



ГЛАВА 3.³ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ

*ПРОБЛЕМИ ВИКОРИСТАННЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ
PROBLEMS OF USING THE INTERNET OF THINGS NETWORKS*

DOI: 10.30888/2663-5569.2021-19-01-009

Введение

Широкое распространение высокоскоростного интернета, беспроводных сетей, а также носимых устройств позволило объединить все устройства, которые так или иначе могут быть подключены к беспроводной сети, воедино. При помощи смартфона можно посмотреть состояние автомобиля, количество бензина в баке и даже завести его прямо из квартиры. Входные двери также могут быть открыты при помощи смартфона, холодильник может присылать сообщения об испорченных продуктах, а мелкая кухонная техника может быть включена дистанционно, чтобы ужин или кофе были готовы уже к вашему приезду домой с работы. Подобные объединения и взаимодействия названы Интернет вещей или IoT (Internet of Things). И интернет вещей имеет определённый набор моделей и алгоритмов информационного взаимодействия.

3.1. Основные понятия и требования относящиеся к IoT

Основной идеей Интернета вещей является предоставление возможности взаимодействия различных предметов, окружающих человека, передачи созданной ими информации и обеспечении бесперебойного соединения. Взаимодействие между этими вещами происходит за счёт существующих и разрабатываемых информационно-коммуникационных технологий. Технология информационной коммуникации состоит из совокупности нескольких составляющих: сенсоры (датчики), данные, сети и услуги. Помимо уже имеющихся требований к сетевым и инфокоммуникационным технологиям, которые должны обеспечить надёжное соединение и подключение к сети в любое время и в любом месте, для IoT добавляется требование обеспечить связь с любой вещью. Это подразумевает под собой соединение и информационный обмен как между подключёнными к сети вещами, так и взаимодействие этих вещей с человеком.

Требование к взаимодействию можно рассмотреть на простом примере. Допустим вы установили у себя дома умное освещение и умный проектор и решили посмотреть фильм. При должной настройке взаимодействия устройств друг с другом, в момент включения проектора свет будет автоматически отключаться, а полотно для вывода изображения с проектора само по себе выдвигаться. После того как всё готово вы выбираете на своём смартфоне фильм и выводите его на проектор по беспроводному подключению. Таким

³ Авторы: Львович И.Я., Львович Я.Е., Преображенский А.П., Преображенский Ю.П.



образом вам пришлось сделать всего два действия – включить проектор и фильм на смартфоне, все остальные действия были произведены автоматически. В этом примере взаимодействие вещей друг с другом показано в автоматическом отключении освещения и выдвижении полотна. В момент включения проектора запустился сценарий, который подал сигнал с проектора на освещение и полотно, что вы собираетесь посмотреть фильм и свет будет мешаться, а без полотна будет некуда вывести изображение. А взаимодействием вещи с человеком является беспроводное подключение проектора к смартфону через Wi-Fi и вывод изображения с экрана смартфона на проектор. И подобный пример взаимодействия лишь один из множества возможных сценариев, которые могут быть настроены внутри сети Интернета вещей.

Технологии Интернета вещей пока находятся на ранних этапах реализации и исследований, однако уже принимают характеристики сформированной технологии. В настоящий момент международные эксперты активно работают над стандартизацией архитектуры, компонентов и приложений. Помимо стандартизации составляющих элементов, необходимо также проработать новые модели и алгоритмы, которые могут помочь в оптимальном проектировании Интернета вещей учитывая особую специфику инфокоммуникационного взаимодействия внутри IoT. В моделях IoT для всех физических вещей, как минимум, необходимо наличие элементов позволяющих производить коммуникацию, а также возможность сбора, хранения и обработки получаемых с датчиков данных.

Информационное взаимодействие между вещами определяется спецификой фундаментальных характеристик Интернета вещей. К ним относятся: связность, гетерогенность, обеспечение вещей услугами, динамические изменения и большое количество вещей. Это определено на основе рекомендаций Международного Союза Электросвязи (МСЭ).

В связи с указанными особенностями применение методов и алгоритмов, на основе которых происходит функционирование традиционных компьютерных сетей, не представляется возможным для Интернета вещей. И во время проектирования IoT необходимо принимать во внимание данные обстоятельства, а также специфику их работы. В связи с чем для обеспечения оптимальных решений, позволяющих организовать информационное взаимодействие, необходимо искать и прорабатывать новые методы и алгоритмы учитывающие условия функционирования IoT. Сложности к моделированию систем Интернета вещей, помимо уже описанных фундаментальных характеристик, добавляет еще и то, что необходимо постоянно учитывать случайные факторы, которые возникают во время информационного взаимодействия.

3.2. Метод построения математической модели IoT

Есть множество различных методов, которые используются при



построении математических моделей, а также различных средств для реализации моделирующих алгоритмов. Но среди них особо выделяется класс имитационных моделей. Данная модель является программой, воспроизводящей пошагово те события, которые происходят в реальных системах. Касательно IoT имитационные модели создают процессы, которые генерируют сообщения от приложений, разбивают эти сообщения на различные пакеты, а также кадры различных протоколов. Воспроизводятся также и задержки, которые связаны с обработкой сообщений, пакетов или кадров, проходящих внутри операционной системы, а также, моделируются процессы получения доступа вещей к сети и многое другое.

Для исследуемых систем одним из преимуществ использования имитационных моделей является предоставление возможности подмены процесса смены событий от масштаба реального времени на более ускоренные по ходу работы программы. Результатом такой подмены является возможность в течение нескольких минут воспроизвести процесс работы ране смоделированной системы, а также оценить процесс работы в диапазоне широко варьируемых параметров. Во время имитационного моделирования появляется возможность воспроизведения реальных процессов, исследовать особые случаи, воспроизвести как реальные, так и гипотетические критические ситуации. Главное преимущество данного способа моделирования — это возможность проведения различных экспериментов над исследуемыми объектами, без прибегания к физической реализации, что может помочь в предсказании и предотвращении большого количества неожиданных ситуаций, которые могут возникнуть во время эксплуатации и возникновение которых привело бы к неожиданным затратам. Результат работы имитационной модели — это статистические данные про самые важные характеристики смоделированной системы, которые были собраны во время наблюдения за происходящими событиями. К этим данным относятся: временные показатели, величина загрузки на каналах и узлах, вероятности потерь и многое другое.

3.3. Организация сети и технология построения IoT

Для того чтобы достичь поставленные цели в технологиях IoT, а точнее объединить разнообразные сенсоры и датчики, а также гетерогенные и сенсорные компьютерные сети, необходимо построить определённую архитектуру. По рекомендации МСЭ-Т функционал Интернета вещей делится на четыре уровня:

- Уровень взаимодействия со средой
- Сетевой уровень, который отвечает за передачу данных внутри сети
- Сервисный уровень, обрабатывающий и преобразующий информацию
- Уровень взаимодействия с пользователем и приложениями

Подобная архитектура способна удовлетворять основным системным характеристикам для сети IoT, таким как лёгкость модернизации, масштабируемость сети, модульность, а также способна отвечать требованию



адаптивности, что может позволить сенсорам адаптироваться под изменения или изменять саму сеть, в зависимости от условий, в которых она функционирует. С точки зрения системного анализа, во время проектирования сети IoT необходимо в первую очередь определить топологию, а также структуру и состав элементов, взаимосвязи между элементами, которые являются наиболее важными, сформулировать назначение и основные задачи, показатели и критерии рациональной организации информационного обмена.

Технологии Интернета вещей берут своё начало от территориально-распределённых сенсорных сетей, которые изначально развивались как локальные сети, а уже впоследствии имели выход в глобальные сети Интернет и GSM. Сенсорные сети определяются как распределённые сети, которые состоят из небольших беспроводных узкоспециализированных узлов, которые в огромном количестве случайно рассредоточены на какой-то поверхности или области. Исходя из этого можно судить, что работа сенсорных сетей основана на совместном взаимодействии большого количества миниатюрных узлов, иначе говоря, сенсорных устройств, которые распределены в определённой области с высокой плотностью. Область покрытия каждого радиосигнала сенсорных устройств должна иметь как минимум ещё и соседнее устройство. Большое количество соседних устройств будет означать гораздо более высокую точность и надёжность, которой будет обладать сенсорная сеть. Технологии радиодоступа, которые применяются в подобного рода устройствах должны быть основаны на стандарте IEEE 802.15.4, который позволяет передавать данные на большие расстояния и могут достигать несколько десятков метров.

Состав сенсорных устройств включает в себя 4 основных компонента. Они включают в себя блоки сбора, передачи данных, обработки и питания. Помимо этого, в составе таких устройств могут находиться модули, определяющие местоположение, а также силовые генераторы и мобилизаторы. Наличие одного из этих компонентов определяется целями, для которых создаётся сенсорная сеть.

Модуль сбора данных должен состоять из датчика, а также аналого-цифрового преобразователя (АЦП). Аналоговый сигнал, который выдаётся датчиком по результатам наблюдаемого явления, при помощи АЦП преобразуется в цифровой сигнал, после чего он подаётся в блок обработки.

Модуль обработки, который должен состоять из процессора и памяти, способен реализовать процедуры, позволяющие вместе с другими узлами выполнить те задачи наблюдения, которые были поставлены. За счёт наличия данного модуля в составе сенсорного устройства вместо передачи исходных данных, они, при помощи простых вычислений, обрабатываются, после чего передаются необходимые данные в частично обработанном виде.

Большинство сенсорных устройств нуждается в определении своего местоположения с большой точностью. И именно для этой цели в их схему интегрирован модуль, определяющий местоположение. В том случае, если устройство нуждается в перемещении, то в его схему добавляется также и мобилизатор. А передатчик, или, иначе говоря, трансивер, должен образовать интерфейс датчика с сетью.



Все описанные модули должны быть размещены в одном корпусе. Корпуса устройств могут быть самых разных размеров, от сравнительно крупных до совсем миниатюрных, в зависимости от устройства, в котором они находятся, но при этом они должны быть достаточно компактными и лёгкими. Также, помимо требования к размеру, для сенсорных устройств есть и другой ряд требований, среди которых:

- Обладание низким энергопотреблением
- Взаимодействие с большим количеством других устройств на небольших расстояниях
- Низкая себестоимость
- Возможность поддерживать работоспособность в автономном режиме
- Адаптация к окружающей среде

Ещё один основной элемент в таких устройствах – это блок питания. Ввиду того, что сенсорные устройства периодически становятся недоступными за счёт перехода в спящий режим, то элементы питания могут определять жизненный цикл подобных устройств. Для беспроводных датчиков внутри интегрированной сети (WINS) средний уровень заряда, который способен обеспечить работоспособность в течение длительного времени, должен составлять менее 30 ЛА. Увеличение эксплуатационного срока для сенсорных сетей возможно за счёт подзаряжаемых аккумуляторов. Аккумуляторы, используемые в таких устройствах, с целью обеспечения более низкого энергопотребления, способны брать энергию в том числе и при помощи окружающей среды, например за счёт солнечных панелей.

Передачики у сенсорных устройств могут быть пассивными или же наоборот активными оптическими устройствами, а также радиочастотными передатчиками. Для обеспечения радиочастотной передачи необходимо применить процессы модуляции сигнала, которые работают на определённой полосе пропускания, а также фильтрация и демодуляция. Их реализация в сенсорных устройствах делает такие устройства более сложными и дорогими. Более того, во время передачи данных между двумя узлами возможно столкнуться с потерями, за счёт того, что антенны располагаются близко к земле. Но, несмотря на это, использование радиосвязи более предпочтительно, ведь передача данных происходит на более низких частотах (зачастую менее 1 Гц), а также из-за частой периодичности циклов передачи за счёт малых расстояний.

Кроме уже рассмотренной классической технологии построения сенсорных устройств возможны и другие. Это вызвано в том числе и тем фактором, что устройству будет необходимо не только мониторить и контролировать измеряемые характеристики, но и воздействовать на измеряемый объект. Элемент, который даёт возможность воздействовать на объект, называется актором. От сенсорных узлов архитектура акторов отличается тем, что в нём должен присутствовать активный элемент, способный взаимодействовать с внешней средой при помощи контроллера принятия решений, которое получает данные о воздействии внешней среды.



Также к особенностям сенсорных сетей можно отнести совместную работу отдельных устройств, за счёт наличия в них модуля обработки. На текущий момент процессоры становятся всё меньше по своим габаритам, при этом увеличивая собственную мощность. Однако, несмотря на это, для сенсорных устройств сохраняется проблема с обработкой и хранением данных. Многие задачи, которые связаны с мониторингом нуждаются в определении местоположения используемого устройства. Как правило для достижения этой задачи в узлы системы встраиваются модули GPS, которые могут работать с точностью до 5 метров.

Одной из ключевых особенностей сенсорных устройств является то, что они не нуждаются в предварительном расчёте размещения устройства. За счёт этого можно добиться размещения устройств хаотичным образом, а также расположить их в труднодоступных местах и оперативно развернуть сеть, в случае если необходимо её временное размещение на каких-то позициях.

Внутри одной сенсорной сети устройства, взаимодействуя друг с другом, образуют топологию mesh. Это означает, что объединение сенсорных устройств происходит за счёт многочисленных соединений, которые образуют топологию в виде ячеек. Топология mesh в самоорганизующихся сетях открывает ряд возможностей, к которым можно отнести:

- Возможность создавать зоны, которые будут обладать сплошным информационным покрытием на большой площади
- Увеличивать площадь зоны покрытия, а также плотность информационных потоков в режиме самоорганизации за счёт масштабируемости сети
- Использование для связи беспроводных транспортных каналов, которые могут работать в режиме «каждый с каждым»
- Устойчивость сети к потере отдельных элементов

К технологиям используемым в IoT можно также отнести M2M (Machine to Machine). Это обобщающее название для тех технологий, которые позволяют производить информационный обмен между машинами, а также автоматическую передачу информации между устройствами в одностороннем порядке и без человеческого вмешательства. К ним могут относиться как проводные, так и беспроводные системы, которые занимаются мониторингом датчиков, а также параметров различных устройств. Распространённость и совершенство технологии M2M позволяет применять её в различных мобильных устройствах, а также в узлах сенсорных сетей. Эта технология напрямую относится к Интернету вещей, так как она представляет под собой особую вычислительную среду, которая состоит из устройств способных взаимодействовать между собой самостоятельно и предоставлять пользователю результат, полученный в процессе совместной работы.

Архитектура Интернета вещей демонстрирует нам то, как инфокоммуникационные технологии, которые обеспечивают функционирование IoT, связаны между собой. Она содержит в себе 4 основных функциональных уровня.

Уровень взаимодействия со средой, который также включает в себя



сенсоры и сенсорные сети, является нижним уровнем в архитектуре Интернета вещей. Он состоит из различных смарт-объектов, которые интегрированы в сенсорные устройства. Сенсоры способны реализовать соединение физических, а также виртуальных миров, которые способны обеспечить сбор и обработку данных в реальном времени. Большинство из них нуждаются в постоянном соединении со шлюзом, которые можно реализовать при помощи локальных вычислительных сетей, как например Ethernet, Wi-Fi или PAN.

На сетевом уровне обеспечивается транспортировка больших объёмов данных, которые создаются большим количеством сенсорных устройств на первом уровне Интернета вещей. Он состоит из конвергентной сетевой инфраструктуры, созданные благодаря соединению разнородных сетей воедино.

Уровень сервиса содержит в себе набор различных информационных услуг, которые способны автоматизировать разнообразные технологические бизнес-процессы в сетях IoT. К их числу можно отнести аналитическую обработку полученной информации, поддержку и управление операционными, а также бизнес-процессами, сбор и хранение информации, осуществление информационной безопасности и многое другое.

На уровне приложений находятся разнообразные типы приложений, которые предназначены для определённых промышленных секторов, а также различных сфер деятельности. Приложения делятся на две основные группы: вертикальные и горизонтальные. Вертикальные приложения специфические и предназначены для какой-то конкретной отрасли промышленности. А горизонтальные приложения используются в разных сферах экономики.

Проведем анализ способов взаимодействия внутри сети IoT. Как правило для сетей IoT выбирают среди трёх способов взаимодействия: прямой, посредством шлюза и посредством сервера. Если был выбран прямой доступ, то обращение к вещи происходит за счёт клиентского приложения, при помощи IP-адреса, который идентифицирует устройство. Интерфейс, который взаимодействует с вещами в сети, представлен в виде графического web-интерфейса, управляемого при помощи браузера. Однако, у данного способа есть и свои недостатки. Среди них можно выделить то, что необходимо постоянно фиксировать адресацию подключённых вещей, а это в свою очередь означает зависимость от того провайдера, который предоставляет доступ к глобальной сети. Данную проблему можно решить при помощи алиаса, но этот способ несовершенен, так как увеличивает время взаимодействия, из-за того, что устройствам требуется обращение к прокси-серверу, чтобы идентифицироваться по имени. Помимо этого, число подключений устройств для передачи данных ограничено. Это связано с тем, что устройства обладают низким качеством связи и невысокими вычислительными мощностями. Решить данную проблему можно при помощи подключения устройства к стабильному источнику сети Интернет, но при этом придётся пожертвовать мобильностью.

Альтернативой данному способу может служить взаимодействие посредством шлюза. Данный способ более рационален и на текущий момент способен заменить прямой доступ, в особенности в тех случаях, когда



необходимо организовать связь туманных и облачных вычислений. За счёт того, что большинство стандартов беспроводных сенсорных сетей не способны поддерживать протокол IP, а используют свои собственные протоколы малого радиуса действия, это обязывает использовать специальный узел – ретранслятор, который предаёт данные из сенсорной сети в Интернет, чтобы согласовывать протоколы. Недостатки такого подхода схожи с методом взаимодействия по прямому доступу, но в отличие от него распространяются только на шлюз.

В том случае если доступ организуется за счёт сервера, то всё взаимодействие выполняется также на сервере. К его функциям относятся:

- Приём и передача сообщений от устройств к пользователям
- Обработка и хранение полученной информации
- Наличие пользовательского интерфейса, с целью обеспечения двустороннего обмена между пользователями и устройствами

Это наиболее рациональный и применяемый способ доступа, так как он способен переносить нагрузку, которая связана с обработкой пользовательских запросов на централизованном сервере. Это позволяет разгрузить маломощные радиоканалы между подключёнными вещами на проводные каналы, которые находятся между пользователем и сервером. Кроме тех достоинств, которыми обладает метод доступа, на сервере есть возможность подключения сервисов по хранению и обработке данных, а также использовать облачные вычисления. Тем не менее, это по-прежнему позволяет использовать шлюзы, способные организовать связь между сервером и локальными беспроводными сетями. Рассмотрим эти способы более подробно.

Рассмотрим взаимодействие посредством шлюза. В Интернет-сетях шлюз предназначен для того, чтобы объединить сенсорные и глобальную сети, а также чтобы организовать связь с конечным пользователем. Шлюз – это центральный узел, который имеет аппаратно-программные средства, позволяющие работать с различными технологиями беспроводного доступа, среди которых GPS, Bluetooth, Wi-Fi, WiMAX и мобильные сети GSM. Вариантов, благодаря которым можно построить шлюзы, может быть несколько.

Одним из них является использование компьютера, подключённого к сенсорной сети. В рамках этой сети компьютер будет являться точкой, которая способна предоставить доступ к WAN (Wide Area Network) или, иначе говоря, глобальной сети. Такой подход имеет свои недостатки, к которым можно отнести неоправданно высокую стоимость и громоздкость самой сети. Ещё один критерий, который должен соблюдаться устройствами в сетях IoT – это автономность. Автономность начинает теряться в случае, если была сенсорная сеть была организована по территориально-распределённому принципу, так как появляется зависимость от электричества и точки, предоставляющей доступ к Интернету.

Ещё одним вариантом будет использовать выделенный узел-шлюз, который будет являться посредником в соединении сенсорных сетей и ближайших проводных сетей с выходом в Интернет, например Ethernet-сетью.



Структура шлюза состоит из приемопередатчика, который должен быть совместим с той сенсорной сетью, с которой его объединяют, порта Ethernet, необходимого для подключения к проводной сети, а также микроконтроллера, который будет выполнять функционал по преобразованию пакетов из формата одной сети в другой. Этот вариант отличается более низкой себестоимостью по сравнению с первым, а также более компактными размерами. Однако этот способ будет нуждаться в более высоком энергопотреблении, за счёт того, что обычные проводные сети не предназначены для работы при низких уровнях сигнала и низких уровнях энергопотребления. Более того, подобное устройство не гарантирует, что в ближайшей к нему проводной сети будет в наличии точка доступа.

Существует также и третий способ, суть которого заключается в том, чтобы использовать автономный узел-шлюз, который может самостоятельно предоставить точку доступа к сети Интернет. Это становится возможным за счёт использования технологий беспроводной передачи данных. Узел поделён на две логические части: совместимый с сенсорной сетью приемопередатчик, а также приемопередатчик, который должен быть совместим с определённой глобальной беспроводной сетью, в которую попадает область действия сенсорной сети. К таким сетям относятся GSM и WiMAX, но сеть GSM более экономична по своему энергопотреблению.

Помимо этого, существуют шлюзы, которые способны предоставить сенсорным сетям доступ к ближайшим беспроводным сетям Wi-Fi, с той целью, чтобы найти точку доступа к сети Интернет.

Исходя из этого можно судить, что в случае необходимости организации полностью автономной территориально-распределённой сети Интернета вещей следует использовать третий способ. А в том случае, когда использование сети IoT в рамках другой крупной проводной сети, то необходимость в автономности отпадает и можно пользоваться любым из первых двух способов.

Рассмотрим взаимодействие посредством сервера. Централизованный сервер управления устройствами в сети Интернета вещей способен выполнять функционал по сбору, хранению и обработке поступающей от устройств информации, а также искать, контролировать и визуализировать информацию для пользователя. Централизованный сервер состоит из следующих компонентов:

- Модуль обработки информации
- База данных, в которой хранится собранная информация
- Необходимы для взаимодействия с устройствами интерфейс (протокол которого поддерживается всеми устройствами)
- Систему, контролирующую доступ пользователя к устройствам, а также управляющую их иерархией, возможными функциями и параметрами

Система контроля доступа может быть вынесена на отдельном сервере и располагаться в особой системе управления, чем отделяет базу, хранящую собранные данные от базы управляющей устройствами.

Модуль обработки информации предназначен для распаковки сжатой информации с целью ускорения её транспортировки, выполнения логических и



арифметических вычислений, преобразования полученной информации к понятному для восприятия формату и её классификации.

Для того чтобы хранить собранную датчиками информацию при мониторинге объектов и для возможности предоставить пользователям актуальную собранную информацию используется база данных.

Управление устройствами происходит при помощи серверных средств. Пользователь посылает команду на управляющий сервер, а сервер впоследствии передаёт её адресату. Набор управляющих команд должен быть общим для всех устройств и минимальным, для того чтобы обеспечить разделение управления и данных. Это может помочь в упрощении информационного обмена между пользователем и устройствами, а также в стандартизации методов взаимодействия в IoT и создании общего центра управления.

Разделение управляющей информации и данных предполагает, что будет выделен минимальный набор команд и сущностей, с которыми может быть произведено выполнение этих команд. Отключение освещения, включение электроприбора или изменение температуры на кондиционере подразумевает под собой выполнение одной и той же команды – смены режима работы. В этом случае данными будет являться информация о текущем состоянии устройства. Для того чтобы получить информацию требуется узнать то состояние, в котором сейчас находится устройство или его отдельная составляющая часть.

Реализуя взаимодействие между вещами в сетях Интернета вещей при помощи централизованного сервера, можно рассматривать два варианта топологии: реальная, она же физическая, и виртуальная, или, иначе говоря, логическая. Для физической топологии в сетях Интернета вещей используется тип «звезда». В данной топологии датчики и шлюзы сконцентрированы вокруг сервера и образуют подобие звезды, в центре которой находится сервер.

В логической топологии используется тип сети mesh. Два устройства соединяются между собой и взаимодействуют как с локальным беспроводным каналом, так и с внешним, при помощи сервера управления, образуя тем самым логическое соединение. Взаимодействие между вещами абсолютно прозрачно и не зависит от того, как они расположены территориально. Это достигается при помощи протоколов взаимодействия.

Рассмотрим облачные технологии в сетях IoT. Идея Интернета вещей подразумевает под собой не только сбор информации от отслеживаемых объектов и управление ими, но также и обмен данными между объектами, перераспределение и планировка задач, учитывая доступность сервисов, которые находятся в зоне действия объектов. Устройства в сети Интернета вещей должны обладать возможностью самоорганизовываться для объединения в локальные беспроводные сети, с целью совместного решения задач.

При помощи IoT можно решать некоторые сложные задачи, требующие больших вычислительных ресурсов. Одним из таких примеров может служить обработка видео в реальном времени, когда локальная беспроводная сеть объединяется с облачными вычислительными ресурсами. Облачные технологии в IoT можно поделить на два типа: облачные вычисления (Cloud Computing) и



туманные вычисления (Fog Computing).

Облачные вычисления представляют собой модель, обеспечивающую удобный сетевой доступ по требованию к определённому общему фонду сконфигурированных вычислительных ресурсов, к которым относятся сети передачи данных, серверы, устройства хранящие данные, приложения и сервисы – как вместе, так и отдельно и могут оперативно предоставляться провайдером с минимальными затратами на эксплуатацию. Облачные вычисления реализуются при помощи сетевой инфраструктуры центров обработки данных.

Туманные вычисления также являются одной из разновидностей облачных сервисов, однако они расположены не в самом облаке, а в окружающей среде, к примеру на соседнем сервере. Туманные вычисления реализованы при помощи локальных сетей, интегрированных в IoT. Они являются дополнением к облачным вычислениям, реализуя задачи, которые требуют значительное количество компьютерных ресурсов. Концепция подобного рода вычислений предполагает под собой децентрализованную обработку данных, за счёт частичной передачи функционала по обработке данных с облака прямо на вычислительные ресурсы локальной сети (туману).

Туманные вычисления определяются как виртуализированные платформы, способные поддерживать три основных типа сервисов, которые соответствуют концепции M2M: вычисления, хранение и передачу. Задачей туманных вычислений является обеспечение взаимодействия между множеством датчиков и облаком. Число элементов в тумане не постоянно и может варьироваться в пределах от 0 до некоторого N_{\max} . Туманные вычисления – это беспроводные сенсорные сети, которые характеризуются самоорганизацией и у них нет общей инфраструктуры, кроме шлюзов предназначенных для связи с другими сетями. Каждый из узлов в сенсорной сети может функционировать в качестве оконечного или транзитного узла. На практике же передача данных в этих сетях происходит за счёт их пошаговой передачи к ближайшему узлу. Шлюз в данном типе вычислений выступает в роли агрегирующего узла, который накапливает данные различных устройств и в дальнейшем передаёт их на сервер. Также, он выступает в роли координатора сенсорной сети.

Рассмотрим протоколы взаимодействия в IoT. Для решения задач, которые ставятся в инфраструктуре Интернета вещей, можно выделить следующие группы протоколов:

- Протоколы по сбору данных датчиками и их передача серверам
- Протоколы, соединяющие устройства с пользователями или же в частных случаях пользователей с сервером
- Протоколы, соединяющие между собой сервера

Существует несколько разных способов их реализации. Выбор протоколов и их применение определяется в зависимости от нагрузки на сеть, аппаратного обеспечения и архитектуры сети IoT.

Одним из основных протоколов является CoAP (Constrained Application Protocol) – это ограниченный протокол передачи данных, схожий с HTTP, но он больше адаптирован для работы с сенсорными устройствами, обладающими



низкой производительностью.

Также можно выделить протоколы MQTT (Message Queue Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) – которые обеспечивают обмен сообщениями с применением брокера. Они реализуют модель типа «издатель-подписчик». «Издатель» отправляет сообщение, публикующееся в централизованном сервисе – брокере сообщений, а «подписчик» в свою очередь получает от брокера сообщение. Для того, чтобы использовать брокера необходимо подписаться на некоторые темы сообщений, которые публикуются.

