Лекция 4. Технологии реализации IoT

Цель лекции – предоставить студентам всестороннее понимание концепции IoT и его ключевых технологий, а также ознакомить с различными типами сетей, включая энергоэффективные решения и протоколы связи, которые обеспечивают передачу данных в системах IoT.

Введение

В данной лекции рассмотрим широкий спектр технологий, обеспечивающих функциональность IoT, включая беспроводные и проводные сети, протоколы связи, а также вспомогательные технологии, такие как RFID и NFC. Также обсудим важность аналитики больших данных и облачных вычислений в контексте IoT, а также то, как эти компоненты взаимодействуют для создания эффективных и адаптивных систем.

Понимание основ этих технологий поможет лучше осознать, как они формируют будущее, улучшая различные аспекты нашей жизни и работы.

Виды технологии IoT

Спектр возможных технологий, используемых для передачи трафика «Интернета вещей», охватывает как беспроводные, так и проводные сети. Для беспроводной передачи данных особо важную роль в построении Интернета вещей играют такие качества, как эффективность в условиях низких скоростей, отказоустойчивость, адаптивность, возможность самоорганизации.

Беспроводные сети для Интернета вещей подразделяются на следующие типы:

- Low Power Short Range Networks – энергоэффективные сети малого радиуса действия;
- Low Power Wide Area Networks (LPWAN) – энергоэффективные сети большого радиуса действия;
- Cellular Network – технологии, основанные на использовании стандартов сотовых сетей в лицензируемом диапазоне.

Short Range и LPWAN построены на использовании нелицензированного диапазона частот – ISM Bands. В секторе Short Range выделяют стандарт IEEE 802.15.4, определяющий физический слой и управление доступом для организации энергоэффективных персональных сетей, и являющийся основой для таких протоколов, как ZigBee, WirelessHart, MiWi, 6LoWPAN, а также Bluetooth low energy, NFC, WLAN (Wi-Fi). В секторе LPWAN существуют следующие основные стандарты и технологии – SigFox, Symphony Link, Nwave, Ingenu (RPMA), Weightless, LoRa. Отдельно выделяются технологии, базирующие на сетях мобильной связи, использующих лицензируемые частотные диапазоны – стандарты eMTC, EC-GSM-IoT, NB-IoT. eMTC и NB-IoT разворачивается на оборудовании сетей LTE (также допускается строительство выделенных сетей NB-IoT в т.ч. в частотных каналах сетей GSM); EC-GSM-IoT разворачивается поверх сетей стандарта GSM. При этом технологию NB-IoT также принято относить к энергоэффективным сетям большого радиуса действия (LPWAN). Сравнение беспроводных технологий IoT по дальности действия и полосе пропускания.

Среди проводных технологий важную роль в проникновении Интернета вещей играют решения PLC – технологии построения сетей по линиям электропередач, так как во многих устройствах присутствует доступ к электросетям. Например, торговые автоматы, банкоматы, интеллектуальные счётчики, контроллеры освещения изначально подключены к сети электроснабжения.

Беспроводные сенсорные сети

Беспроводные сенсорные сети состоят из распределенных устройств с датчиками, которые используются для мониторинга окружающей среды и физических условий. Беспроводная сенсорная сеть состоит из конечных узлов, маршрутизаторов и координаторов. К конечным узлам подключено несколько датчиков, данные с которых передаются координатору с помощью маршрутизаторов. Координатор также выступает в качестве шлюза, который соединяет беспроводную сенсорную сеть с Интернетом. Примеры применения:

- Система мониторинга погоды;
- Система мониторинга качества воздуха в помещении;
- Система мониторинга влажности почвы;
- Система наблюдения;
- Система мониторинга здоровья.

