СТАНДАРТЫ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

МИХАИЛ КАРЦЕВ, инженер

В статье описаны уровни, на которые делится архитектура интернета вещей. Приведены общие сведения о протоколах, используемых на различных уровнях. Затронуты менее очевидные вопросы, которые необходимо учитывать при организации умных сетей.

С совершенствованием интернета вещей (IoT) возникает потребность в гибкой многослойной архитектуре, которая позволяет объединить миллиарды и триллионы узлов через интернет.

Представлены отдельные проекты, например IoT-A, нацеленные на создание общей архитектуры, однако преимущественное решение до сих пор не появилось. Большинство исходных моделей имеет трехслойную структуру: уровень восприятия (Perception), сетевой (Network) и прикладной (Application) уровни.

На первом уровне физические датчики собирают данные и оцифровывают их для последующей передачи по защищенному каналу. На сетевом уровне производится управление сбором данных, их фильтрацией и передачей в концентраторы IoT и интеллектуальные устройства. На уровне приложения данные передаются конечным устройствам.

Некоторые модели более абстрактны – они содержат пять уровней и основаны на запросах и пропускной способности IoT (см. рис. 1).

УРОВНИ IoT

Объектный

На этом уровне происходит формирование больших данных. Уровень включает физические датчики, которые собирают и обрабатывают информацию. Под объектами могут пониматься датчики и исполнительные механизмы для мониторинга местонахождения, температуры, веса, движения, вибрации, ускорения, влажности и других параметров.

Уровень абстракции объектов

Осуществляется передача данных с объектного слоя на уровень управления и обслуживания. Применяются такие технологии как RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, ИК-связь и ZigBee. На уровне управления и обслуживания выполняются облачные вычисления и процессы управления данными. На рисунке 2 показаны стандарты, используемые на разных уровнях.

Уровень обслуживания и управления

На этом уровне производится назначение службы запрашивающему устройству на основе имен и адресов. На данном уровне происходит работа со всеми объектами из разных аппаратных платформ. Кроме того, осуществляется обработка полученных данных, принятие решения и предоставление требуемой службы по сетевому проводному протоколу.

Уровень приложения

На данном уровне предоставляются интеллектуальные функции для систем «умный дом», «умное здание», транспортного оборудования и систем промышленной автоматизации, а также носимых биодатчиков.

Рис. 1. **Примеры трех- и пятиуровневых моделей**

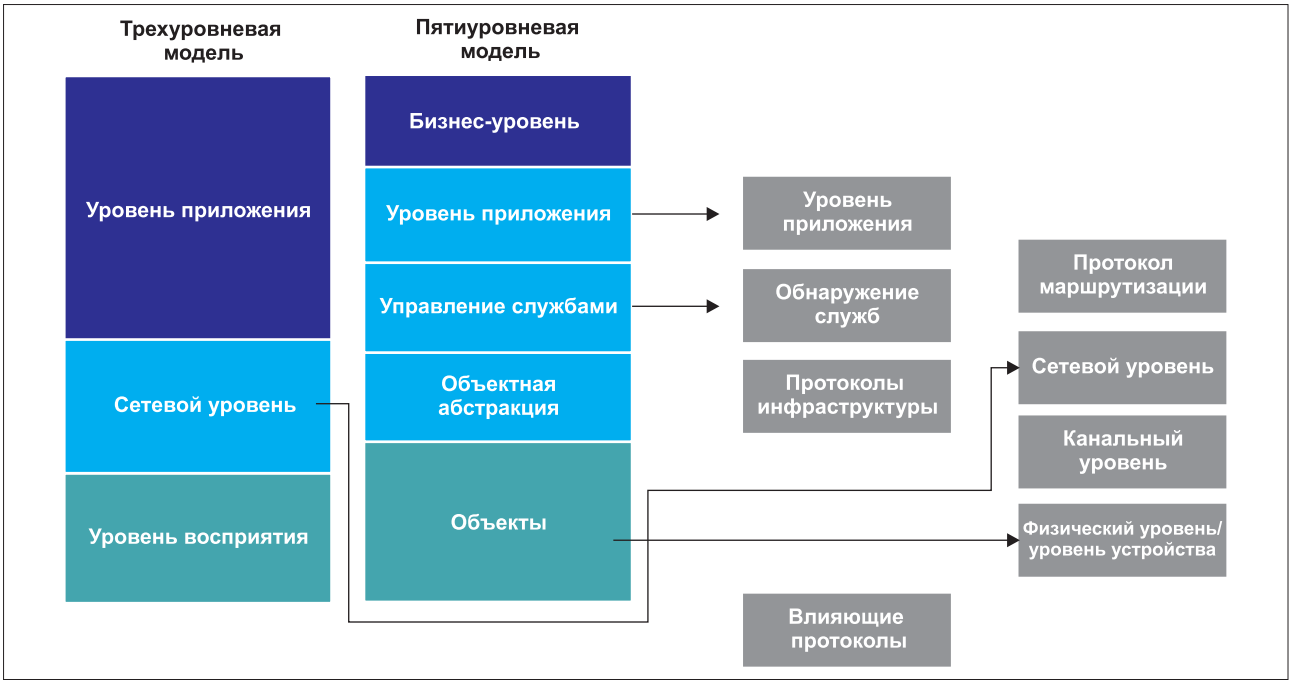

Рис. 2. **Уровни интернета вещей и соответствующие протоколы**

Бизнес-уровень

На данном уровне осуществляется управление процедурами и службами IoT, построение бизнес-моделей, графиков, диаграмм и т. д. в соответствии с данными, полученными на уровне приложения. Кроме того, производится проектирование, анализ, исполнение, оценка, мониторинг и развитие сопряженных системных элементов IoT. Бизнес-уровень поддерживает процессы принятия решения на основе анализа больших данных.

ЭЛЕМЕНТЫ IoT

В системе IoT работа с данными разбивается на несколько стадий: идентификацию, получение данных, передачу, вычисление, обслуживание, семантическую обработку. Эта взаимосвязанная сеть управления информацией отвечает растущим потребностям IoT, в т. ч. по сбору, защите и доставке данных. На каждой стадии компании могут тщательно оценить протоколы, процедуры и модернизировать их для повышения эффективности.

Шестью главными элементами, необходимыми для систем IoT, являются: идентификация, измерение и контроль, передача, вычисление, сервисы, семантическая обработка (см. табл. 1)

Методы идентификации обеспечивают четкое опознание каждого объекта внутри сети и назначение сервисов в соответствии с потребностями. Не следует путать идентификацию объекта и его адрес, т. к. методы идентификации не уникальны в глобальном масштабе. Многочисленные методы идентифи-

Таблица 1. **Обзор элементов IoT**

Элемент	Определение	Пример
Идентификация *Создание ясных уникальных кодов всех объектов сети и согласование сервисов с запросами пользователя*	Имена – уникальные коды для каждого объекта	Коды EPC и ucode
	Адреса обеспечивают глобальную уникальность. Уникальные коды применяются локально	IPv4, IPv6
Измерение и контроль	Сбор данных с объектов внутри сети, их отправка в хранилище, базу данных или облако	Интеллектуальные датчики, носимые датчики, встраиваемые датчики, исполнительные механизмы, метки RFID
Связь	Обмен между гетерогенными объектами для предоставления специфичных интеллектуальных сервисов	RFID, NC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, Wi-Fi, Wi-Fi Direct, LTE-A
Вычисления	Аппаратная часть включает вычислительные устройства: микроконтроллеры, микропроцессоры, СнК, ПЛИС	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, смартфоны
	Программная часть представляет собой операционные системы, которые работают, пока устройство активно	Contiki, TinyOS, LiteOS, RIOT OS, Android), облако (Nimbits, Hadoop и т.д.)
Службы	Идентификация (цепь поставки)	Распознает реальные объекты, которые используются в виртуальной среде
	Сбор информации (интеллектуальные электросети)	Сбор и обобщение показаний датчиков для последующей обработки
	Взаимодействие («умный дом»)	Работают поверх служб сбора информации. На основе полученных данных принимают решение и выполняют его
	Повсеместность («умный город»)	Предоставляют возможность взаимодействия в любой момент любому узлу
Семантические функции	Гарантируют, что данные направляются по назначению	Resource Description Framework (RDF), Web, Ontology Language (OWL)

Таблица 2. **Рекомендуемые операционные системы реального времени**

ОС	Язык	Мин. память, Кбайт	Программирование по событию	Многопоточность	Динамическая память
TinyOS	nesC	1	есть	частично	есть
Contiki	C	2	есть	есть	есть
LiteOS	C	4	есть	есть	есть
RIOT OS	C/C++	1,5	нет	есть	есть
Android	Java	–	есть	есть	есть

кации, например единые коды (ucode) и электронные коды изделий (EPC), доступны для IoT.

Измерение и контроль

Датчики IoT могут представлять собой интеллектуальные сенсоры, например нательные сенсоры и исполнительные механизмы, которые контролируют их. Эти датчики осуществляют сбор данных и отправляют их в облако, базу данных или хранилище. Собранные данные анализируются – над ними производятся операции, определяемые службами.

Передача

Технологии передачи IoT предоставляют специфичные интеллектуальные сервисы путем соединения гетерогенных объектов. Эти узлы часто работают в энергосберегающем режиме в присутствии помех и при высоком уровне потерь передачи.

Вычисления

Вычисления производятся в программно-аппаратном блоке. Вычислительным ядром может быть микроконтроллер, микропроцессор, СнК, ПЛИС. Для них требуются операционные системы, которые запускаются при активации устройства. В таблице 2 упомянуто несколько операционных систем реального времени (RTOS), которые наиболее подходят для IoT.

Службы

Службы делятся на четыре категории.

- *Сервисы идентификации.* Они распознают реальные объекты, которые приложение использует в виртуальном пространстве. Эти сервисы являются одновременно и наиболее базовыми, и наиболее важными. Они используются в других категориях служб.
- *Службы сбора данных* осуществляют сбор и обобщение показаний датчиков, которые впоследствии обрабатываются и отправляются в приложение.
- *Сервисы взаимодействия* работают поверх служб сбора данных – на основе собранных данных принимают решения и формулируют ответы.
- *Глобальные сервисы* предоставляют сервисы взаимодействия в любое требуемое время любому пользователю в любом месте.

Эти сервисы позволяют унифицировать все приложения IoT, сделав их едиными и повсеместными.

Семантические функции

Семантические функции гарантируют, что данные, извлеченные из системы, направляются по назначению.

Понятие «семантический» подразумевает способность выделить информацию с разных устройств и предоставить требуемую службу. При извлечении информации необходимо обнаружить ресурс, использовать его и воспроизвести информацию. Кроме того, осуществляется распознание и анализ данных, принятие решения и предоставление точного сервиса.

Таким образом, семантический блок – это своего рода «мозг» IoT, который дает команды ресурсам.

СТАНДАРТЫ IoT

Стандарты можно разделить на четыре категории, которые не обязательно работают совместно в приложении (см. табл. 3). Организация IEEE разработала тысячи стандартов, обеспечивающих связность разнотипных устройств, например носимых биодатчиков и транспортного оборудования. Эти стандарты получат применение в системах будущего.

Прикладные протоколы

Расширяемый протокол передачи сообщений и обозначения присутствия (Extensible Messaging and Presence Protocol, XMPP) является ключевым элементом инновационных систем связи. Этот протокол предназначен для передачи мгновенных сообщений независимо от используемой ОС между несколькими устройствами сразу: передачу голоса и видео, обеспечение удаленного присутствия. Ранее он назывался Jabber.

Прикладной протокол CoAP

Протокол основан на передаче состояния (Representational State Transfer, REST) по HTTP.

Состояние REST упрощает обмен данными внутри мобильных приложений между клиентом и сервером. Состояние REST позволяет избежать неопределенностей, возникающих при использовании методов HTTP GET, POST, PUT и DELETE.

Протокол очередности сообщений MQTT

Протокол передачи последовательности сообщений (Message Queuing Telemetry Transport, MQTT) осуществляет соединение встроенных устройств и сетей с приложением и промежуточным ПО. Разработанный специально для сетей датчиков, он обеспечивает механизмы маршрутизации (точка–точка, точка–многоточка, многоточка–многоточка), благодаря которым упрощается работа устройств с ограниченными ресурсами.

Таблица 3. **Категории стандартов IoT**

Прикладной протокол		DDS	CoAP	AMQP	MQTT	MQTT-SN	XMPP	HTTP REST
Обнаружение службы		mDNS				DNS-SD		
Протоколы инфраструктуры	Протокол маршрутизации	RPL						
	Сетевой уровень	6LoWPAN				IPv4/IPv6		
	Канальный уровень	IEEE 802.15.4						
	Физический уровень/ уровень устройства	LTE-A	EPCglobal		IEEE 802.15.4		Z-Wave	
Влияющие протоколы		IPsec					IEEE 1905.1	

Таблица 4. **Основные различия между прикладными протоколами**

Протокол	RESTful	Транспортный протокол	Публикация/подписка	Запрос/ответ	Защита	QoS	Размер заголовка, байт
CoAP	есть	UDP	есть	есть	DTLS	есть	4
MQTT	нет	TCP	есть	нет	SSL	есть	2
MQTT-SN	нет	TCP	есть	нет	SSL	есть	2
XMPP	нет	TCP	есть	есть	SSL	нет	–
AMQP	нет	TCP	есть	нет	SSL	есть	8
DDS	нет	UDP	есть	нет	SSL, DTLS	есть	–

Усовершенствованный протокол очередности сообщений AMQP

Открытый протокол (Advanced Message Queuing Protocol, AMQP) обеспечивает улучшенные механизмы передачи сообщений между устройствами, в первую очередь по TCP.

Сервис распределения данных DDS

Служба распределения данных (Data Distribution Service, DDS) основана на принципе публикаций и подписок. Она обеспечивает связь между машинами (M2 M) в реальном времени. В отличие от MQTT и AMQP, служба DDS не использует посредников и основана на групповой рассылке. Основные различия между рассматриваемыми протоколами показаны в таблице 4.

Протоколы обнаружения сервисов

Протоколы обнаружения сервисов (Service Discovery Protocols, SDP) осуществляют регистрацию ресурсов и протоколов, доступных через сервисы IoT. Доминирующими протоколами этой категории являются групповая рассылка через DNS (mDNS) и обнаружение сервисов через DNS (DNS-SD). Хотя они изначально разработаны для устройств с широким функционалом, эти два протокола могут быть адаптированы для IoT.

mDNS

Для некоторых приложений IoT, таких как чат, протокол групповой рассылки mDNS (Multicast DNS) может взять на себя роль сервера DNS. Поскольку DNS обычно используется локально, mDNS обеспечивает функциональную гибкость без дополнительных затрат.

Протокол хорошо подходит для встраиваемых интернет-устройств, поскольку не требует изменения их конфигурации вручную, дополнительной инфраструктуры, а в случае сбоя продолжает работать в инфраструктуре.

Протокол обнаружения сервиса DNS-SD

Обнаружение сервисов через DNS-службу (DNS Service Discovery) позволяет клиентам, используя стандартные сообщения DNS, найти требуемые службы. Протокол DNS-SD, как и mDNS, соединяет машины без внешней конфигурации и управления.

ПРОТОКОЛЫ ИНФРАСТРУКТУРЫ

Протокол маршрутизации RPL

Протокол маршрутизации для малопотребляющих сетей и сетей с высоким уровнем потерь (Routing Protocol for Low-Power and Lossy Networks, RPL) представляет собой протокол маршрутизации, не зависимый от канала. Он основан на IPv6, поддерживает простые и сложные модели передачи, такие как многоточка–точка, точка–точка, точка–многоточка.

6LoWPAN

Данный протокол обеспечивает отображение сервисов, требуемых в IPv6, на персональные сети с низким энергопотреблением (Low-Power WPAN). Это уровень адаптации, на котором пакеты IPv6 конвертируются под формат IEEE 802.15.4. В частности, производится сжатие заголовка для снижения нагрузки на сеть, фрагментация для обеспечения соответствия максимальной единице передачи IPv6 MTU, а также пересылка на уровень связи для передачи с перескоками частоты.

IEEE 802.15.4

Данный протокол является прослойкой между канальным (Medium Access Control, MAC) и физическим уровнем (PHY) для беспроводных персональных сетей с низкой скоростью передачи (LR-WPAN).

IEEE 802.15.4, который может управлять большим количеством узлов, обеспечивает надежную передачу данных и работу на разных платформах. Поскольку протокол имеет низкое энергопотребление и стоимость, предусматривает низкую скорость передачи данных и высокую пропускную способность, его часто используют в IoT, M2M и беспроводных сетях датчиков (WSN). Хотя IEEE 802.15.4 имеет высокий уровень защиты, обеспечивает шифрование и аутентификацию, он не предоставляет гарантии QoS.

Bluetooth Low Energy (BLE)

Другое название протокола – Bluetooth Smart. Это протокол связи на малом расстоянии. За счет низкой потребляемой энергии обеспечивается более продолжительное время работы. Это особенно важно для IoT. Покрываемый диапазон составляет около 100 м – в 10 раз больше, чем обеспечивал классический стандарт Bluetooth. Задержка прохождения сигнала примерно в 15 раз меньше, чем в классической версии. Мощность передачи составляет 0,01–10 мВт.

Таблица 5. **Особенности физических протоколов**

Протокол	Метод расширения спектра	Полоса, МГц	Доступ к среде	Скорость передачи данных	Масштабируемость
IEEE 802.15.4	DSSS	868/915/2400	TDMA, CSM/CA	20/40/250 Кбит/с	65K узлов
BLE	FHSS	2400	TDMA	1024 Кбит/с	5917 подчиненных устройств
EPCglobal	DS-CDMA	860–960	Aloha	5–640 Кбит/с	–
LTE-A	Несколько CC	разная	OFDMA	IG (восх.), 500 Мбит (нисх.)	–
Z-Wave	–	868/908/2400	CSMA/CA	40 Кбит/с	232 узла

Таблица 6. **Протоколы защиты**

Уровень	Уровень приложения	Протокол защиты	Решение
Приложения	Файловая система	Codo (для ОС Contiki)	Кэширует данные для группового шифрования и дешифрования в беспроводных сетях датчиков (WSN)
Приложения	Канал	IEEE 802.15.4	Защищает обмен между двумя соседними устройствами в беспроводных персональных сетях (WPAN)
Сетевой		IPsec	Обслуживает протокол обязательной защиты для IPv6
Сетевой		IPsec для 6LoWPAN	Обслуживает протоколы приложения, которые отвечают по TCP или UDP
Восприятия/транспортный		Transport Layer Security (TLS)	Обеспечивает криптографическую защиту обмена по TCP
Восприятия/ транспортный		Datagram TLS (DTLS)	Осуществляет защиту приложений на основе диаграмм, в т.ч. UDP

EPCglobal

Электронный код продукта (EPC) – это уникальный идентификационный номер (ИН), хранящийся в метке RFID, по которому опознается продукт в цепи поставки. Данные, поступающие с метки и считывающего устройства, хранятся в интернете. Благодаря поддержке объектных ИН и функции обнаружения сервисов, а также открытости, масштабируемости и надежности, EPCglobal является перспективным стандартом.

Long Term Evolution-Advanced (LTE-A)

Набор протоколов сотовой связи LTE-A подходит как для машинных сетей, так и для IoT. По стоимости и масштабируемости он выгодно отличается от других протоколов сотовой связи. Последние улучшения в LTE Category M и NarrowBand IoT (NB-IoT) позволяют еще больше увеличить срок службы от батареи, повысить скорость передачи и качество связи. Это перспективный стандарт для системы «умный город».

Z-Wave

Протокол Z-Wave предназначен для сетей бытовой автоматизации (сети HAN). Он широко применяется в небольших коммерческих доменах, а также в приложениях дистанционного контроля в умных домах. Z-Wave имеет дальность покрытия около 30 м (точка–точка) и используется в приложениях, где требуется передача малого количества данных, например в системах управления освещением, бытовыми устройствами, энергопотреблением и HVAC, контроля доступа, для управления носимыми датчиками, обнаружения возгорания. В таблице 5 показаны особенности основных протоколов.

Безопасность

Помимо выбора протокола важны вопросы безопасности передачи и взаимодействия узлов. В настоящее время протоколы защиты данных в интернете работают на больших устройствах, таких как компьютеры или ноутбуки. Для узлов IoT требуются принципиально другие протоколы общей защиты. Особенно это касается простых устройств с ограниченными ресурсами. В таблице 6 приведены некоторые решения для разных уровней IoT.

Функциональная совместимость (IEEE 1905.1)

Стандарт IEEE 1905.1 был разработан для конвергенции цифровых бытовых сетей с гетерогенными технологиями. Не требуя изменения расположенных ниже слоев, он предоставляет уровень абстракции, который позволяет скрыть различия между топологиями управления доступом к среде (MAC). Протокол также предлагает единый интерфейс для общераспространенных домашних сетей, обеспечивая сосуществование протоколов физического уровня и протоколов передачи данных. В качестве примера можно привести IEEE 1901 для сетей питания, Wi-Fi/IEEE 802.11TM для радиоканалов, Ethernet для витой пары или оптоволоконного кабеля, MoCA 1.1 для коаксиального кабеля.

ВЫВОДЫ

Итак, мы рассмотрели протоколы, которые применяются на разных уровнях интернета вещей. Несмотря на то, что IoT в целом способствует повышению качества жизни, остаются некоторые опасения, связанные, в частности, с экологическими вопросами. Таким образом, технологии IoT, обеспечивающие безопасную и надежную передачу данных, должны развиваться в сторону снижения негативного воздействия на окружающую среду. В настоящее время разрабатываются технологии использования энергии из возобновляемых источников.

Меры противодействия несанкционированному доступу к данным должны постоянно совершенствоваться, поскольку речь идет о масштабной системе, объединяющей миллионы узлов. Одна DDoS-атака может привести к непоправимым последствиям: утечка данных может затронуть не только персональную жизнь отдельных пользователей, но и повлечь за собой значительные финансовые потери предприятий и даже государств.

Еще одним важным вопросом является обеспечение энергоэффективности. Чем больше узлов и чем больше объем передаваемых данных, тем больше энергопотребление. Одной из задач, которую предстоит решить, является уменьшение энергопотребления.