На текущий момент MQTT один из наиболее распространённых протоколов, использующихся в организации инфраструктуры Интернета вещей. Это связано с низкими накладными расходами, за счёт хорошо продуманного формата заголовков, что позволяет снижать расход энергии аккумуляторов и увеличивать количество сообщений, которые передаются в одну единицу времени. Этот протокол создан специально для того, чтобы преодолевать ограничения, связанные с подключением стремительно увеличивающегося количества датчиков, приводов, микрокомпьютеров и носимых устройств.

В протоколе XMPP между точками доступа обеспечивается обмен текстовыми сообщениями. В качестве встроенного типа в нём используется текстовый формат XML, что обеспечивает естественную связь между пользователями. Так же, как и MQTT он работает по TCP. Преимущество этого протокола заключается в методе адресации вида `example@domain.ru`, что позволяет объединить пользователей в пространстве глобальной сети Интернет. В случае с Интернетом вещей это добавляет удобства в тех случаях, когда приходится передавать данные между отдалёнными, зачастую независимыми точками. Однако этот протокол не наделён большими скоростями и зачастую используется в качестве опроса или проверки по требованию. Преимуществом протокола XMPP является возможность подключения устройства к веб-серверу, что позволяет подключаться к нему при помощи смартфона. Также к преимуществам можно отнести масштабируемость, адресацию и безопасность, что делает его лучшим решением в клиентоориентированных приложениях IoT.

Протокол AMQP (Advanced Message Queuing Protocol, или усовершенствованный протокол организации очереди сообщений) порой рассматривается как протокол IoT. Следуя из названия, этот протокол занимается исключительно обслуживанием очереди, пересылая между различными серверами транзакционные сообщения. Много внимания в AMQP уделяется борьбе с потерей сообщений. Разные линии коммуникации, в число которых входят поставщики контента, коммутаторы, списки очередности и даже пользователи, пользуются протоколом TCP, обеспечивающим двухточечное соединение высокой надёжности. Помимо этого, конечные точки подтверждают принятие всех сообщений. В этом стандарте также описывается и опциональный режим транзакции, обладающий формальной последовательностью многофазного обновления транзакций. Для AMQP ПО фиксируется на отслеживании всех сообщений и обеспечивает их доставку по назначению, вне зависимости от сбоя или перезагрузки системы. В основном



AMQP используется для обмена деловыми сообщениями и в Интернете вещей идеален для того, чтобы реализовать аналитические функции на серверах.

Связь в IoT реализуется при помощи Wi-Fi, свода стандартов беспроводной связи IEEE 802.11, используемой в построении локальных беспроводных вычислительных сетей в стеке TCP/IP. Стандарт IEEE 802.11 состоит из стека протоколов физического и канального уровней, имея также в себе подуровни управляющие доступом к среде и логической передачей данных. Этот протокол также находится и на сетевом уровне интерфейсов стека TCP/IP. Подключение беспроводных сетей Wi-Fi происходит при помощи шлюза или маршрутизатора. Организацией Wi-Fi Alliance была создана новая спецификация беспроводных сетей IEEE 802.11s, специально для построения в рамках IoT. Эта спецификация способна обеспечить технологию построения ячеистых сетей. Ещё одним новым стандартом, работающим в спецификации IEEE 802.11ah, стал Wi-Fi HaLow, отличающийся более низким энергопотреблением.

Выводы

По результатам проведённых исследований и изучения IoT можно сделать вывод, что Интернет вещей плотно проник и продолжает проникать в нашу жизнь. И рано или поздно в каждом доме будет набор из смарт-девайсов, которые существенно упростят нашу жизнь. Но для того, чтобы эти устройства работали правильно и стабильно, необходимо грамотно организовать сеть Интернета вещей на основе имеющихся и развивающихся алгоритмов и моделей построения. Самыми основными задачами является обеспечение доступа, информационного взаимодействия и самоорганизации устройств в сети.