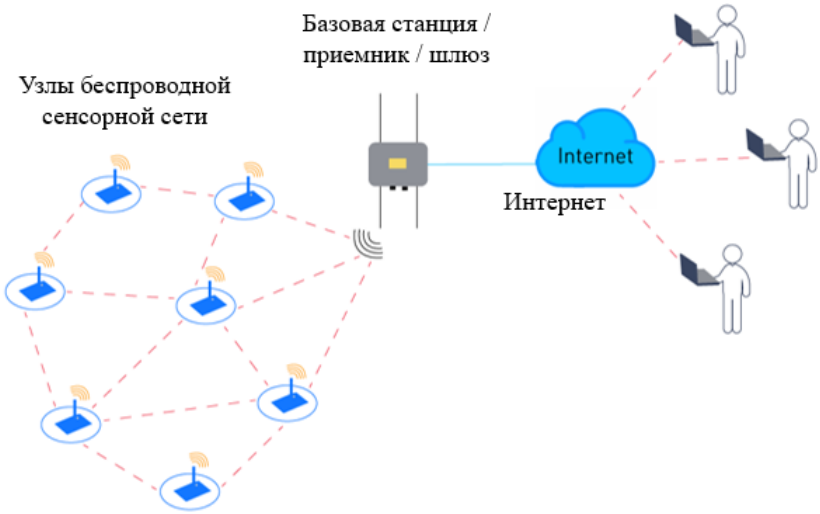

Рисунок 4.1. Схема беспроводной сенсорной сети

IoT в первую очередь использует стандартные протоколы и сетевые технологии. Однако основными вспомогательными технологиями и протоколами IoT являются RFID, NFC, Bluetooth с низким энергопотреблением, беспроводная связь с низким энергопотреблением, радиопротоколы с низким энергопотреблением и LTE-A. Эти технологии поддерживают определенную сетевую функциональность, необходимую в системе IoT, в отличие от стандартной однородной сети общих систем. Помимо этих вспомогательных технологий, IoT также опирается на другие технологии для максимизации возможностей, которые создает IoT: аналитика Big Data, облачные вычисления, протоколы связи, встроенная система.

Аналитика больших данных (Big Data)

Это относится к методу изучения огромных объемов данных или Big Data. Сбор данных, объем, скорость или разнообразие которых просто слишком огромны и сложны для хранения, контроля, обработки и изучения данных с использованием традиционных баз данных. Big Data собираются из различных источников, включая видеоролики социальных сетей, цифровые изображения, датчики и записи о торговых операциях.

Big Data – это объемные и разнообразные данные, которые приходят из различных источников и могут быть структурированными, полуструктурированными или неструктурированными. Основные характеристики Big Data можно описать через 5 «V»:

- **Volume (Объем)**: большие объемы данных, которые требуют специальных технологий для хранения и обработки.
- **Velocity (Скорость)**: скорость, с которой данные генерируются и обрабатываются.
- **Variety (Разнообразие)**: различные типы данных (текст, изображения, видео и т.д.).
- **Veracity (Достоверность)**: качество и надежность данных.
- **Value (Ценность)**: способность данных приносить бизнес-ценность и инсайты.

Этапы анализа Big Data:

1. **Сбор данных** – использование различных источников данных (датчики, социальные сети, базы данных и т.д.) и применение инструментов для интеграции и сбора данных.
2. **Очистка данных** – обработка и фильтрация данных для удаления ошибок, дубликатов и пропусков.
3. **Хранение данных** – выбор подходящей архитектуры для хранения данных, например, Hadoop, NoSQL базы данных или облачные решения.
4. **Обработка и анализ данных** – использование методов статистики, машинного обучения и аналитических инструментов для выявления паттернов и тенденций, а также применение алгоритмов для прогнозирования и классификации данных.
5. **Визуализация данных** – презентация результатов анализа в наглядной форме с помощью графиков, диаграмм и дашбордов.
6. **Интерпретация результатов** – анализ полученных инсайтов в контексте бизнес-целей и принятие решений на основе этих данных.

Применение анализа Big Data

- **Бизнес**: оптимизация маркетинга, управление запасами, анализ поведения клиентов.
- **Здравоохранение**: анализ клинических данных, прогнозирование вспышек заболеваний.
- **Финансовый сектор**: управление рисками, обнаружение мошенничества.
- **Торговля**: персонализация предложений, оптимизация цепочек поставок.

Облачные вычисления

Облачные вычисления предоставляют нам средства, с помощью которых мы можем получать доступ к приложениям как к утилитам через Интернет. Облако означает что-то, что присутствует в удаленных местах. С помощью облачных вычислений пользователи могут получать доступ к любым ресурсам из любой точки мира, таким как базы данных, веб-серверы, хранилища, любое устройство и любое программное обеспечение через Интернет. К основным характеристикам облачных вычислений относятся – широкий сетевой доступ, самообслуживание по требованию, быстрая масштабируемость, измеряемый сервис, оплата по факту использования.

Облачные вычисления делятся на несколько моделей:

- IaaS (Infrastructure as a service – Инфраструктура как услуга). IaaS предоставляет онлайн-услуги, такие как физические машины, виртуальные машины, серверы, сети, хранилища и центры обработки данных на основе оплаты за использование. Основные провайдеры IaaS: Google Compute Engine, Amazon Web Services и Microsoft Azure и т.д. Примеры применения: веб-хостинг, виртуальная машина и т.д.
- PaaS (Platform as a service – Платформа как услуга) предлагает платформу для разработки, тестирования и развертывания приложений. Примеры PaaS-платформ включают: Heroku – простая платформа для развертывания веб-приложений; Google App

Engine – позволяет создавать приложения на Google Cloud; Microsoft Azure App Service – предлагает инструменты для разработки на различных языках.

- SaaS (Software as a service – Программное обеспечение как услуга). Это способ доставки приложений через Интернет как услуги. Вместо установки и обслуживания программного обеспечения вы просто получаете к нему доступ через Интернет, освобождая себя от сложного управления программным обеспечением и оборудованием. SaaS-приложения иногда называют веб-программным обеспечением по требованию или размещенным программным обеспечением. SaaS-приложения работают на сервисе SaaS-провайдера и управляют безопасностью, доступностью и производительностью. Например: Google Docs, Gmail, office и т.д.

Протоколы связи

Они являются основой систем IoT и обеспечивают сетевое подключение и связь с приложениями. Протоколы связи позволяют устройствам обмениваться данными по сети. Несколько протоколов часто описывают различные аспекты одного сообщения. Группа протоколов, предназначенных для совместной работы, известна как набор протоколов; при реализации в программном обеспечении они представляют собой стек протоколов. Они используются в кодировании данных и схемах адресации.

Встроенная система

Это комбинация аппаратного и программного обеспечения, используемая для выполнения специальных задач. Она включает в себя память микроконтроллера и микропроцессора, сетевые блоки (адаптеры Ethernet Wi-Fi), блоки ввода-вывода и устройства хранения. Она собирает данные и отправляет их в Интернет.

Эти вспомогательные технологии существуют для того, чтобы гарантировать, что данные с устройств IoT могут быть собраны, сохранены и проанализированы.

Теперь давайте подробнее рассмотрим технологии, обеспечивающие Интернет вещей.

RFID (radio frequency identification – радиочастотная идентификация)

RFID (радиочастотная идентификация) — это форма беспроводной связи, которая включает использование электромагнитной или электростатической связи в радиочастотной части электромагнитного спектра для уникальной идентификации объекта, животного или человека..

Каждая система RFID состоит из трех компонентов: сканирующей антенны, приемопередатчика и транспондера. Когда сканирующая антенна и приемопередатчик объединены, они называются считывателем или считывателем RFID. Существует два типа считывателей RFID – стационарные считыватели и мобильные считыватели. Считыватель RFID – это подключенное к сети устройство, которое может быть портативным или постоянно подключенным. Он использует радиоволны для передачи сигналов, которые активируют метку. После активации метка посылает волну обратно на антенну, где она преобразуется в данные.

Транспондер находится в самой метке RFID. Диапазон считывания меток RFID зависит от таких факторов, как тип метки, тип считывателя, частота RFID и помехи в окружающей среде или от других меток RFID и считывателей. Метки, которые имеют более мощный источник питания, также имеют больший диапазон считывания.

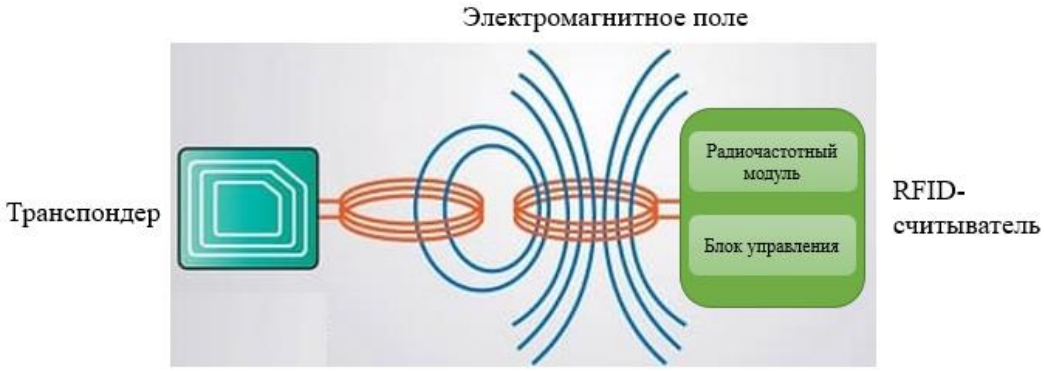

Рисунок 4.2. Принцип работы RFID

RFID-метки состоят из интегральной схемы (ИС), антенны и подложки. Часть RFID-метки, которая кодирует идентификационную информацию, называется RFID-вкладышем.

Существует два основных типа RFID-меток:

- Активная RFID. Активная RFID-метка имеет собственный источник питания, часто аккумулятор.
- Пассивная RFID. Пассивная RFID-метка получает питание от считывающей антенны, электромагнитная волна которой индуцирует ток в антенне RFID-метки.

Существуют также полупассивные RFID-метки, в которых питание схемы осуществляется от батареи, а связь обеспечивается RFID-считывателем.

Маломощная встроенная энергонезависимая память играет важную роль в каждой системе RFID. RFID-метки обычно содержат менее 2000 КБ данных, включая уникальный идентификатор/серийный номер. Метки могут быть только для чтения или для чтения и записи, когда данные могут быть добавлены считывателем или существующие данные перезаписаны.

Диапазон считывания RFID-меток зависит от таких факторов, как тип метки, тип считывателя, частота RFID и помехи в окружающей среде или от других RFID-меток и считывателей. Активные RFID-метки имеют больший диапазон считывания, чем пассивные RFID-метки, из-за более сильного источника питания.

Смарт-метки – это простые RFID-метки. Эти этикетки имеют RFID-метку, встроенную в клейкую этикетку, и содержат штрих-код. