применяется многоуровневый подход, в котором предоставляются функции мониторинга (контроль используемой мощности и ресурсов), предварительной обработки (фильтрация, обработка и анализ данных), хранения (репликация данных, распространение и хранение) и обеспечения защищенности данных между физическим и транспортным уровнями (шифрование и обеспечение целостности и конфиденциальности данных) [4]. На текущий момент эта архитектура представляет наибольший интерес и, по мнению исследователей, является наиболее перспективной.

Питание устройств. Важная задача IoT — организация электропитания устройств, которые постоянно перемещаются и не обладают постоянным источником энергии. Во многих случаях батареи и блоки питания являются проблемными из-за их размера, веса и требований к обслуживанию. Разработчики и исследователи возлагают надежды на будущее маломощных процессоров для встроенных систем, которые будут потреблять значительно меньшую энергию [6]. Существуют аккумуляторные беспроводные датчики, которые могут передавать свои показания на расстояние в несколько метров. Как и RFID-системы, они получают энергию либо удаленно, либо от самого процесса измерения, например, с помощью пьезоэлектрических или пироэлектрических материалов [6]. Также для уменьшения расходов на питание необходимо сформировать стек протоколов с наименьшим объемом передаваемых данных [4].

На основе изложенных выше соображений можно сформулировать задачи разработки и выбора стандарта беспроводной связи. С точки зрения энергетических затрат стандартные технологии, такие как GSM, Wi-Fi и Bluetooth, являются неподходящими — они обладают широкой полосой пропускания и используют недопустимый для IoT-систем объем энергии. Для решения этой задачи были разработаны стандарты, соответствующие требованиям «Интернета вещей», например, IEEE 802.15.4, IEEE 802.11 Low Power, Bluetooth Low Energy, 6LoWPAN, RFID, NFC, ZigBee, Sigfox, LoRaWAN и другие протоколы для беспроводных сетей, которые используют мало энергии и совместимы с существующими протоколами транспортного и сетевого уровней [6].

Разработка стека сетевых протоколов. Разработка веб-стека для IoT требует грамотного построения его структуры, которая должна отвечать как требованиям коммуникационной инфраструктуры (совместимость с существующими стандартами), так и требованиям «Интернета вещей». Примерами таких стандартов являются: на уровне форматирования данных — EXI; на уровне представления — CoAP; на транспортном уровне — UDP; на сетевом —

IPv6/6LoWPAN [1]. Данные стандарты взаимодействуют с коммуникационной инфраструктурой точно так же, как и протоколы неограниченного стека, однако объем передаваемых данных значительно меньше. Этот факт способствует уменьшению потребляемой IoT-устройствами мощности и увеличению времени работы [8].

Схема адресации устройств. Схемы адресации является критичным аспектом в плане уникальности адресов, присваиваемых IoT-устройствам, поскольку они должны однозначно идентифицировать другие устройства и обмениваться с ними информацией. Наиболее важными особенностями создания уникального адреса являются его уникальность, надежность, устойчивость и масштабируемость. Существующий и повсеместно используемый протокол IPv4 позволяет идентифицировать лишь группу устройств, находящихся в определенной географической зоне, но не имеет возможности выделить каждый отдельный узел IoT. Облегчить проблемы идентификации устройств может протокол IPv6, однако неоднородность беспроводных узлов, переменные типы данных, одновременные операции и слияние данных с разных устройств еще больше усугубляют проблему [7].

Важным аспектом IoT является большое количество подключенных устройств, которое влечет за собой передачу огромных объемов данных. Поэтому одной из задач остается поиск путей для надежного хранения и интерпретации больших массивов данных [3]. Извлечение полезной информации из сложной сенсорной среды при различных пространственных и временных характеристиках является одной из задач исследования искусственного интеллекта. Конечной целью будет выявление событий, основанных на больших пространственных и временных интервалах [8].

Масштабируемость IoT-систем. Следующей проблемой IoT является масштабируемость. По оценкам Cisco, к 2020 г. к «облаку» будет подключено 50 миллиардов устройств, а согласно оценкам Gartner — 26 миллиардов. IoT имеет более широкий общий объем, чем обычный Интернет, поэтому масштабируемость пространства IoT будет более сложной, чем у обычных веб-приложений. Однако большинство данных, полученных IoT-устройствами, могут или должны быть обработаны локально и немедленно отброшены [5].

IoT-устройства интенсивно воспринимают неопределенную информацию физического мира, которая нуждается в точном представлении после таких процедур, как реорганизация, очистка и слияние. Объединение информации элементов сети необходимо для высокоэффективного обмена данными. Это приводит к другой ключевой задаче: представить, реорганизовать и использовать воспринимаемую информацию, а также решить проблемы адаптации взаимодействия, такие как представление информации, баланс между эффективностью и энергопотреблением в целях обеспечения эффективной поддержки служб приложений. Таким образом, эффективное использование неопределенной сенсорной информации является одной из ключевых научных проблем, т. е. проблемой эффективной интеграции и адаптации неопределенной информации [9].

