GeekBrains

Кибернетика умных устройств

Технологии передачи данных в IoT

Оглавление

Введение

На данном занятии мы рассмотрим современные протоколы передачи данных; какие типы беспроводных протоколов существует: отличие LPWAN от WLAN систем. Разберем самые популярные протоколы и технологии передачи данных, а также изучим протоколы взаимодействия самих устройств.

Типы протоколов

Протоколы данных и сетевые протоколы необходимы для IoT, поскольку они обеспечивают связь между устройствами и системами стандартизированным и эффективным образом.

Протоколы данных

Протоколы передачи данных, такие как MQTT, CoAP, AMQP и iBeacon, определяют формат, структуру и правила обмена данными между устройствами, приложениями и сервисами IoT. Они обеспечивают безопасную, надежную и эффективную передачу данных независимо от типа данных, местоположения устройств и состояния сети. Протоколы данных также поддерживают различные схемы передачи данных, такие как публикация-подписка, запрос-ответ и событийно-ориентированные, что очень важно для приложений IoT, требующих обработки данных в реальном времени, аналитики и принятия решений.

Протоколы передачи данных являются важной частью экосистемы Интернета вещей (IoT), поскольку они позволяют устройствам обмениваться данными и общаться друг с другом. Существует несколько типов протоколов передачи данных, используемых в IoT, каждый из которых имеет свои уникальные особенности и преимущества.

Одним из наиболее широко используемых протоколов передачи данных в IoT является MQTT (Message Queuing Telemetry Transport). MQTT – это легкий протокол обмена сообщениями, который разработан для обеспечения эффективности, надежности и безопасности. Он использует схему публикации/подписки сообщений, при которой сообщения отправляются в определенные темы, а устройства, заинтересованные в этих темах, могут подписаться на получение этих сообщений. В качестве примера можно привести облачное дисковое хранилище, где есть группа людей с доступом к какой-либо папке. Как только администратор загрузит файл в эту папку, он сразу же станет доступен всем участникам. Только в mqtt вместо папки - топик, а вместо файла - сообщение с данными. Если говорить о самом mqtt, то представьте себе систему умного дома, светильники которого подключены к различным топикам, каждый из которых ответственен за определенную комнату. Вы в приложении нажимаете на кнопку “включить свет в гостинной”, и все устройства в гостинной включают свет.

Другим широко используемым протоколом передачи данных является CoAP (Constrained Application Protocol). CoAP – это легкий протокол, предназначенный для использования в средах с ограниченными ресурсами, таких как устройства IoT с ограниченной вычислительной мощностью и памятью. Он использует модель

клиент/сервер и поддерживает различные методы взаимодействия с ресурсами, такие как GET, PUT, POST и DELETE.

AMQP (Advanced Message Queuing Protocol) – еще один популярный протокол передачи данных, который используется в IoT. Это протокол обмена сообщениями, который разработан для обеспечения надежности и совместимости с широким спектром платформ и языков программирования. AMQP поддерживает различные схемы обмена сообщениями, включая "точка-точка" (напрямую устройству) и "публикация/подписка", и может использоваться как с TCP/IP, так и с другими транспортными протоколами.

iBeacon – это собственный протокол, разработанный компанией Apple, который используется для предоставления услуг, основанных на определении местоположения. Он разработан для работы с Bluetooth Low Energy (BLE) и использует широковещательную схему передачи сообщений, когда устройство посылает сигнал, который может быть принят другими устройствами, находящимися поблизости. iBeacon обычно используется в розничной торговле для отправки целевой рекламы и рекламных акций покупателям на основе их местоположения в магазине.

Каждый из этих протоколов передачи данных имеет свои сильные и слабые стороны, а также конкретные случаи использования, когда он наиболее эффективен. Понимание характеристик каждого протокола важно для разработки и внедрения систем IoT, которые могут эффективно обмениваться данными.

Сетевые протоколы

С другой стороны, сетевые (и беспроводные) протоколы, такие как Wi-Fi, Bluetooth, ZigBee, LoRaWAN, SigFox, NB-IoT и RFID, обеспечивают инфраструктуру и средства для подключения устройств IoT к Интернету, облаку или другим устройствам. Они определяют правила и стандарты передачи данных по различным типам беспроводных и проводных сетей, таких как сотовая связь, Wi-Fi, Ethernet и LPWAN. Сетевые протоколы также обеспечивают связь устройств IoT друг с другом и с другими устройствами независимо от производителя, операционной системы или приложения.

Сетевые протоколы используются для обеспечения связи между устройствами в сети IoT. Существуют различные типы сетевых протоколов, включая проводные, беспроводные и протоколы маломощных глобальных сетей (LPWAN).

Проводные сетевые протоколы, такие как Ethernet, используют физические кабели для соединения устройств. Ethernet – это популярный протокол для подключения устройств в локальных сетях (LAN). Он обеспечивает надежную и высокоскоростную связь, что делает его пригодным для использования в

приложениях, требующих обмена данными в реальном времени, таких как промышленная автоматизация, видеонаблюдение, потоковое аудио и видео.

Протоколы беспроводных сетей, с другой стороны, используют радиоволны для обеспечения связи между устройствами. Некоторые из наиболее распространенных протоколов беспроводных сетей включают сотовую связь, Wi-Fi, Bluetooth, ZigBee, NFC и RFID.

Сотовые протоколы, такие как 2G, 3G и 4G, широко используются для подключения мобильных устройств к Интернету. Они обеспечивают высокоскоростную передачу данных и широко доступны в городских и пригородных районах. Сотовые протоколы широко используются в таких приложениях, как подключенные автомобили, отслеживание активов и удаленный мониторинг.

Wi-Fi – это популярный беспроводной протокол, использующий радиоволны для подключения устройств к Интернету. Он обеспечивает высокоскоростную передачу данных и широко используется в домах, офисах и общественных местах. Wi-Fi широко используется в таких приложениях, как "умные дома", автоматизация офиса и общественные точки доступа Wi-Fi.

Bluetooth и BLE (Bluetooth Low Energy) – это беспроводные протоколы, обычно используемые для связи между устройствами на коротких расстояниях. Они широко используются в таких приложениях, как носимые устройства, мониторинг здоровья и устройства "умного дома". Bluetooth обеспечивает надежную и безопасную передачу данных, а BLE – связь с низким энергопотреблением, что делает его пригодным для использования в устройствах с питанием от батарей.

ZigBee – это беспроводной протокол, разработанный для приложений с низкой скоростью передачи данных, требующих низкого энергопотребления, таких как системы домашней автоматизации и управления зданиями. Он обеспечивает надежную и безопасную связь и подходит для использования в крупномасштабных сетях.

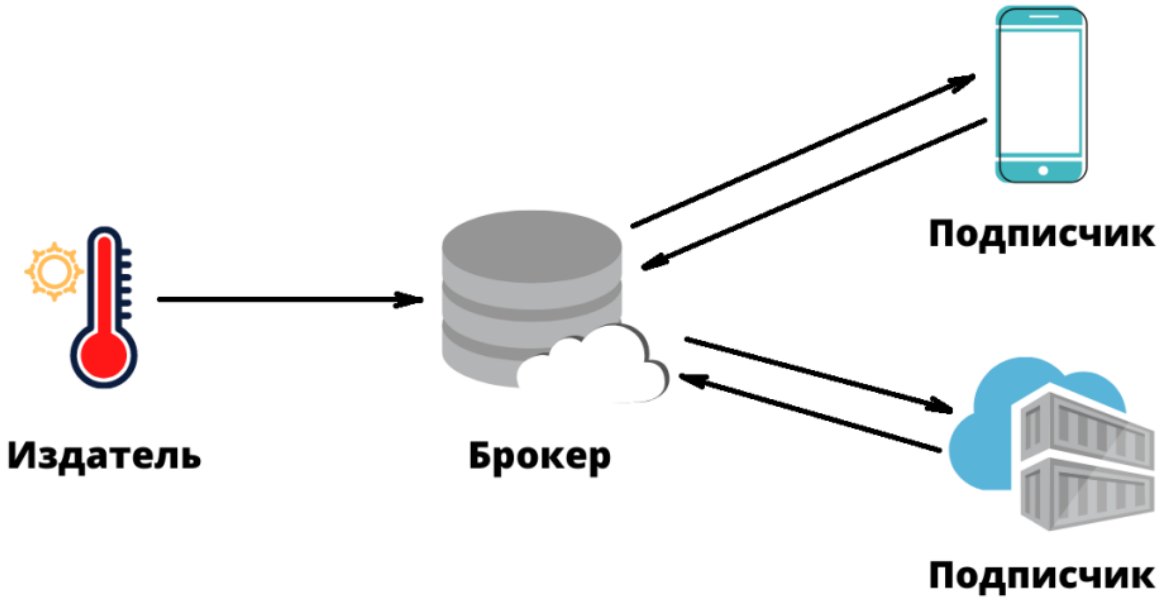
NFC (Near Field Communication) и RFID (Radio Frequency Identification) – беспроводные протоколы, обычно используемые для связи между устройствами на коротких расстояниях. NFC обычно используется в таких приложениях, как бесконтактные платежи и продажа билетов, а RFID широко применяется в управлении цепочками поставок, отслеживании активов и управлении запасами.

Протоколы LPWAN, такие как LoRaWAN, Sigfox и NB-IoT, предназначены для обеспечения связи на большие расстояния с низким энергопотреблением. Они широко используются в таких приложениях, как "умные" города, "умное" сельское хозяйство и отслеживание активов. Протоколы LPWAN обеспечивают надежную и безопасную связь, что делает их пригодными для использования в устройствах с низкой пропускной способностью и питанием от батарей.

В целом, сетевые протоколы необходимы для обеспечения связи между устройствами в сети IoT. Проводные и беспроводные протоколы обеспечивают надежную и высокоскоростную передачу данных, а протоколы LPWAN – связь на большие расстояния при низком энергопотреблении. Каждый протокол имеет свои сильные и слабые стороны, что делает его подходящим для различных приложений IoT.

Протоколы данных

MQTT



MQTT (Message Queuing Telemetry Transport) – это легкий протокол обмена сообщениями, разработанный для IoT-устройств с ограниченной вычислительной мощностью и сетями с низкой пропускной способностью. MQTT – это протокол публикации-подписки, в котором устройства, подключенные к сети, могут публиковать сообщения на определенные темы или подписываться на получение сообщений на эти темы.

MQTT широко используется в приложениях IoT благодаря низким накладным расходам и эффективному использованию пропускной способности сети. Он работает поверх TCP/IP и может работать с несколькими транспортными протоколами, такими как Wi-Fi, Ethernet, сотовые и спутниковые сети. MQTT использует небольшой заголовок, состоящий всего из 2 байт, что делает его идеальным для устройств с ограниченной вычислительной мощностью.

