УДК 004.738.5
ББК 32.973.202
Д 58

Довгаль Виталий Анатольевич
Кандидат технических наук, доцент, доцент кафедры информационной безопасности и прикладной информатики факультета информационных систем в экономике и юриспруденции Майкопского государственного технологического университета, Майкоп, e-mail: urmia@mail.ru
Довгаль Дмитрий Витальевич
Студент факультета энергетики и нефтегазопромышленности Донского государственного технического университета, Ростов-на-Дону, e-mail: lanayamen@gmail.com

Интернет Вещей: концепция, приложения и задачи

(Рецензирована)

Аннотация. *В настоящий момент все наблюдаемые формы коммуникаций сводятся либо к схеме человек-человек, либо человек-устройство. Но Интернет Вещей (IoT) предлагает нам колоссальное Интернет-будущее, в котором появятся коммуникации типа машина-машина (M2M). Это дает возможность для объединения всех коммуникаций в общую инфраструктуру, позволяя не только управлять всем, что находится вокруг нас, но и предоставляя информацию о состоянии этих вещей. Целью этой статьи является обзор вариантов использования IoT, а также обзор технологий, расширяющих его возможности и сетей датчиков. Также она описывает шестиступенчатую структуру IoT и указывает на связанные с этим ключевые задачи. Статья предназначена в основном исследователям, которые хотят начать свои работы в области Интернета Вещей и будет способствовать эффективному накоплению знаний.*

Ключевые слова: *Интернет Вещей, RFID, беспроводная сенсорная сеть, архитектура Интернета Вещей, концепция Интернета Вещей, приложения Интернета Вещей, безопасность в Интернете Вещей.*

Dovgal Vitaliy Anatolyevich
Candidate of Technical Sciences, Associate Professor, Associate Professor of Department of Information Security and Application Informatics of Faculty of Information Systems in Economy and Law, Maikop State University of Technology, Maikop, e-mail: urmia@mail.ru
Dovgal Dmitriy Vitalyevich
Student of Faculty of Energy Production and Oil-Gas Industry, Don State Technical University, Rostov-on-Don, e-mail: lanayamann@gmail.com

Internet of Things: concept, applications and tasks

Abstract. *At the moment all observed forms of communications come down either to the scheme of human-human, or human-device. But the Internet of Things (IoT) offers us the enormous Internet future in which communications of the machine-machine (M2M) type will appear. Thist will allow us to unite everything in our world in the general infrastructure, making it possible not only to operate everything that is around us, but also to provide us information on a condition of these things. The purpose of this paper is the comprehensive review of possible options of IoT use and also the review of the technologies expanding its opportunities and networks of sensors. Also, it describes six step structure of IoT and points to the key tasks connected with it. Anyway, this paper will give good understanding to other researchers who wish to begin their researches in the field of the Internet of Things, and will promote effective accumulation of knowledge.*

Keywords: *Internet of Things, RFID, WSN, IOT architecture, IoT Vision, IoT applications, IoT security.*

1. Введение

Интернет Вещей (IoT) – это новая концепция, в которой Интернет эволюционирует от объединения компьютеров и людей к объединению (умных) объектов/вещей [1]. С непрерывным продвижением технологий Интернет Вещей потенциальные инновации «обрушиваются» на нас, разрастаясь к глобальной вычислительной сети, где все и всё будут соединены посредством Интернет. IoT постоянно развивается и является горячей темой для исследований в настоящее время. Привычная форма Интернета переходит в его модифицированную и интегрированную версию. Количество устройств, использующих Интернет-услуги, растет с каждым днем и соединение их всех с помощью проводов или беспроводных технологий даст нам мощный источник информации на кончиках наших пальцев. Концепция расширяющих возможности взаимодействий между умными машинами является ультрасовременной технологией. Но технологии, которые составляют Интернет Вещей, не являются чем-то новым.

IoT является подходом соединения информации, полученной от различных источников, на любой виртуальной платформе или существующей Интернет-инфраструктуре. Концепция Интернета Вещей появилась в 1982 году, когда модифицированный автомат с газировкой был подключен к Интернету и был способен сообщать о наличии в нем напитков и их температуре. Позднее, в 1991 году Марком Вайзером была впервые дана современная оценка Интернета Вещей. Так или иначе, в 1999 году Билл Джой дал подсказку о связи между устройствами в своей таксономии Интернета [2]. В том же году Кевин Эштон предложил термин «Интернет Вещей» для связанных устройств. Базовой идеей IoT является предоставление возможности автономного обмена полезной информацией между уникально идентифицируемыми устройствами реального мира. Эти устройства оснащены новейшими технологиями, такими, как радиочастотная идентификация (RFID) и беспроводные сети датчиков (WSNs), и в дальнейшем получают возможность принимать самостоятельные решения в зависимости от того, какое автоматизированное действие выполняется.

2. Концепция

В 2005 году Международный союз по электросвязи (International Telecommunications Union, ITU) объявил эру всепроникающих сетей, главным признаком которых является связь сетей между собой. Главная концепция Интернета Вещей – это среда, в которой вещи имеют способность слушаться управления, а данные о вещах могут быть обработаны для выполнения желаемой задачи посредством обучения устройств. Практическая реализация IoT хорошо продемонстрирована в Twine, компактном и маломощном аппаратном обеспечении, работающим вместе с сетевым программным обеспечением в реальном времени и позволяющим сделать эту концепцию реальностью. Тем не менее, у разных людей и организаций есть свои отличающиеся концепции Интернета Вещей.

3. Архитектура

В компании Cisco считают, что в 2020 году будет более 50 миллиардов связанных объектов при населении 7 миллиардов человек [3]. Существующая архитектура Интернета с ее TCP/IP-протоколами не может справиться с такой большой сетью, как IoT. Поэтому возникает необходимость в новой открытой архитектуре, которая может отправлять отчеты о безопасности, качестве и классе предоставляемых услуг передачи данных (QoS), вместе с тем поддерживая существующие сетевые приложения, используя открытые протоколы. Интернет Вещей не может быть внедрен без должных гарантий безопасности. Следовательно, защита данных и приватность являются ключевыми задачами для IoT. Для дальнейшего развития IoT предложено некоторое количество многоуровневых архитектур безопасности. Например – шестиуровневая архитектура, основанная на иерархической структуре сетей, как показано на рисунке 1.

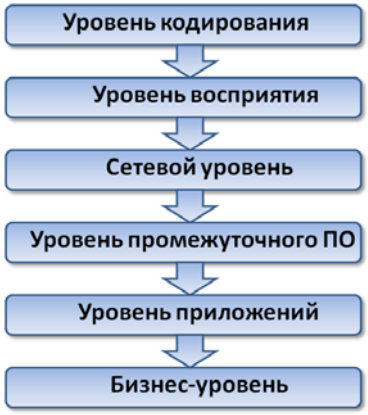

Рис. 1. Шестиуровневая архитектура IoT

Уровень кодирования: идентифицирует объект интереса (основа Интернета Вещей). Этот уровень назначает каждому объекту свой уникальный идентификатор (ID), что позволяет легко различать объекты.

Уровень восприятия: уровень устройств IoT, придающий каждому объекту физическое значение. Он состоит из датчиков данных различных видов, таких, как RFID-метки, IR датчики или другие сети датчиков, которые могут считывать температуру объекта, влажность, скорость, местоположение и т.д. Этот уровень собирает полезную информацию об объектах от датчиков, соединенных с ними, и преобразует эту информацию в цифровые сигналы, которые затем передаются на ступень сети для дальнейшей обработки.

Сетевой уровень: получает полезную информацию в форме цифровых сигналов от уровня восприятия и передает ее обрабатывающим системам, представленным на уровне промежуточного ПО через связующие среды, такие, как WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G и т.д., используя протоколы IPv4, IPv6, MQTT, DDS и т.д.

Уровень промежуточного ПО: обрабатывает информацию, полученную от датчиков, используя такие технологии, как облачные вычисления, глобальные вычисления, гарантируя прямой доступ к базе данных для того, чтобы поместить в нее всю необходимую информацию. Используя Intelligent Processing Equipment (Оборудование Интеллектуальной Обработки), информация обрабатывается, а затем выполняется полностью автоматизированное действие на основе результатов обработки этой информации.

Уровень приложений: реализует IoT-приложения для всех видов промышленности на основе обработанных данных. Этот уровень полезен при крупномасштабном развитии сети IoT. С IoT могут быть связаны умные дома, умные перевозки, умная планета и т.д.

Бизнес-уровень: управляет приложениями и услугами IoT и ответственен за все исследования, связанные с IoT. Он генерирует разные бизнес-модели для эффективных бизнес-решений.

4. Технологии

Развитие всепроникающих вычислительных систем, в которых цифровые объекты могут быть уникально идентифицированы и имеют возможность думать и взаимодействовать с другими объектами, чтобы собирать данные на базе того, какое автоматизированное действие производится, требует необходимости в комбинации новых и эффективных технологий, что возможно только при интеграции разных технологий, которые могут идентифицировать объекты и заставить их взаимодействовать друг с другом. В крупномасштабном развитии IoT могут оказать помощь следующие технологии.

Радиочастотная идентификация (RFID)

RFID – ключевая технология, предназначенная для уникальной идентификации объектов. Небольшие размеры метки и малая стоимость позволяют интегрировать технологию в любой объект. Метка – это приемопередатчик в виде микрочипа, схожий со стикером, который может быть как активным, так и пассивным, в зависимости от типа приложения. В активные метки встроена батарея, поскольку они постоянно активны и, следовательно, постоянно испускают сигналы с данными, в то время как пассивные метки активируются, только когда они приведены в действие. Активные метки стоят дороже, чем пассивные. RFID система состоит из средств чтения и RFID-связанных меток, генерирующих идентификационные, топографические и другие данные об объекте, активируясь с помощью генерации любого соответствующего сигнала. Сигналы данных излучающего объекта передаются средствам чтения с помощью радиоволн, а затем обрабатываются процессорами, чтобы проанализировать данные в зависимости от типа приложения. RFID-частоты разделены на 4 диапазона частот:

1. Низкая частота (135 кГц или меньше);
2. Высокая частота (13,56 МГц);
3. Ультравысокая частота (862 Мгц – 928 Мгц);
4. Микроволновая частота.

Также существует другая технология: идентификация – штрих-код, который имеет такую же функцию, как и RFID, хотя RFID считается эффективнее. Будучи радиотехнологией, RFID не требует непосредственного визуального контакта со средством чтения, в то время

как штрих-код – это оптическая технология, которая не работает, если средство чтения не находится прямо перед ним. Более того, RFID может работать как привод, активируя различные события, и даже имеет возможность модификации, на что штрих-код, очевидно, не способен.

Беспроводная сенсорная сеть (WSN)

WSN – это двусторонняя беспроводная сеть датчиков, построенная из нескольких узлов, разбросанных по полю датчиков, соединенных с одним или несколькими датчиками, которые могут захватывать такие данные объекта, как температура, влажность, скорость и т.д., а затем передавать их обрабатывающему оборудованию. Каждый датчик – это приемопередатчик, имеющий антенну, микроконтроллер и интерфейсные цепи (такие, как коммуникация, активация и сенсорный блок), соответственно, вместе с источником питания, которым может быть как батарея, так и любое устройство накопления энергии. Также может быть добавлен дополнительный элемент для сохранения данных, называемый элементом памяти.