Гарантированное качество обслуживания (QoS). Веб-пользователи допускают переменную задержку обычных веб-служб, однако временная недоступность датчиков или исполнительных IoT-устройств будет непосредственно воздействовать на физический мир. Необходим управляемый, оптимальный подход к обслуживанию различных сетевых трафиков, каждый из которых имеет свои собственные потребности [5]. Еще одним аспектом IoT является постоянное функционирование сети для повсеместной и непрерывной передачи данных. Хотя стек TCP/IP гарантирует это путем маршрутизации более надежным и эффективным способом, от источника до назначения, IoT сталкивается с узким местом в интерфейсе между шлюзом и беспроводными сенсорными устройствами. Добавление сетей и устройств не должно препятствовать производительности сети, функционированию устройств, надежности передачи данных по сети или эффективному использованию устройств из пользовательского интерфейса [9].

Безопасность и конфиденциальность личной информации. В дополнение к аспектам безопасности, таким как конфиденциальность связи, подлинность и надежность канала связи и целостность сообщений, в IoT будут иметь важное значение и другие требования. Необходимо предоставить устройству выборочный доступ к кругу услуг или в определенное время предотвратить общение с другими устройствами [10]. Промежуточное программное обеспечение должно иметь встроенные механизмы для решения этой задачи наряду с аутентификацией пользователей и реализацией контроля доступа. Многие задачи по защите информации могут быть решены с помощью криптографических методов и требуют больше исследований, прежде чем они могут быть широко использованы [2].

Международная деятельность. Международная деятельность в области «Интернета вещей» набирает обороты, и многие инициативы осуществляются в отраслях промышленности, научных кругах и на различных уровнях государственного управления. В Европе прилагаются значительные усилия по объединению деятельности исследовательских групп и организаций, охватывающей M2M, WSN и RFID, в единую систему IoT для определения эталонной модели взаимодействия систем «Интернета вещей» и ключевых составных блоков для достижения этой цели [10]. В Японии, Корее, США и Австралии реализуются масштабные инициативы, где промышленность и правительственные ведомства сотрудничают по различным программам в области IoT. Интенсивная работа в сфере IoT также ведется и в Китае в его 12-й пятилетке, в целях которой указано, что ресурсы и инвестиции должны быть ориентированы на разработку IoT в различных областях. Следовательно, необходимо сформировать единый для всех стран союз по решению проблем IoT, чтобы увеличить темпы развития сферы и определить путь для скоординированной реализации этой технологической идеи [2].

Выводы. С непрекращающимся расцветом новых технологий IoT концепция «Интернета вещей» скоро будет неумолимо развиваться в очень больших масштабах. Эта новая парадигма сетевого взаимодействия будет

влиять на каждую часть нашей жизни, начиная от автоматизированных домов до интеллектуального мониторинга здоровья и окружающей среды путем внедрения интеллекта в объекты вокруг нас. «Интернет вещей» является комплексной сферой, которая требует разработки стандартов в разных областях. Вследствие сложности и структурности концепции на пути ее развития возникает множество задач, связанных с различными областями. В данной статье выявлены наиболее острые научные и технические проблемы, стоящие перед сферой, выполнен обзор существующих средств, способствующих решению некоторых из выделенных задач. Промышленность может извлечь выгоду из развития «Интернета вещей», который тесно связан с телекоммуникационной, аппаратной, программной и сервисной отраслями.

Литература

- [1] Zanella A., Bui N., Castellani A., et al. Internet of Things for smart cities. *IEEE Internet of Things J.*, 2014, vol. 1, no. 1, pp. 22–32. DOI: 10.1109/JIOT.2014.2306328 URL: <https://ieeexplore.ieee.org/document/6740844>
- [2] Gubbi J., Buyya R., Marusic S., et al. Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener. Comput. Syst.*, 2013, vol. 29, no. 7, pp. 1645–1650. DOI: 10.1016/j.future.2013.01.010 URL: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241>
- [3] Tadejko P. Application of Internet of Things in logistics – current challenges. *MEPS*, 2015, vol. 7, no. 4, pp. 54–64. URL: <http://jem.pb.edu.pl/data/magazine/article/492/en/tadejko.pdf> (дата обращения: 10.10.2018).
- [4] Sethi P., Sarangi S.R. Internet of Things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017, vol. 2017, art. 9324035D. DOI: 10.1155/2017/9324035 URL: <https://www.hindawi.com/journals/jece/2017/9324035/>
- [5] Zhang B., Mor N., Kolb J., et al. Internet of Things: objectives and scientific challenges. *HotCloud'15 Proc. 7th USENIX Conf. Hot Topics in Cloud Computing*, 2015. URL: <https://www.usenix.org/system/files/conference/hotcloud15/hotcloud15-zhang.pdf>
- [6] Mattern F., Floerkemeier C. From the Internet of computers to the Internet of Things. *From active data management to event-based systems and more*. Springer, 2010, pp. 242–259.
- [7] Farooq M.U., Waseem M., Mazhar S., et al. A review on Internet of Things (IoT). *IJCA*, 2015, vol. 113, no. 1. DOI: 10.5120/19787-1571 URL: <https://www.ijcaonline.org/archives/volume113/number1/19787-1571>
- [8] Guinard D., Trifa V., Wilde E. A resource oriented architecture for the Web of Things. *IEEE Internet Things J.*, 2010. DOI: 10.1109/IOT.2010.5678452 URL: <https://ieeexplore.ieee.org/document/5678452>
- [9] Ma H.D. Internet of Things: objectives and scientific challenges. *J. Comput. Sci. Technol.*, 2011, vol. 26, no. 6, pp. 919–924. DOI: 10.1007/s11390-011-1189-5 URL: <https://link.springer.com/article/10.1007%2Fs11390-011-1189-5>
- [10] Angrishi K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. *arXiv.org*: веб-сайт. URL: <https://arxiv.org/abs/1702.03681> (дата обращения: 10.10.2018).