💡 **TCP/IP (Transmission Control Protocol/Internet Protocol)** - это семейство протоколов, используемых для связи компьютерных сетей, включая Интернет. Он обеспечивает стандартизированную, надежную и эффективную доставку данных между устройствами в сети, разделяя информацию на пакеты, управляя их передачей и перенаправлением, а также устанавливая соединения между устройствами. Каждый протокол в семействе TCP/IP выполняет определенную функцию, обеспечивая тем самым эффективную передачу данных между компьютерами.

Одной из ключевых особенностей MQTT является низкая задержка. Он разработан для минимизации задержек между отправкой и получением сообщений, что делает его идеальным для связи в реальном времени в таких приложениях, как домашняя автоматизация, промышленный контроль и мониторинг окружающей среды.

MQTT также отличается высокой надежностью благодаря встроенным функциям для обеспечения доставки сообщений. Он использует уровни качества обслуживания (QoS), которые позволяют устройствам определять, насколько важно сообщение и сколько раз оно должно быть доставлено для обеспечения надежности. MQTT может работать с уровнями QoS 0 (не более одного раза), 1 (не менее одного раза) и 2 (точно один раз).

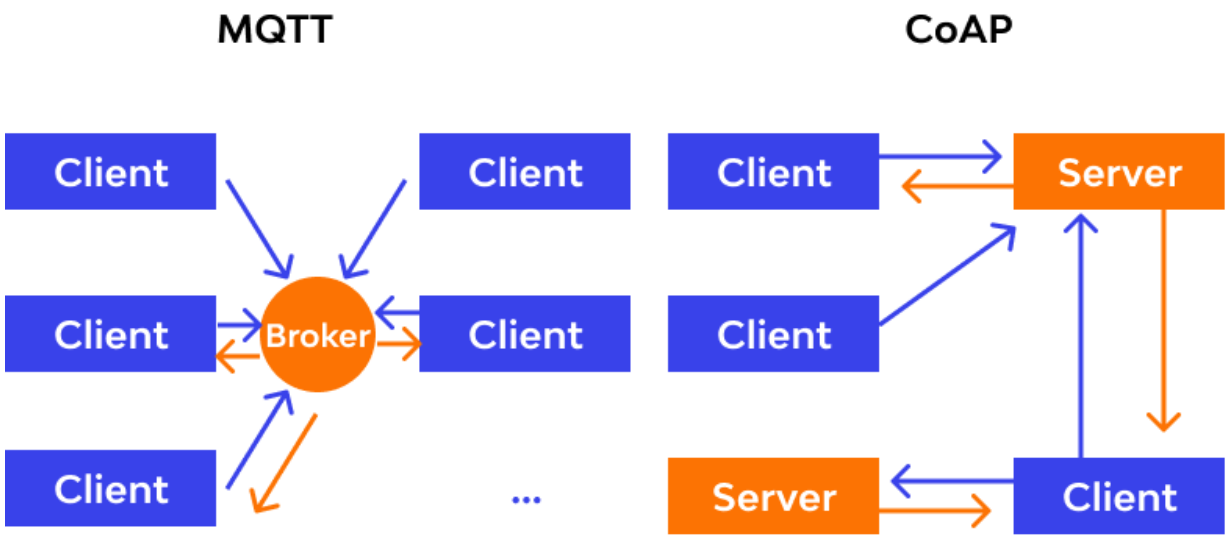
Одной из сильных сторон MQTT является его гибкость. Он хорошо настраивается и может использоваться в различных приложениях, от маломощных датчиков до высокопроизводительных промышленных систем управления. MQTT также поддерживает двунаправленную связь, что означает, что устройства могут как публиковать, так и подписываться на сообщения, обеспечивая более сложное взаимодействие между устройствами.

Однако одним из потенциальных недостатков MQTT является отсутствие встроенных функций безопасности, что означает, что он может быть уязвим для таких атак, как подслушивание или фальсификация данных. Чтобы решить эту проблему, MQTT можно использовать вместе с Transport Layer Security (TLS) или другими протоколами безопасности для обеспечения безопасного соединения между устройствами.

Некоторые примеры использования MQTT включают в себя устройства "умного дома", мониторинг окружающей среды и промышленную автоматизацию. Например, умный термостат в доме может использовать MQTT для связи с облачной службой, позволяя владельцу дома дистанционно управлять температурой в своем доме. В промышленной автоматизации MQTT может использоваться для мониторинга и управления машинами на заводе, позволяя анализировать данные в режиме реального времени и принимать решения.

MQTT является популярным и широко используемым протоколом в сфере IoT благодаря своим низким накладным расходам, низкой задержке и высокой надежности. Гибкость и настраиваемые функции делают его подходящим для широкого спектра приложений, от маломощных датчиков до высокопроизводительных промышленных систем управления.

CoAP



Constrained Application Protocol (CoAP) – это легкий протокол обмена сообщениями, разработанный специально для IoT-приложений, в которых ограниченные устройства должны взаимодействовать друг с другом. Он основан на тех же базовых принципах, что и HTTP, но гораздо проще и эффективнее с точки зрения пропускной способности и энергопотребления.

Одной из ключевых особенностей CoAP являются низкие накладные расходы. CoAP использует UDP в качестве основного транспортного протокола, что означает, что он имеет очень маленький заголовок и не требует трехстороннего рукопожатия, как TCP. Это делает его идеальным для использования в маломощных устройствах с ограниченной вычислительной мощностью и памятью.

> 💡 UDP (User Datagram Protocol) - это протокол передачи данных в компьютерных сетях, который обеспечивает быструю и эффективную доставку пакетов данных без гарантии их доставки или последовательности. В отличие от TCP, UDP не устанавливает соединение и не предоставляет механизмы для контроля ошибок и повторной передачи данных, что делает его более быстрым и менее надежным. UDP часто используется для передачи потоковых данных, таких как аудио и видео, где скорость передачи является более важным фактором, чем точность и порядок доставки.

CoAP также включает ряд функций, которые делают его хорошо подходящим для приложений IoT. Например, он поддерживает многоадресную передачу данных, что означает, что одно сообщение может быть отправлено нескольким получателям одновременно. Это полезно в сценариях, когда несколько устройств должны получать одну и ту же информацию, например, в приложениях "умного дома".

С точки зрения задержки, CoAP разработан для того, чтобы быть очень отзывчивым. Он включает поддержку асинхронного обмена сообщениями, что

означает, что устройства могут отправлять запросы и получать ответы параллельно, без необходимости ждать завершения одного запроса перед отправкой другого.

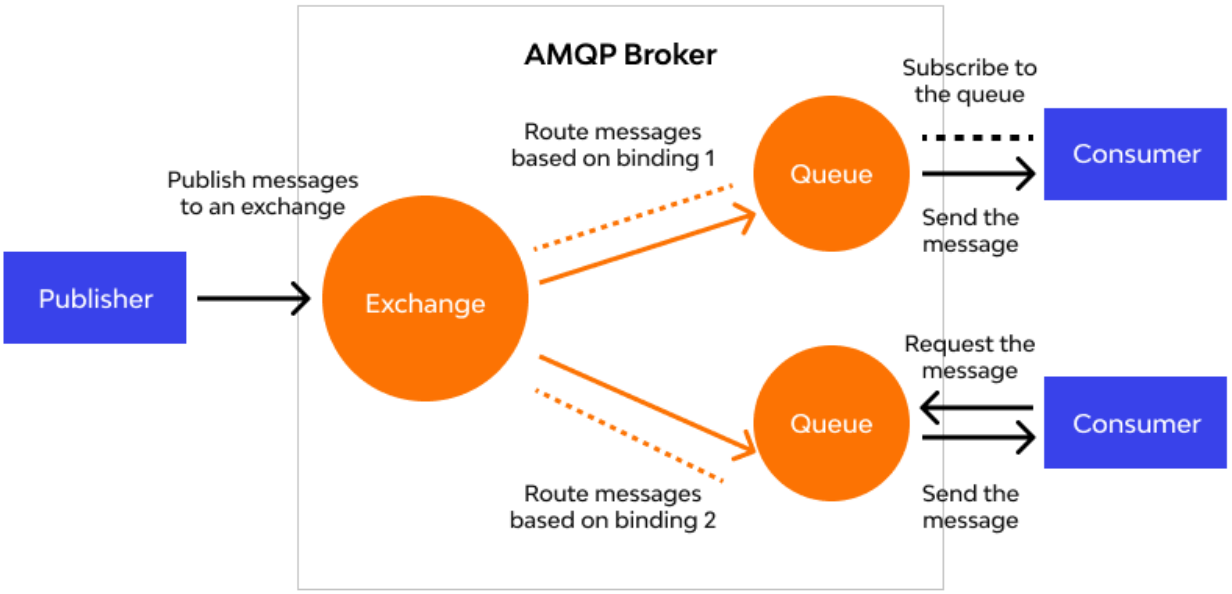
CoAP также включает ряд функций, повышающих надежность. Например, он поддерживает повторную передачу и подавление дубликатов, что означает, что если сообщение потеряно или повреждено, оно будет повторно передано до тех пор, пока не будет успешно получено. Это обеспечивает надежную доставку сообщений даже в шумной или ненадежной сетевой среде.

Одной из сильных сторон CoAP является его гибкость. Он поддерживает широкий спектр форматов данных, включая двоичные и текстовые данные, и может использоваться для передачи как коротких сообщений, так и большой полезной нагрузки.

Однако у CoAP есть и некоторые недостатки. Например, он не так широко распространен, как другие протоколы IoT, такие как MQTT, что означает, что может быть сложнее найти библиотеки и инструменты для работы с ним. Кроме того, поскольку он основан на UDP, он может не подходить для использования в сценариях, где критически важна надежная доставка сообщений.

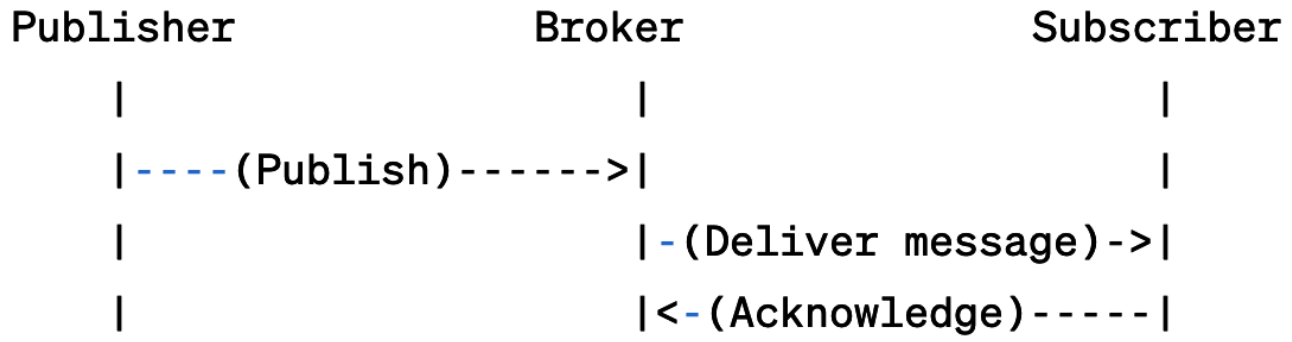
CoAP имеет множество вариантов использования в приложениях IoT, включая автоматизацию "умного дома", промышленные системы управления и мониторинг здравоохранения. Он хорошо подходит для сценариев, где важны низкое энергопотребление, низкие накладные расходы и надежная передача сообщений, это мощный и гибкий протокол обмена сообщениями, который хорошо подходит для приложений IoT. Его низкие накладные расходы, быстрое реагирование на задержки и надежный обмен сообщениями делают его идеальным выбором для широкого спектра сценариев использования.

AMQP



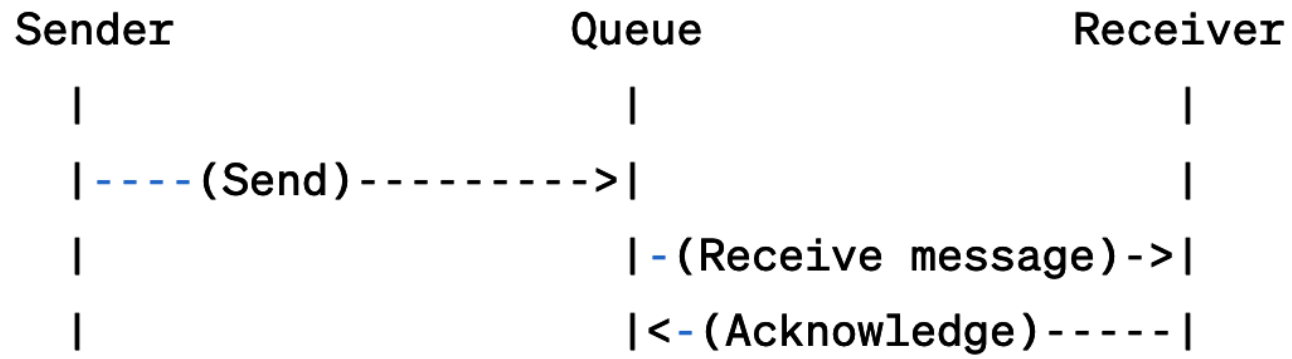
Advanced Message Queuing Protocol (AMQP) – это протокол обмена сообщениями, предназначенный для высокопроизводительного и надежного обмена сообщениями между приложениями в распределенных системах, включая приложения IoT. AMQP – это открытый стандартный протокол, определяющий формат и семантику сообщений, а также правила доставки и управления сообщениями.

Одной из ключевых особенностей AMQP является поддержка широкого спектра брокеров сообщений и клиентских библиотек, что позволяет использовать его в различных средах IoT. Это гибкий протокол, который можно использовать как для обмена сообщениями по схеме pub/sub, так и по схеме "точка-точка". Пример схемы pub/sub показан на рисунке ниже.



Здесь publisher (издатель) отправляет сообщение на брокера (message broker), который доставляет его всем зарегистрированным на него subscriber'ам (подписчикам).

Пример схемы точка-точка показан на рисунке ниже:



Здесь отправитель отправляет сообщение в очередь (queue), а получатель читает его из этой очереди. Каждое сообщение доставляется только одному получателю, а очередь гарантирует, что сообщения будут обработаны в порядке их поступления. Если получатель не может обработать сообщение, оно остается в очереди, пока не будет обработано или не истечет время его жизни.

С точки зрения задержки, AMQP разработан как протокол с низкой задержкой, что означает, что он подходит для использования в приложениях, требующих обмена данными в режиме реального времени. AMQP обеспечивает надежную передачу сообщений, гарантируя, что сообщения будут доставлены в том

порядке, в котором они были отправлены, и что ни одно сообщение не будет потеряно. Это делает его высоконадежным протоколом, подходящим для использования в критически важных приложениях.

К сильным сторонам AMQP относятся его гибкость, надежность и совместимость с широким спектром систем обмена сообщениями. AMQP также обеспечивает поддержку сложной маршрутизации и фильтрации сообщений, что делает его пригодным для использования в крупномасштабных приложениях IoT.

Однако одним из недостатков AMQP является его сложность. Протокол может быть сложным в реализации и настройке, и для его эффективного использования может потребоваться высокий уровень технических знаний. Кроме того, AMQP может не подойти для использования в приложениях с ограниченной пропускной способностью или высокими требованиями к задержкам.

Варианты использования AMQP в приложениях IoT включают удаленный мониторинг, сбор и анализ данных, а также межмашинную связь. Например, AMQP может использоваться для сбора и передачи данных с датчиков в интеллектуальном здании или на производственном предприятии, или для обеспечения управления устройствами в режиме реального времени в интеллектуальном доме или промышленном IoT.

HTTP

HTTP (Hypertext Transfer Protocol) – это протокол, который широко используется в веб-приложениях на протяжении многих лет. Он также является важным протоколом для приложений IoT. HTTP обеспечивает связь между клиентом и сервером через Интернет или любую другую сеть. В IoT-приложениях HTTP часто используется в качестве протокола передачи данных для передачи информации от IoT-устройств к серверам и наоборот.

Одним из ключевых преимуществ HTTP является то, что это устоявшийся протокол с большой экосистемой инструментов и библиотек. Это означает, что разработчики могут легко интегрировать HTTP в свои IoT-проекты, и существует

множество ресурсов, которые помогут им в этом. HTTP также поддерживает различные механизмы безопасности, такие как шифрование и аутентификация SSL/TLS, которые важны для защиты данных IoT.

Однако использование HTTP в приложениях IoT имеет и некоторые недостатки. Один из них заключается в том, что это относительно тяжелый протокол, что означает, что он может не подходить для всех случаев использования IoT, особенно для тех, которые связаны с маломощными устройствами. Кроме того, зависимость HTTP от TCP/IP может привести к проблемам с высокой задержкой, особенно в случаях, когда между устройствами IoT и сервером большие расстояния.

Несмотря на эти ограничения, HTTP остается важным протоколом для приложений IoT. Его сильные стороны заключаются в широком распространении, большом сообществе и надежных функциях безопасности. Он особенно хорошо подходит для тех случаев, когда объем передаваемых данных относительно велик, а безопасность и надежность имеют первостепенное значение. Примерами IoT-приложений, использующих HTTP, являются "умные дома", подключенные транспортные средства и промышленные системы управления.

Сетевые протоколы

Ethernet

Ethernet – это протокол связи, который существует с 1970-х годов и широко используется в проводных локальных сетях (LAN) и глобальных сетях (WAN). Это надежный и эффективный протокол, который позволяет устройствам взаимодействовать друг с другом по сети. Ethernet широко используется в приложениях IoT, поскольку это зрелая технология, стандартизированная в течение многих лет.

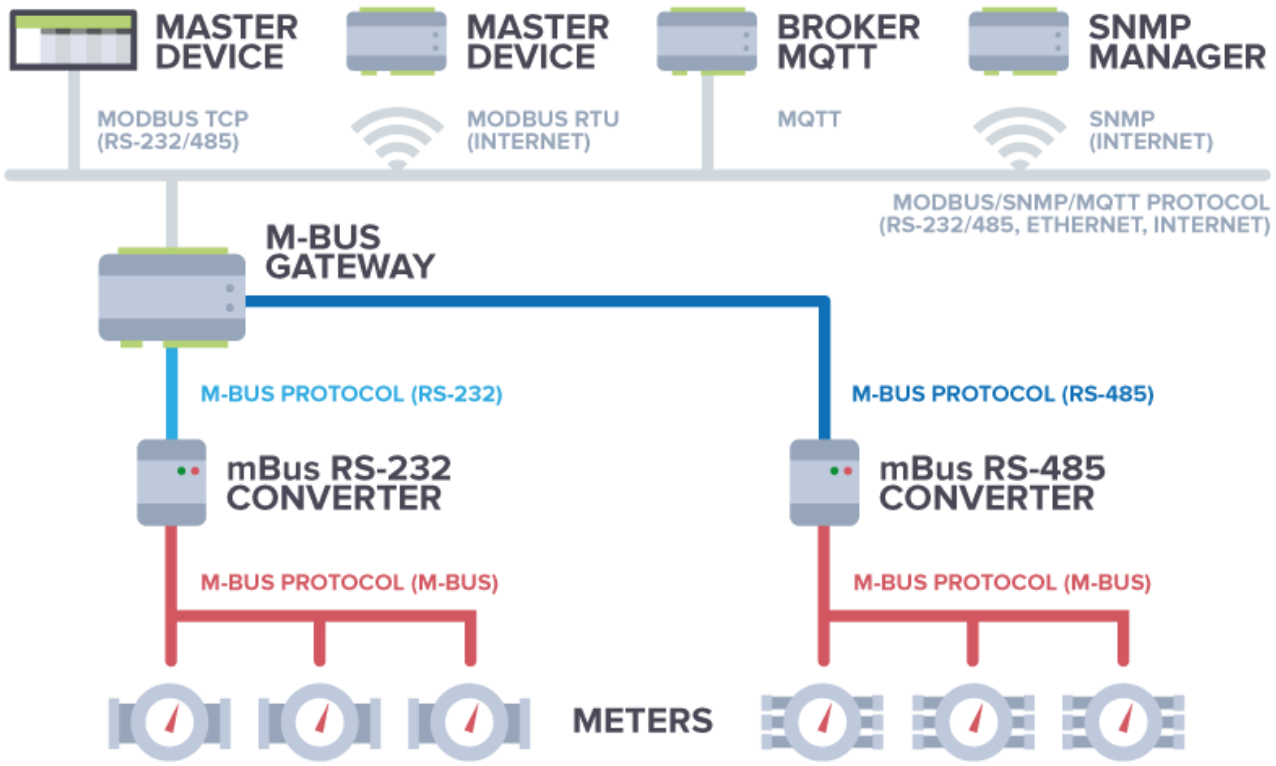
Ethernet работает на различных частотах, в зависимости от типа кабеля и используемой сети. В сетях Ethernet обычно используются следующие частоты: 10 Мбит/с, 100 Мбит/с и 1 Гбит/с. Ethernet может использовать как лицензированный, так и бесплатный спектр в зависимости от сети и местоположения. Ethernet обладает высокой пропускной способностью, что позволяет быстро и эффективно передавать данные между устройствами. Он также имеет низкое энергопотребление, что делает его идеальным для использования в устройствах IoT, работающих от батарей.