Облачные вычисления

Облако считается единственной технологией, которая может анализировать и сохранять все данные эффективно. Это интеллектуальная вычислительная технология, в которой несколько серверов соединяются в одной облачной платформе для того, чтобы совместно использовать ресурсы друг друга в любое время и в любом месте. Облачные вычисления не только объединяют серверы, но также обрабатывают на увеличенных обрабатывающих мощностях и анализируют полезную информацию, полученную от датчиков, и даже могут предложить хорошую емкость. Но это лишь начало раскрытия истинного потенциала этой технологии. Облачные вычисления с интерфейсом в виде умных объектов, используя миллионы потенциальных датчиков, могут помочь крайне крупномасштабному развитию IoT, поэтому исследования будут начаты, только когда IoT будет полностью зависеть от облачных вычислений.

Сетевые технологии

Эти технологии отвечают за связь между объектами. Итак, нам нужна быстрая и эффективная сеть, чтобы справиться с огромным числом потенциальных устройств. Для широкополосных передающих сетей обычно используют 3G, 4G, но, как известно, мобильный трафик очень предсказуем с тех пор, как он начал выполнять только простые вещи, такие как совершение звонков, передача текстовых сообщений и т.д.; но поскольку мы вступаем в современную эру повсеместных вычислений, он более не будет столь предсказуемым, что приводит к необходимости супербыстрой, суперэффективной беспроводной системы пятого поколения. Точно так же для сетей ближнего действия используем такие технологии, как Bluetooth, WiFi и т.д.

Нано-технологии

Эта технология полезна для небольших и улучшенных версий соединяемых объектов. Она может снизить потребление системы при развитии устройств в нано-масштабе, которые могут быть использованы как датчик и как активный элемент также, как и обычные устройства.

Технологии микроэлектромеханических систем (MEMS)

MEMS – это комбинация электрических и механических компонентов, работающих совместно, обеспечивающих работу некоторых приложений, включая восприятие и активацию, которые уже были коммерчески реализованы во многих областях (преобразователи, акселерометры и т.д.). MEMS в комбинации с нано-технологиями являются довольно эффективным решением в плане затрат для воспроизведения коммуникационной системы IoT, а также имеют ряд других преимуществ, таких как уменьшение размеров датчиков, интеграция общедоступных вычислительных устройств и расширенный диапазон частот.

Оптические технологии

Быстрое развитие области оптических технологий в виде таких, как Li-Fi и BiDi от Cisco, делает их основным прорывом в развитии IoT. Li-Fi – эпохальная технология Visible Light Communication (VLC), предоставляющая отличное соединение в большом диапазоне

частот для объектов, соединенных в концепте IoT. Похожим образом технология Bi-Directional (BiDi) позволяет использовать 40-гигабайтовый Ethernet-канал для больших объемов информации, поступающих от многообразных устройств IoT.

5. Приложения

Большинство повседневных приложений, которые мы видим, уже относятся к категории “smart” (умные), но они не могут взаимодействовать между собой, и понадобится создать широкий спектр инновационных приложений, чтобы заставить их взаимодействовать и делиться полезной информацией между собой. Эти появляющиеся приложения с некоторыми автономными возможностями, безусловно, улучшат качество нашей жизни. Приведем примеры некоторых возможных в будущем приложений, которые могут предоставить огромные преимущества.

Умная дорожная сеть. Дорожная сеть является важной составляющей современного общества, поэтому все связанные проблемы должны быть правильно решены. Для этого необходима система, которая может улучшить ситуацию на дорогах, основываясь на данных о трафике, полученных от объектов с использованием технологии IoT. Для такой умной системы мониторинга трафика реализация системы для автоматической идентификации транспортных средств и других дорожных факторов очень важна, для чего нам и нужна технология IoT вместо использования обычной системы распознавания изображений. Умная система мониторинга трафика облегчит транспортировку, устранив заторы. У этой системы есть также такие особенности, как распознавание краж, сообщения о дорожных происшествиях, меньшее загрязнение среды. Дороги «умного города» будут также предлагать объезды в связи с плохими погодными условиями или пробками, поскольку все маршруты будут оптимизированы. Система светофоров будет адаптироваться к погодным условиям для сбережения энергии. Также каждому потребителю будут доступны данные о возможностях парковочных мест.

Умная среда. Предсказание природных катастроф, таких как наводнение, пожар, землетрясение, станет возможным благодаря инновационным технологиям IoT. Они также позволят тщательнее контролировать загрязнение воздуха в окружающей среде.

Умный дом. IoT также обеспечивает непромышленные решения для автоматизации дома, с помощью которых можно удаленно управлять бытовыми приборами в зависимости от нужд пользователя. Тщательный контроль счетчиков коммунальных услуг, поставок энергии и воды поможет сберегать ресурсы и определять неожиданные перегрузки, отключение воды и т.д. Улучшенная система определения вторжения предотвратит кражи. Датчики в саду смогут измерять освещение, температуру, влажность и другие важные для сада параметры и поливать растения в соответствии с их потребностями.

Умные больницы. Больницы будут оборудованы умными перенастраиваемыми приборами, оснащенными RFID-метками, и выдаваемыми пациентам по прибытию, с помощью которых не только доктора, но и медсестры смогут отслеживать пульс, кровяное давление, температуру и другие параметры пациента внутри и за пределами больницы. Множество экстренных случаев, таких как остановка сердца, требуют времени для реакции скорой помощи и для того, чтобы добраться до пациента. На рынке уже существуют дроны скорой помощи, которые могут долететь до места происшествия с экстренным медицинским набором и, благодаря лучшему отслеживанию пациента, доктор сможет определить местоположение пациента и отправить дрон скорой медицинской помощи, пока не прибудет скорая помощь.

Умное сельское хозяйство. Это приложение сможет контролировать питание почвы, освещение, влажность и улучшит озеленение домов, автоматически увеличивая температуру для получения максимального результата. Корректный полив и внесение удобрений помогут улучшить качество воды и сберечь удобрения.

Умная розничная торговля и управление цепью поставки. IoT вместе с RFID предоставляют розничным торговцам множество преимуществ. Используя продукты с RFID, продавец сможет отслеживать запасы и определять кражи. Более того, продавец может составлять топы продаж и графики для эффективных стратегий.

6. Задачи безопасности и приватности

IoT делает возможным найти любого человека, упрощая нашу жизнь; однако без должной уверенности в безопасности и приватности данных пользователя эта система многими не будет принята. Поэтому для повсеместного внедрения IoT должен иметь сильную защитную инфраструктуру. Проблемы и задачи безопасности сетей, основанных на Интернете Вещей, уже были рассмотрены подробно ранее [4]. Здесь приведем только некоторые конкретные возможные проблемы, связанные с безопасностью IoT и использованием технологий, описанных в п. 4.

Несанкционированный доступ к RFID. Несанкционированный доступ к меткам, которые могут содержать идентификационную информацию, – это главная проблема безопасности IoT (возможно раскрытие любой конфиденциальной информации о пользователе), поэтому она должна быть решена в первую очередь. Метка может быть не только прочитана считывающим устройством злоумышленника, но даже модифицирована или повреждена. Существуют несколько реальных угроз для RFID, которые включают RFID-вирус, атаку с помощью мобильного телефона и взлом SpeedPass.

Нарушение безопасности узлов датчиков. WSN уязвима к некоторым видам атак, поскольку узлы датчиков – это часть двусторонней сети датчиков, что означает не только возможность передачи, но и захвата данных. Возможные атаки включают в себя забивание канала, вмешательство, атаку Сибиллы (сетевая атака, при которой один из узлов может иметь несколько идентификаторов, тем самым нарушая работу системы), заполнение и некоторые другие виды атак, которые заключаются в следующем:

1) забивание затрудняет работу всей сети, интерферируя с частотами узлов датчиков;
2) вмешательство – это вид атаки, в которой информация с узлов может быть извлечена или изменена злоумышленником для того, чтобы взять узел под свой контроль;
3) атака Сибиллы – навязывание множественных псевдоанонимных идентификационных данных, придавая им большое значение;
4) заполнение – это вид DOS-атаки, вызванный огромным объемом трафика, приводящим к израсходованию ресурсов памяти.

Злоупотребление облачными вычислениями. Облачные вычисления – это большая сеть объединенных серверов, которая позволяет делиться ресурсами друг с другом. Разделение ресурсов может столкнуться с множеством угроз безопасности, таких как Man-in-the-middle атака (MITM), фишинг и т.д. Альянс безопасности облачных вычислений (CSA) предложил еще некоторые угрозы, такие как вредоносный инсайдер, потери данных, кража аккаунтов, невероятное использование компьютеров, разделяющих ресурсы, которые заключаются в следующем:

1) вредоносный инсайдер – это угроза того, что легальный пользователь, имеющий доступ к данным, может быть вовлечен в манипуляции с данными;
2) потеря данных – это угроза, суть которой заключается в том, что любой злоумышленник, имеющий несанкционированный доступ к сети, может изменять или удалять существующие данные;
3) Man-in-the-middle – это вид угрозы кражи аккаунтов, суть которой в том, что атакующий может изменять или перехватывать сообщения в обмене между двумя участниками;
4) облачные вычисления могут быть использованы жестоким образом, поскольку если атакующий получает возможность загрузить любое вредоносное программное обеспечение на сервер, используя, например, ботнет, это может дать атакующему контроль над многими связанными устройствами.

7. Вывод

Быстрое распространение появляющихся технологий IoT, концепция Интернета Вещей будет масштабно развиваться. Парадигма сетей повлияет на каждую часть нашей жизни – от автоматизированных домов, до умного здравоохранения и мониторинга среды, встраивая интеллект во все объекты вокруг нас. В статье рассмотрены концепция IoT и четко определенная архитектура для его развертывания, различные технологии и некоторые связанные угро-

зы. Обсуждены приложения, использующие технологию Интернет Вещей, призванных сделать нашу жизнь лучше. Анализ многочисленных исследований по данной теме показывает, что в них не учитывались задачи обеспечения конфиденциальности и безопасности пользователя. Развертывание IoT требует больших усилий и современных решений по ликвидации угроз безопасности и приватности.

Примечания:

1. Довгаль В.А., Довгаль Д.В. Управление ресурсами в Интернете Вещей // Дистанционные образовательные технологии: материалы II Всерос. науч.-практ. конф., г. Ялта, 2017 г. Симферополь: АРИАЛ, 2017. С. 168–173.
2. Kevin Ashton. That “Internet of Things” Thing // RFID Journal. 2009. 22 June. URL: http://www.rfidjournal.com/articles/pdf?4986 (дата обращения: 11/03/2018).
3. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL. pdf (дата обращения: 11/03/2018).
4. Довгаль В.А., Довгаль Д.В. Проблемы и задачи безопасности интеллектуальных сетей, основанных на Интернете Вещей // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2017. Вып. 4 (211). С. 140–147. URL: http://vestnik.adygnet.ru

References:

1. Dovgal V.A., Dovgal D.V. Management of resources on the Internet of Things // Distance educational technologies: proceedings of the II Russian scient.-pract. conf., Yalta, 2017. Simferopol: ARIAL, 2017. P. 168–173.
2. Kevin Ashton. That “Internet of Things” Thing // RFID Journal. 2009. 22 June. URL: http://www.rfidjournal.com/articles/pdf?4986 (date of access: 11/03/2018).
3. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL. pdf (date of access: 11/03/2018).
4. Dovgal V.A., Dovgal D.V. Security issues and challenges for the intellectual networks founded on the Internet of Things // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2017. Iss. 4. P. 140–147. URL: http://vestnik.adygnet.ru