Кадыров Руслан Рамилевич — студент кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Горин Сергей Викторович, доцент кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

PROBLEMS IN THE IMPLEMENTATION AREA OF THE INTERNET OF THINGS CONCEPT

R.R. Kadyrov

kadyrov9634@gmail.com

SPIN-code: 6133-2755

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The Internet of Things is a rapidly developing integrated concept that includes research in the field of computer science, network technologies, microelectronics, and sensor technology. This paradigm represents the main direction of development of network technologies in the future and will allow to solve many routine tasks of humanity, ranging from measuring environmental indicators and ending with an increase in production efficiency. This paper is devoted to the analysis of key scientific problems arising in the implementation of the Internet of Things concept. The main critical problems on this topic are listed, their descriptions and possible solutions are presented, and the existing means of solving these problems are analyzed.

Keywords

Internet of Things (IoT) concept, network technologies, area of concern analysis, implementation problems, information processing, IoT architecture, power supply, scalability, data protection

Received 21.01.2019

© Bauman Moscow State Technical University, 2019

References

- [1] Zanella A., Bui N., Castellani A., et al. Internet of Things for smart cities. *IEEE Internet of Things J.*, 2014, vol. 1, no. 1, pp. 22–32. DOI: 10.1109/JIOT.2014.2306328 URL: <https://ieeexplore.ieee.org/document/6740844>
- [2] Gubbi J., Buyya R., Marusic S., et al. Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener. Comput. Syst.*, 2013, vol. 29, no. 7, pp. 1645–1650. DOI: 10.1016/j.future.2013.01.010 URL: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241>
- [3] Tadejko P. Application of Internet of Things in logistics – current challenges. *MEPS*, 2015, vol. 7, no. 4, pp. 54–64. URL: <http://jem.pb.edu.pl/data/magazine/article/492/en/tadejko.pdf> (accessed: 10.10.2018).
- [4] Sethi P., Sarangi S.R. Internet of Things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017, vol. 2017, art. 9324035D. DOI: 10.1155/2017/9324035 URL: <https://www.hindawi.com/journals/jece/2017/9324035/>
- [5] Zhang B., Mor N., Kolb J., et al. Internet of Things: objectives and scientific challenges. *HotCloud'15 Proc. 7th USENIX Conf. Hot Topics in Cloud Computing*, 2015. URL: <https://www.usenix.org/system/files/conference/hotcloud15/hotcloud15-zhang.pdf>
- [6] Mattern F., Floerkemeier C. From the Internet of computers to the Internet of Things. *From active data management to event-based systems and more*. Springer, 2010, pp. 242–259.
- [7] Farooq M.U., Waseem M., Mazhar S., et al. A review on Internet of Things (IoT). *IJCA*, 2015, vol. 113, no. 1. DOI: 10.5120/19787-1571 URL: <https://www.ijcaonline.org/archives/volume113/number1/19787-1571>
- [8] Guinard D., Trifa V., Wilde E. A resource oriented architecture for the Web of Things. *IEEE Internet Things J.*, 2010. DOI: 10.1109/IOT.2010.5678452 URL: <https://ieeexplore.ieee.org/document/5678452>

- [9] Ma H.D. Internet of Things: objectives and scientific challenges. *J. Comput. Sci. Technol.*, 2011, vol. 26, no. 6, pp. 919–924. DOI: 10.1007/s11390-011-1189-5
URL: <https://link.springer.com/article/10.1007%2Fs11390-011-1189-5>
- [10] Angrishi K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. *arXiv.org*: website. URL: <https://arxiv.org/abs/1702.03681> (accessed: 10.10.2018).

Kadyrov R.R. — Master's Degree Student, Department of Computer Software and Information Technologies, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — S.V. Gorin, Assoc. Professor, Department of Computer Software and Information Technologies, Bauman Moscow State Technical University, Moscow, Russian Federation.