Задержка – это время, необходимое для передачи пакета данных от одного устройства к другому по сети. Ethernet имеет низкий уровень задержки, что означает, что данные передаются быстро и эффективно. Это важно для приложений IoT, где требуется связь в режиме реального времени, например, в системах промышленной автоматизации и управления.

Ethernet – это высоконадежный протокол, в котором предусмотрены механизмы проверки и исправления ошибок для обеспечения правильной передачи данных. Это также безопасный протокол, который может быть зашифрован для защиты данных от несанкционированного доступа. Однако одним из потенциальных недостатков Ethernet является то, что он уязвим к помехам от других электронных устройств и может быть подвержен влиянию шумов в сети.

Ethernet находит свое применение в приложениях IoT благодаря своим преимуществам в надежности, безопасности и скорости. Он применяется в системах промышленной автоматизации и управления, где важна связь в реальном времени и высокая надежность. Ethernet также используется в "умных" домах и зданиях, где такие устройства, как термостаты, системы управления освещением и системы безопасности, должны взаимодействовать друг с другом по сети.

MBus



MBus (Meter-Bus) – это коммуникационный протокол, используемый для дистанционного считывания показаний счетчиков в энергетической и водной отраслях. Он был впервые разработан в Германии в 1990-х годах и широко используется в Европе для автоматического считывания показаний счетчиков (AMR) и автоматического управления счетчиками (AMM). MBus – это протокол проводной связи, который работает по витой паре и способен взаимодействовать с несколькими счетчиками, подключенными параллельно.

Протокол MBus имеет относительно низкую пропускную способность 2400 бит в секунду (бит/с) и дальность действия до 100 метров. Он работает в лицензированном диапазоне частот, что делает его более надежным и менее подверженным помехам. MBus известна своим низким энергопотреблением и может работать в течение длительного времени при использовании счетчиков, питающихся от батарей.

Одним из главных достоинств протокола MBus является его способность поддерживать несколько счетчиков на одной шине, что делает его идеальным для использования в зданиях с большим количеством счетчиков. Протокол также обладает хорошими функциями безопасности, гарантируя, что показания счетчиков не будут подделаны.

Однако одним из недостатков протокола MBus является его ограниченная пропускная способность, что означает, что он не подходит для передачи больших

объемов данных. Он также не подходит для приложений реального времени из-за своей задержки.

Протокол MBus широко используется в различных приложениях, широко применяясь при считывании показаний с различных счетчиков: газа, электроэнергии и воды. Он также используется в системах автоматизации зданий для мониторинга использования энергии и управления системами отопления, вентиляции и кондиционирования воздуха.

RS-485

RS-485, также известный как ModBus, является протоколом последовательной связи, обычно используемым в контексте приложений IoT. Он предназначен для обмена данными между устройствами на больших расстояниях, со скоростью передачи данных до 10 Мбит/с на расстояние до 1200 метров.

Одной из ключевых особенностей RS-485 является его способность поддерживать связь между несколькими устройствами на одной шине. Это позволяет создавать сложные сети IoT, в которых устройства могут взаимодействовать друг с другом и обмениваться данными в режиме реального времени. RS-485 может поддерживать до 32 устройств на одной шине, что делает его популярным выбором для многих приложений IoT.

С точки зрения пропускной способности, RS-485 имеет относительно низкую скорость передачи данных, которая обычно составляет от 300 бит/с до 115,2 кбит/с. Однако этого часто бывает достаточно для многих приложений IoT, где между устройствами передаются небольшие объемы данных. RS-485 также известен своим низким энергопотреблением, что делает его популярным выбором для IoT-устройств с батарейным питанием.

Одним из ключевых достоинств RS-485 является его надежность. Этот протокол известен своей прочностью и способностью работать в жестких условиях, где шум и помехи могут быть проблемой. Кроме того, RS-485 включает в себя функции обнаружения и исправления ошибок, которые помогают обеспечить точную и надежную передачу данных.

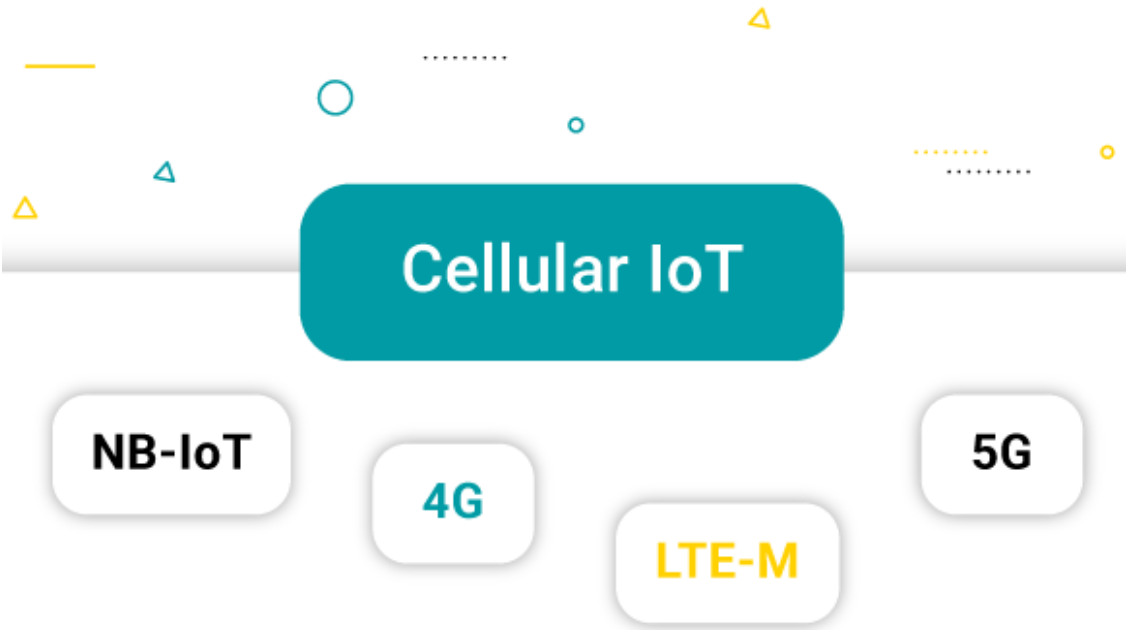
Несмотря на множество достоинств, у протокола RS-485 есть и недостатки. Одним из них является относительно низкая скорость передачи данных, что может ограничить его использование в приложениях, где необходимо передавать большие объемы данных. Кроме того, RS-485 требует физического подключения устройств к шине, что может ограничить гибкость сети.

С точки зрения применения, RS-485 обычно используется в промышленности и автоматизации, где его надежность и прочность делают его популярным выбором. Он часто используется для таких приложений, как мониторинг и управление

машинами и оборудованием, а также для систем автоматизации и управления зданиями.

RS-485 (ModBus) – это широко используемый протокол в сфере IoT, который предлагает хороший баланс надежности и производительности, что делает его популярным выбором для многих приложений.

Сотовые технологии передачи данных



Сотовые сети являются одним из наиболее используемых сетевых протоколов для устройств IoT. Они основаны на использовании мобильных сетей, которые обеспечивают беспроводную связь на больших географических территориях с помощью вышек сотовой связи. Сотовые сети использовались в течение многих лет для обеспечения беспроводной связи для мобильных телефонов, и они также эволюционировали для поддержки устройств IoT.

- **Частоты**: Сотовые сети работают в диапазоне частот, которые зависят от типа сети и региона. В целом, они работают в диапазоне от 700 МГц до 2600 МГц.
- **Лицензирование**: Сотовые сети используют лицензионный спектр, который регулируется правительством и требует лицензии на эксплуатацию. Это гарантирует, что сеть работает без помех со стороны других беспроводных устройств.
- **Пропускная способность**: Сотовые сети имеют ограниченную пропускную способность, которая распределяется между всеми устройствами, подключенными к сети. Пропускная способность обычно измеряется в мегабитах в секунду (Мбит/с).

- **Энергопотребление**: Для работы сотовых сетей требуется умеренное количество энергии, что делает их подходящими для устройств с умеренными требованиями к питанию. Однако они не подходят для устройств с очень низким энергопотреблением, так как потребление энергии может быть слишком высоким.
- **Задержка**: Сотовые сети обычно имеют более высокую задержку по сравнению с другими сетевыми протоколами, что может сделать их непригодными для приложений, требующих низкой задержки, таких как приложения управления в реальном времени.
- **Надежность**: Сотовые сети обычно считаются надежными, поскольку они были разработаны для обеспечения высокой доступности и надежности.
- **Сильные и слабые стороны**: Главной сильной стороной сотовых сетей является их широкая зона покрытия и надежность. Они также хорошо подходят для приложений, требующих умеренной пропускной способности и умеренного энергопотребления. Однако они могут не подходить для приложений, которым требуется очень низкое энергопотребление.
- **Примеры использования**: Сотовые сети широко используются в приложениях IoT, таких как отслеживание автопарка, мониторинг активов и инфраструктура "умного города". Они также используются в приложениях, где требуется широкая зона покрытия, например, в сельской местности или удаленных районах.

Wi-Fi

Wi-Fi, сокращение от "Wireless Fidelity", – это широко используемый протокол беспроводных сетей, который позволяет устройствам подключаться к Интернету и общаться друг с другом без использования кабелей. Wi-Fi работает в различных частотных диапазонах, включая 2,4 ГГц и 5 ГГц, в зависимости от устройства и его возможностей.

Доступная полоса пропускания для Wi-Fi зависит от частотного диапазона и количества используемых каналов. Обычно диапазон 2,4 ГГц обеспечивает пропускную способность до 20 МГц на канал, а диапазон 5 ГГц – до 160 МГц.

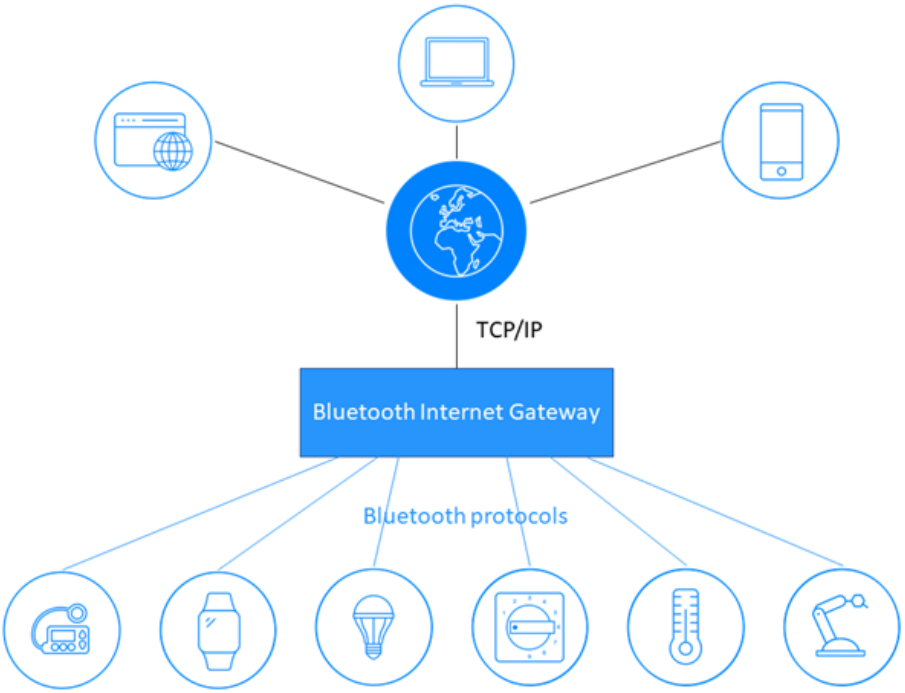
Wi-Fi становится все более популярным протоколом связи в IoT благодаря своей надежности, низкой задержке и высокой пропускной способности. Устройства с поддержкой Wi-Fi могут быстро и беспрепятственно взаимодействовать друг с другом, что делает его идеальным для приложений реального времени, таких как потоковое видео или онлайн-игры.

Однако энергопотребление Wi-Fi может быть относительно высоким по сравнению с другими протоколами беспроводной связи, что может быть

недостатком для IoT-устройств с питанием от батарей. Кроме того, на сигналы Wi-Fi могут влиять помехи от других устройств, работающих в том же частотном диапазоне, что может привести к снижению надежности.

Несмотря на эти ограничения, Wi-Fi остается популярным выбором для IoT-приложений, требующих высокоскоростного и надежного беспроводного соединения. Некоторые распространенные случаи использования Wi-Fi в IoT включают домашнюю автоматизацию, "умные города" и промышленные приложения.

Bluetooth



Bluetooth – это протокол беспроводной связи, использующий радиоволны малого радиуса действия для передачи данных между устройствами. Он работает в частотном диапазоне 2,4 ГГц, который является нелицензируемым и свободным спектром, что означает, что любой может использовать его без необходимости получения лицензии.

Bluetooth имеет относительно низкую пропускную способность, а последняя версия Bluetooth 5.2 обеспечивает максимальную скорость передачи данных 2 Мбит/с. Однако этого более чем достаточно для большинства приложений IoT, которые обычно предполагают передачу небольших объемов данных между устройствами.

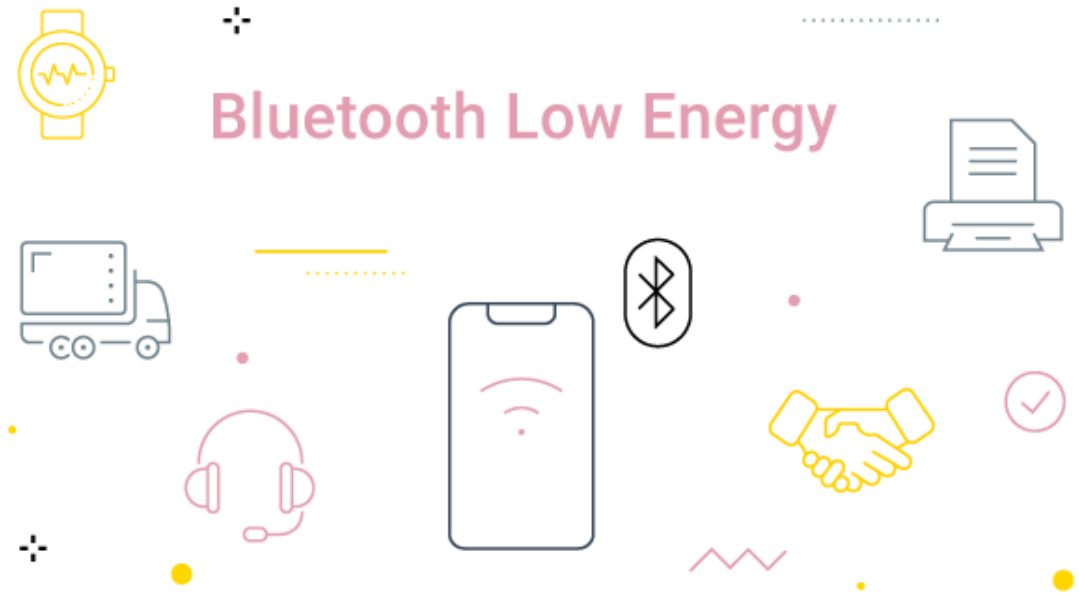
Одним из достоинств Bluetooth является низкое энергопотребление, что делает его идеальным для IoT-устройств, питающихся от батарей или других маломощных источников. Устройства Bluetooth также относительно дешевы в

производстве, а протокол широко поддерживается смартфонами, ноутбуками и другими вычислительными устройствами.

С точки зрения надежности Bluetooth прошел долгий путь с первых дней своего существования, новые версии протокола отличаются улучшенной коррекцией ошибок и другими технологиями, обеспечивающими надежную передачу данных. Однако Bluetooth по-прежнему имеет ограничения по дальности действия и помехам, поэтому он не всегда является лучшим выбором для IoT-приложений, требующих связи на большом расстоянии или работающих в условиях сильных помех.

Bluetooth используется в широком спектре приложений IoT, включая устройства умного дома, носимые устройства и медицинские приборы. Например, Bluetooth используется для подключения смартфона к устройству "умного дома", такому как термостат, что позволяет пользователям дистанционно управлять температурой в доме. Bluetooth также используется в носимых устройствах, таких как фитнес-трекеры, для передачи данных на смартфон или другое устройство. Кроме того, Bluetooth используется в медицинских устройствах, таких как измерители уровня глюкозы в крови и мониторы артериального давления, для передачи данных в приложение для смартфона, что позволяет пациентам и их врачам удаленно контролировать состояние здоровья.

BLE



Bluetooth Low Energy (BLE) – это протокол беспроводной связи, разработанный для устройств IoT с низким энергопотреблением. Он является подмножеством классического протокола Bluetooth и также известен как Bluetooth Smart. BLE работает в диапазоне 2,4 ГГц ISM (Industrial, Scientific, and Medical),

который представляет собой безлицензионный спектр, используемый многими беспроводными технологиями. Максимальный радиус действия BLE составляет около 100 метров, но он может меняться в зависимости от окружающей среды и других факторов.

BLE имеет меньшую пропускную способность по сравнению с классическим Bluetooth, с максимальной скоростью передачи данных 1 Мбит/с. Однако BLE оптимизирован для маломощных устройств и имеет гораздо меньшее энергопотребление по сравнению с классическим Bluetooth. Это делает его подходящим для IoT-устройств с питанием от батарей, которые должны работать в течение длительного времени без подзарядки.

Одним из достоинств BLE является низкая задержка, что означает быструю передачу данных между устройствами. BLE также отличается высокой надежностью, поскольку в протокол встроены функции коррекции ошибок и повторной передачи пакетов для обеспечения правильной (достоверной) передачи данных.

У BLE есть несколько сильных и слабых сторон. Одним из достоинств является низкое энергопотребление, что делает его идеальным для IoT-устройств, которые должны работать от аккумулятора. BLE также имеет низкую задержку, что делает его подходящим для приложений, требующих быстрой передачи данных. С другой стороны, BLE имеет меньшую пропускную способность по сравнению с другими беспроводными протоколами, что может ограничить объем передаваемых данных. BLE также может иметь проблемы с подключением в среде с высоким уровнем помех или там, где работает много других беспроводных устройств.

BLE используется в различных приложениях IoT, таких как устройства "умного дома", носимые фитнес-трекеры и медицинские устройства. BLE может использоваться для передачи данных, таких как температура, пульс и показания других датчиков с устройств IoT на смартфон или другое шлюзовое устройство. BLE также может использоваться для определения близости, когда IoT-устройства могут обнаруживать близлежащие устройства и инициировать действия, основанные на их присутствии.

В целом, BLE – это мощный беспроводной протокол, который хорошо подходит для маломощных устройств IoT, требующих низкой задержки и высокой надежности. Низкое энергопотребление и способность быстро передавать данные делают его идеальным выбором для широкого спектра приложений IoT.

Bluetooth vs BLE

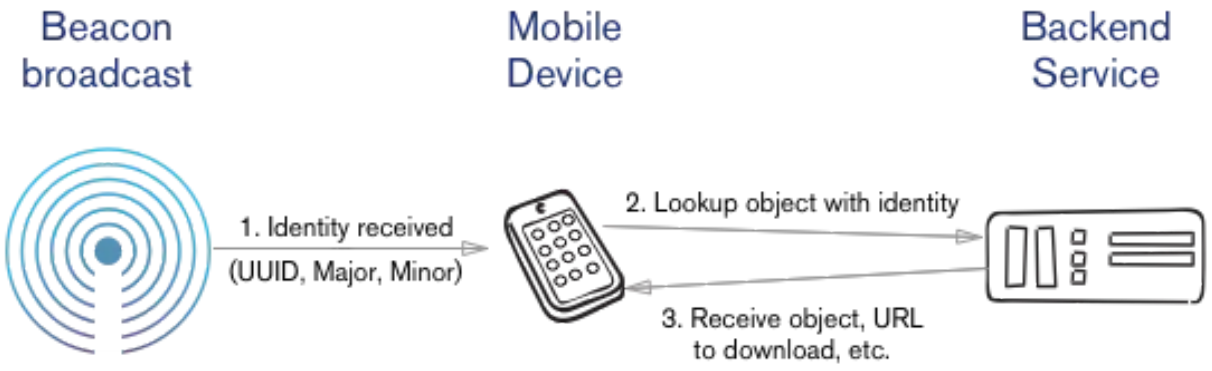
Bluetooth и Bluetooth Low Energy (BLE) – два популярных протокола беспроводной связи, используемых в приложениях IoT. Хотя они имеют некоторые общие черты, между ними есть и некоторые важные различия.

- **Частота**: И Bluetooth, и BLE работают в диапазоне ISM (промышленный, научный и медицинский) 2,4 ГГц, но BLE использует частотно-скачкообразный спектр (FHSS), чтобы избежать помех от других устройств в этом диапазоне.
- **Лицензирование**: Диапазон 2,4 ГГц, используемый как Bluetooth, так и BLE, является свободным, нелицензируемым спектром.
- **Пропускная способность**: Bluetooth имеет максимальную скорость передачи данных 2 Мбит/с, а BLE – 1 Мбит/с.
- **Энергопотребление**: BLE разработан для низкого энергопотребления и оптимизирован для низкого потребления энергии, что делает его идеальным для устройств с питанием от батареи. Bluetooth, с другой стороны, может потреблять больше энергии, что может ограничить его использование в устройствах IoT.
- **Задержки**: BLE имеет более низкую латентность, чем Bluetooth, что означает, что он может передавать данные быстрее.
- **Надежность**: BLE использует механизмы обнаружения потери пакетов и повторной передачи для обеспечения надежной передачи данных. Bluetooth также имеет подобные механизмы, но он не так надежен, как BLE.
- **Сильные стороны**: BLE идеально подходит для устройств IoT, которым требуется низкое энергопотребление и низкая задержка, таких как носимые устройства и устройства "умного дома". Bluetooth лучше подходит для устройств, которым требуется более высокая скорость передачи данных, например, для потокового аудио и видео.
- **Слабые стороны**: Более низкая скорость передачи данных BLE может ограничить его использование в некоторых IoT-приложениях, а более высокое энергопотребление Bluetooth может сделать его менее подходящим для устройств с питанием от аккумулятора.
- **Сферы применения**: BLE обычно используется в приложениях IoT, таких как устройства "умного дома", фитнес-трекеры и медицинские устройства. Bluetooth обычно используется в устройствах для потоковой передачи аудио и видео, таких как наушники и колонки.

Specifications	Classic Bluetooth	Bluetooth Low Energy (BLE)
Range	100 m	Greater than 100 m
Data Rate	1-3 Mbps	1 Mbps
Application Throughput	0.7 -2.1 Mbps	0.27 Mbps
Frequency	2.4 GHz	2.4 GHz
Security	56/128-bit	128-bit AES with Counter Mode CBC-MAC
Robustness	Adaptive fast frequency hopping, FEC, fast ASK	24-bit CRC, 32-bit Message Integrity Check
Latency	100 ms	6 ms
Time Lag	100 ms	3 ms
Voice Capable	Yes	No
Network Topology	Star	Star
Power Consumption	1 W	0.01 to 0.5 W
Peak Current Consumption	less than 30 mA	less than 15 mA

В целом, BLE разработан для низкого энергопотребления, низкой задержки и надежной передачи данных, что делает его идеальным для IoT-устройств, которым необходимы эти характеристики. Bluetooth, с другой стороны, лучше подходит для устройств, требующих более высокой скорости передачи данных, таких как потоковое аудио и видео.

iBeacon



Протокол **iBeacon** – это разновидность технологии маячков Bluetooth Low Energy (BLE), разработанная компанией Apple. Он использует небольшие беспроводные устройства, называемые iBeacons, которые передают сигналы на близлежащие мобильные устройства. Протокол iBeacon позволяет предоставлять услуги на основе местоположения, такие как маркетинг по принципу близости и навигация внутри помещений, непосредственно через смартфоны и другие интеллектуальные устройства.

iBeacon – это небольшие устройства, работающие от батареек, которые можно разместить в любом физическом месте. Они постоянно передают уникальный идентификатор, который может быть обнаружен мобильными устройствами, оснащенными технологией Bluetooth Low Energy. Это позволяет мобильным устройствам определять близость к iBeacon и инициировать действия, основанные на местоположении пользователя.

Одним из основных преимуществ технологии iBeacon является ее способность предоставлять пользователям высоко персонализированный и контекстуально релевантный опыт. Например, розничная компания может использовать iBeacon для предложения скидок или акций покупателям, которые просматривают товары в магазине. Аналогичным образом, музеи и галереи могут использовать iBeacons для предоставления информации о местоположении экспонатов и произведений искусства.

Еще одним преимуществом технологии iBeacon является ее низкая стоимость и простота развертывания. iBeacon можно быстро и легко установить в различных физических местах, что позволяет предприятиям и организациям легко воспользоваться преимуществами услуг на основе местоположения.

Однако технология iBeacon также имеет свои ограничения. Радиус действия iBeacon относительно невелик, обычно всего несколько метров, что означает, что он может не подходить для более масштабных приложений. Кроме того, технология iBeacon основана на Bluetooth Low Energy, который может быть подвержен помехам от других беспроводных сигналов, что приводит к снижению надежности.

iBeacon представляет собой мощный инструмент для предоставления пользователям высоко персонализированного и контекстуально релевантного опыта в различных условиях. Простота развертывания и низкая стоимость делают ее привлекательным вариантом для предприятий и организаций, желающих воспользоваться преимуществами услуг на основе местоположения.

Как связаны BLE и iBeacon?

iBeacon фактически является конкретной реализацией протокола Bluetooth Low Energy (BLE). BLE – это технология беспроводной связи, разработанная для приложений с низким энергопотреблением и малым радиусом действия. iBeacon

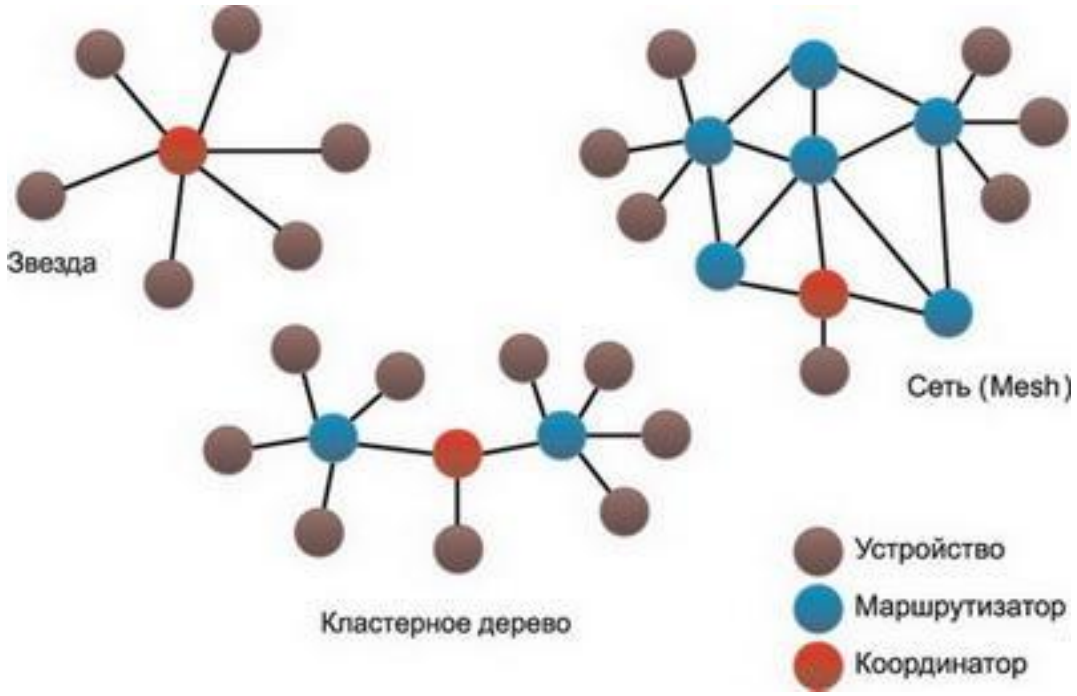
использует протокол BLE для передачи небольших пакетов данных, или рекламных пакетов, на соседние устройства. Эти рекламные пакеты содержат информацию о iBeacon, такую как его уникальный идентификатор, уровень сигнала и местоположение.

Основное различие между BLE и iBeacon заключается в их функциональности. BLE – это беспроводной протокол общего назначения, который может использоваться для широкого спектра приложений, в то время как iBeacon специально разработан для сервисов, основанных на определении местоположения. Технология iBeacon позволяет компаниям доставлять пользователям целевой контент и сообщения, основанные на их физическом местоположении, например, персонализированные рекламные предложения, направления, информацию о товарах или услугах.

Еще одно различие между BLE и iBeacon заключается в их технических характеристиках. Хотя iBeacon использует технологию BLE, он имеет уникальный формат пакетов и протокол передачи, оптимизированный для конкретного случая использования. iBeacon обычно передает пакеты с фиксированным интервалом и использует определенный формат для передачи информации о своем местоположении и идентификации.

В целом, хотя iBeacon построен на основе протокола BLE, он добавляет слой функциональности, основанной на определении местоположения, что делает его мощным инструментом для предприятий и других организаций, стремящихся взаимодействовать с клиентами новыми и инновационными способами.

ZigBee



ZigBee – это беспроводной протокол, разработанный для связи с низкой скоростью передачи данных, низким энергопотреблением и малым радиусом действия. Он работает в нелицензируемых частотных диапазонах 2,4 ГГц и 915 МГц, которые являются свободными для использования, что делает его подходящим для широкого спектра приложений IoT.

Одним из ключевых преимуществ ZigBee является низкое энергопотребление. Он рассчитан на минимальное потребление энергии, что делает его идеальным для использования в устройствах с батарейным питанием, которые должны работать в течение длительного времени без подзарядки или замены. Это делает ZigBee привлекательным вариантом для IoT-устройств, требующих длительного времени автономной работы, таких как датчики умного дома, пульты дистанционного управления и системы безопасности.

ZigBee также имеет относительно низкую пропускную способность, что означает, что он может обрабатывать ограниченный объем данных. Однако это делает его хорошо подходящим для IoT-приложений, в которых используются небольшие пакеты данных, например, показания датчиков, а не большие объемы непрерывных данных.

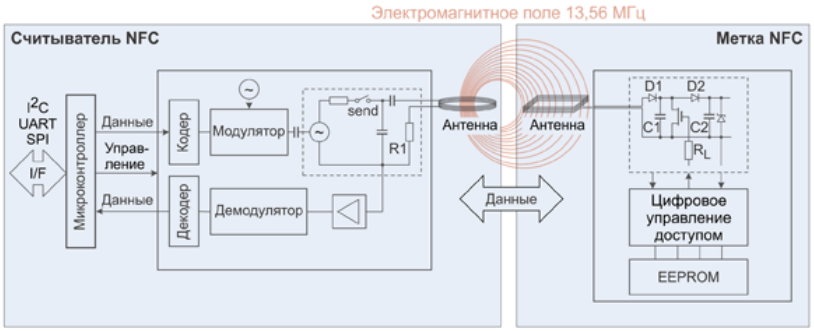
Что касается надежности, ZigBee использует ячеистую сеть, что означает, что все узлы в сети могут общаться друг с другом напрямую или косвенно через промежуточные узлы. Это повышает надежность и дальность действия сети, поскольку сигнал может передаваться от узла к узлу, пока не достигнет цели.

Одним из недостатков ZigBee является относительно высокая задержка, что может стать проблемой для приложений, требующих обработки данных в реальном времени, например, для промышленных систем управления. Кроме того, сети

ZigBee могут быть сложнее в установке и настройке, чем другие беспроводные протоколы, что может сделать их менее доступными для начинающих пользователей.

Сильные и слабые стороны ZigBee делают его хорошо подходящим для целого ряда приложений IoT, включая умные дома, автоматизацию зданий и промышленные системы управления. В контексте "умного дома" ZigBee можно использовать для подключения широкого спектра устройств, включая выключатели света, термостаты и дверные замки. В системах автоматизации зданий он может использоваться для мониторинга и управления системами отопления, вентиляции и кондиционирования воздуха (HVAC). В промышленных системах управления ZigBee может использоваться для мониторинга и управления производственными процессами и оборудованием.

NFC



Near Field Communication (NFC) – это протокол беспроводной связи малого радиуса действия, который позволяет двум устройствам общаться друг с другом, когда они находятся на расстоянии нескольких сантиметров друг от друга. Он работает на частоте 13,56 МГц и обычно используется для бесконтактных платежных систем, контроля доступа и передачи данных между устройствами.

Одним из главных достоинств NFC является низкое энергопотребление, что делает его идеальным для IoT-приложений, где время автономной работы является проблемой. Кроме того, NFC имеет очень короткий радиус действия, что делает его более безопасным, чем другие протоколы беспроводной связи, такие как Wi-Fi или Bluetooth. Поскольку протокол NFC основан на принципе приближения, он менее

восприимчив к помехам и может работать в местах, где другие беспроводные технологии могут работать неэффективно.

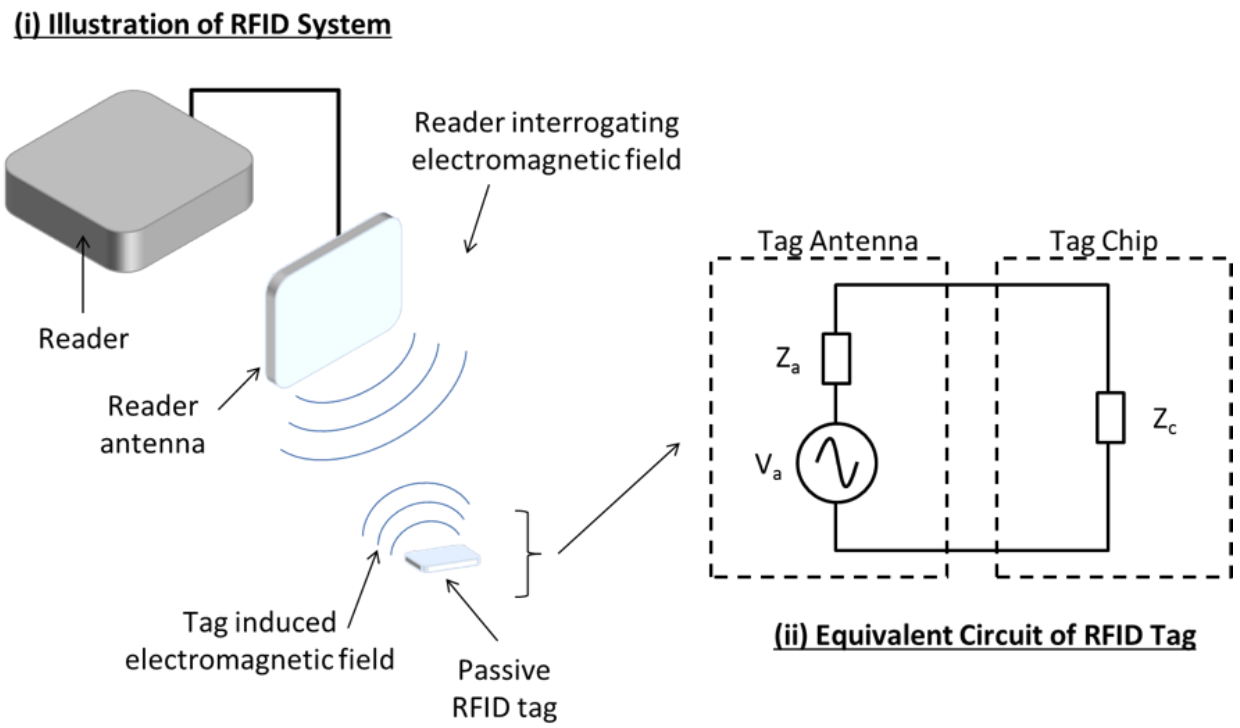
NFC также относительно надежен, с низким уровнем ошибок и высокой скоростью передачи данных. Однако ограниченный радиус действия также означает, что он не подходит для приложений, требующих связи на большие расстояния.

Некоторые из основных вариантов использования NFC в IoT включают:

- **Бесконтактные платежные системы**: NFC обычно используется в бесконтактных платежных системах, в которых пользователи могут оплачивать товары и услуги простым прикосновением смартфона или смарт-карты к считывающему устройству.
- **Контроль доступа**: NFC может использоваться для систем контроля доступа, в которых пользователи могут прикоснуться своим устройством к считывателю, чтобы получить доступ в здание или охраняемую зону.
- **Передача данных**: NFC может использоваться для передачи данных между устройствами, например, для передачи контактной информации между смартфонами или обмена файлами между устройствами.
- **Автоматизация умного дома**: NFC можно использовать для управления различными устройствами "умного дома", такими как включение света или регулировка термостата, простым прикосновением смартфона или смарт-карты к считывающему устройству.

В целом, NFC – это удобный и безопасный протокол беспроводной связи, который хорошо подходит для различных приложений IoT.

RFID



RFID (Radio Frequency Identification) – это протокол, используемый для отслеживания и идентификации объектов с помощью радиоволн. Он широко используется в приложениях IoT, особенно в управлении цепочками поставок, отслеживании запасов и управлении активами.

Протокол RFID работает на различных частотах, включая низкочастотные (НЧ), высокочастотные (ВЧ) и сверхвысокочастотные (СВЧ). LF RFID работает в диапазоне частот от 125 кГц до 134 кГц, в то время как HF RFID работает на частоте 13,56 МГц. УВЧ RFID работает в диапазоне от 860 МГц до 960 МГц. Диапазон частот влияет на дальность действия и скорость передачи данных RFID-меток.

RFID использует комбинацию лицензированных и нелицензированных частот в зависимости от конкретной используемой частоты. Некоторые частоты требуют лицензий, а другие – нет.

RFID имеет низкую пропускную способность и работает с относительно низкой скоростью передачи данных по сравнению с другими протоколами, но она отлично справляется с идентификацией и отслеживанием большого количества объектов быстро и точно. Потребление энергии также относительно низкое, что делает этот протокол подходящим для устройств, работающих от батарей.

Метки RFID можно считывать на расстоянии, не требующем прямой видимости, что делает их популярным выбором для отслеживания активов и управления запасами. Однако в определенных условиях RFID может страдать от помех, что снижает ее надежность.

RFID – это универсальный протокол, используемый во многих приложениях IoT, включая отслеживание розничных запасов, управление цепочками поставок,

отслеживание активов и контроль доступа. Он также используется в платежных системах, таких как бесконтактные платежные карты и системы мобильных платежей.

В целом, RFID – это надежный и эффективный протокол для отслеживания и идентификации объектов в приложениях IoT. Хотя он может не обладать высокой пропускной способностью, как другие протоколы, его способность быстро и точно идентифицировать большое количество объектов делает его ценным инструментом во многих отраслях.

LoRaWAN

LoRaWAN (Long Range Wide Area Network) – это беспроводной протокол с низким энергопотреблением и большим радиусом действия, разработанный для приложений IoT. Он работает в безлицензионном диапазоне ISM и может достигать дальности действия до 15 км в сельской местности, что делает его пригодным для использования в удаленных и труднодоступных местах.

LoRaWAN использует технологию модуляции в распределенном спектре под названием Chirp Spread Spectrum (CSS) для передачи данных с низкой скоростью на большие расстояния, потребляя при этом очень мало энергии. Она может поддерживать двунаправленную связь между конечными устройствами и централизованным сетевым сервером, позволяя устройствам отправлять данные и получать команды.

Одним из ключевых преимуществ LoRaWAN является ее способность работать в условиях низкого энергопотребления, что позволяет устройствам годами работать от одной батареи. Кроме того, LoRaWAN обладает высоким уровнем надежности, даже в зонах с высоким уровнем помех.

Однако низкая скорость передачи данных и ограниченная пропускная способность LoRaWAN могут сделать ее менее подходящей для приложений, требующих высокой пропускной способности, таких как потоковое видео или аудио. Кроме того, сети LoRaWAN требуют значительных инвестиций в инфраструктуру, включая шлюзовые устройства и сетевые серверы, что может стать барьером для некоторых организаций.

LoRaWAN особенно хорошо подходит для приложений, требующих подключения на большие расстояния и низкого энергопотребления, таких как интеллектуальное сельское хозяйство, отслеживание активов и интеллектуальная городская инфраструктура. Она также может использоваться в промышленных приложениях, например, для мониторинга оборудования в удаленных местах или отслеживания перемещения товаров по цепочке поставок.

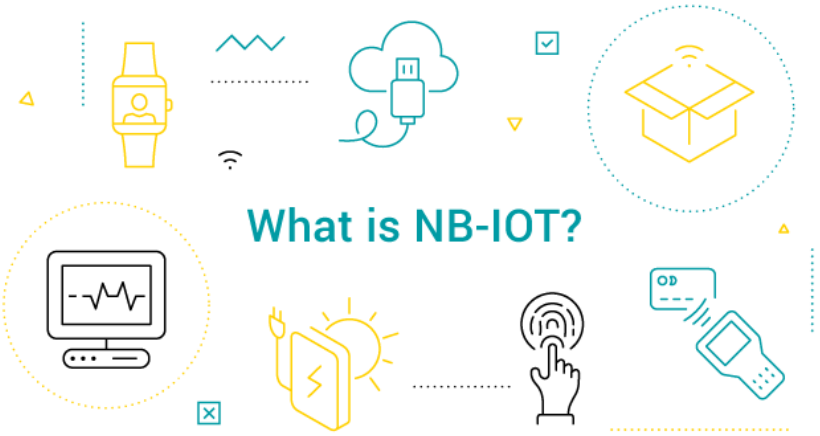
SigFox

Sigfox – это запатентованный протокол маломощной глобальной сети (LPWAN), предназначенный для обеспечения связи на большие расстояния с низкой пропускной способностью для устройств IoT. Протокол работает на нелицензируемых радиочастотах, используя сверхширокополосную модуляцию для передачи данных на большие расстояния.

- **Частоты**: Sigfox работает в безлицензионных промышленных, научных и медицинских (ISM) диапазонах 868 МГц в Европе и 915 МГц в США и других регионах.
- **Рабочий спектр**: Sigfox работает на нелицензированном спектре, что означает, что пользователям не нужно получать лицензию для работы своих устройств.
- **Пропускная способность**: Sigfox является протоколом с низкой пропускной способностью, с максимальной скоростью передачи 100 бит в секунду (бит/с).
- **Энергопотребление**: Одним из ключевых преимуществ Sigfox является низкое энергопотребление, что позволяет IoT-устройствам работать в течение длительного времени от одной батареи.
- **Задержки**: Sigfox – это протокол с низкой задержкой, типичное время передачи данных из конца в конец составляет около 1-2 секунд.
- **Надежность**: Sigfox разработан для обеспечения надежности, с сильными возможностями коррекции и обнаружения ошибок. Однако из-за дальнобойности протокола в некоторых условиях возможна потеря пакетов или помехи.

- **Сильные стороны**: Низкое энергопотребление и дальнобойность Sigfox делают его хорошо подходящим для приложений, где устройства должны работать в течение длительного времени без обслуживания, или где им требуется связь на больших расстояниях. Низкая стоимость и простота протокола также делают его привлекательным вариантом для многих приложений IoT.
- **Слабые стороны**: Низкая пропускная способность Sigfox может ограничить его полезность для некоторых приложений, например, тех, которые требуют высокоскоростной передачи данных или связи в режиме реального времени. Кроме того, поскольку Sigfox является проприетарным протоколом, пользователи вынуждены использовать инфраструктуру компании, что может ограничить гибкость и масштабируемость.
- **Примеры использования**: Sigfox широко используется в различных приложениях, включая отслеживание активов, умное сельское хозяйство, промышленную автоматизацию и умные города. В этих контекстах низкое энергопотребление протокола и его возможности дальнего радиуса действия могут быть особенно полезны.

NB-IoT



NB-IoT (Narrowband Internet of Things) – это протокол маломощной широкозоновой сети (LPWAN), разработанный для приложений IoT, требующих надежного и недорогого соединения на больших расстояниях. Это сотовая технология, которая работает в лицензированных частотных диапазонах, что означает, что для развертывания сетей NB-IoT сетевые операторы должны получить лицензии от регулирующих органов.

NB-IoT использует узкополосный радиочастотный (РЧ) канал для передачи небольших пакетов данных на большие расстояния с минимальным энергопотреблением. Он имеет низкую пропускную способность до 250 кбит/с, что

достаточно для передачи небольших объемов данных, таких как показания датчиков или координаты GPS. Технология также имеет низкую задержку и высокую надежность, что делает ее идеальной для IoT-приложений, требующих передачи данных в реальном времени, таких как промышленная автоматизация, "умные города" и удаленный мониторинг.

Одним из достоинств NB-IoT является низкое энергопотребление, что позволяет устройствам работать годами от одного заряда батареи. Он также обладает отличным проникновением сигнала, что позволяет устройствам поддерживать связь даже в местах со слабым покрытием сотовой связи, например, в подвалах или на подземных парковках. Кроме того, сети NB-IoT легко интегрируются с существующими сотовыми сетями, что делает их удобным вариантом для операторов сетей и производителей устройств.

Однако одним из недостатков NB-IoT является ограниченная пропускная способность, что делает ее непригодной для приложений, требующих высокой скорости передачи данных, таких как потоковое видео или передача изображений высокого разрешения. Кроме того, требование лицензирования частотных диапазонов может стать барьером на пути к выходу на рынок для небольших сетевых операторов или производителей устройств, поскольку получение лицензий может быть дорогостоящим и длительным.

Сферы применения NB-IoT включают "умные" города, сельское хозяйство, мониторинг окружающей среды, отслеживание активов и промышленную автоматизацию. Например, "умные" города могут использовать NB-IoT для мониторинга качества воздуха, дорожного движения и систем управления отходами, а сельскохозяйственные приложения могут использовать технологию для мониторинга влажности почвы и погодных условий. Приложения для отслеживания активов и промышленной автоматизации могут использовать NB-IoT для мониторинга оборудования и обеспечения бесперебойной работы.

LoRaWAN, SigFox и NB-IoT – три популярные технологии маломощных глобальных сетей (LPWAN), используемые в приложениях IoT. Каждая из них имеет свои уникальные характеристики и случаи использования, а также сильные и слабые стороны.

LoRaWAN (Long Range Wide Area Network) работает в нелицензируемых субгигагерцовых частотных диапазонах, которые являются бесплатными для использования, и может достигать дальности действия до 10 км в сельской местности. LoRaWAN использует технологию распространения спектра и может поддерживать большое количество конечных устройств, что делает ее подходящей для приложений, требующих связи на большом расстоянии и низкого энергопотребления, таких как интеллектуальное сельское хозяйство, интеллектуальные города и промышленный мониторинг. Сильной стороной

LoRaWAN является большой радиус действия и низкое энергопотребление, но она имеет меньшую пропускную способность по сравнению с другими технологиями LPWAN, что делает ее непригодной для приложений, требующих высокой скорости передачи данных.

SigFox работает в лицензированных субгигагерцовых частотных диапазонах и имеет радиус действия до 50 км в сельской местности. SigFox использует сверхширокополосную технологию и может поддерживать до 1 миллиона устройств на базовую станцию, что делает его подходящим для приложений, требующих связи на большом расстоянии и низкого энергопотребления, таких как интеллектуальное сельское хозяйство, интеллектуальные города и промышленный мониторинг. Сильной стороной SigFox является большой радиус действия и низкое энергопотребление, но он имеет низкую пропускную способность и ограниченную емкость восходящего канала, что делает его непригодным для приложений, требующих двунаправленной связи или высокой скорости передачи данных.

NB-IoT (Narrowband IoT) работает в лицензированных частотных диапазонах сотовой связи и является частью сотовых сетей 4G и 5G. NB-IoT имеет радиус действия до 10 км и может поддерживать большое количество устройств, что делает его подходящим для приложений, требующих подключения к сотовой сети, таких как "умные города", управление автопарком и отслеживание активов. Сильной стороной NB-IoT является ее надежность и высокая скорость передачи данных, но она имеет более высокое энергопотребление по сравнению с другими технологиями LPWAN и требует наличия сотовой инфраструктуры, что может сделать ее развертывание более дорогостоящим.

LoRaWAN, SigFox и NB-IoT – это три технологии LPWAN, которые предлагают различные преимущества и подходят для разных случаев использования. LoRaWAN и SigFox идеально подходят для связи на большие расстояния и низкого энергопотребления, а NB-IoT обеспечивает надежность и высокую скорость передачи данных. При выборе технологии LPWAN для конкретного приложения IoT важно учитывать дальность связи, энергопотребление, скорость передачи данных и стоимость развертывания.

Выбор правильной технологии

Выбор правильной технологии для приложения IoT зависит от различных факторов, таких как требования приложения, среда, бюджет и потребности в масштабируемости. Вот некоторые факторы, которые следует учитывать при выборе технологии:

- **Дальность**: Если приложение требует подключения на большом расстоянии, то могут подойти такие технологии, как LoRaWAN, SigFox или NB-IoT.

- **Скорость передачи данных**: Если приложение требует высокоскоростной передачи данных, то могут подойти такие технологии, как Wi-Fi, Bluetooth или сотовая связь.
- **Энергопотребление**: Если устройства, используемые в приложении, работают от батарей и требуют длительного времени автономной работы, то такие технологии, как LoRaWAN или SigFox, могут быть предпочтительными из-за их низкого энергопотребления.
- **Стоимость**: Стоимость внедрения технологии является решающим фактором, который необходимо учитывать. Такие технологии, как Wi-Fi или Bluetooth, легко доступны и менее дороги, чем такие технологии, как SigFox или NB-IoT.
- **Масштабируемость**: Если приложение требует подключения большого количества устройств, то такие технологии, как ZigBee или Wi-Fi, могут подойти из-за их высокой пропускной способности и масштабируемости.
- **Среда**: Среда, в которой развертывается приложение, играет решающую роль в выборе подходящей технологии. Например, если приложение будет развернуто в удаленном районе, то такие технологии, как LoRaWAN или SigFox, могут быть предпочтительными благодаря их возможности подключения на большие расстояния.

Attribute	Bluetooth® Low Energy Technology	Wi-Fi	Z-Wave	IEEE 802.15.4 (Zigbee, Thread)	LTE-M	NB-IoT	Sigfox	LoRaWAN
Range	10 m – 1.5 km	15 m – 100 m	30 m - 50 m	30 m – 100 m	1 km – 10 km	1 km – 10 km	3 km – 50 km	2 km – 20 km
Throughput	125 kbps – 2 Mbps	54 Mbps – 1.3 Gbps	10 kbps – 100 kbps	20 kbps – 250 kbps	Up to 1 Mbps	Up to 200 kbps	Up to 100 bps	10 kbps – 50 kbps
Power Consumption	Low	Medium	Low	Low	Medium	Low	Low	Low
Ongoing Cost	One-time	One-time	One-time	One-time	Recurring	Recurring	Recurring	One-time
Module Cost	Under $5	Under $10	Under $10	$8-$15	$8-$20	$8-$20	Under $5	$8-$15
Topology	P2P, Star, Mesh, Broadcast	Star, Mesh	Mesh	Mesh	Star	Star	Star	Star
Shipments in 2019 (millions)	~3,500	~3,200	~120	~420	~7	~16	~10	~45

В конечном итоге важно оценить конкретные потребности вашего приложения IoT и выбрать технологию, которая наилучшим образом отвечает этим требованиям.

Заключение

На данном занятии мы рассмотрели мы рассмотрели современные протоколы передачи данных; какие типы беспроводных протоколов существует: отличие LPWAN от WLAN систем. Разобрали самые популярные протоколы и технологии передачи данных, а также изучим протоколы взаимодействия самих устройств.

Данное занятие является последним в лекционном цикле, поэтому подытожим, что же удалось изучить за курс.

На первом занятии мы изучили, что такое IoT, какие рынки IoT существуют, его движущие силы (то , почему к IoT прибегают), сферы применения и достигаемые эффекты внедрения. Разобрали плюсы и минусы IoT, изучили терминологию и эталонный подход по описанию данной концепции технологий.

На втором занятии мы изучили архитектуру IoT решений, узнали из чего состоит экосистема интернета вещей. Посмотрели, как вещи могут взаимодействовать между собой или с информационными системами.

На третьем занятии мы рассмотрели датчики и телеметрию в контексте IoT, как работает датчик и его состав, типы чувствительных элементов и примеры датчиков, а также что такое подготовка датчиков.

На четвертом занятии мы рассмотрели платформы интернета вещей. Что это такое и в чем их назначение, посмотрели конкретно их роль в решениях интернета вещей, рассмотрели из каких ключевых элементов состоят подобные платформы. Разобрали с вами примеры реальных IoT платформ, как отечественных, так и зарубежных вендоров.

Домашнее задание

1. Какую технологию (или набор технологий) вы бы использовали в своем решении и почему? Чем это решение лучше альтернатив?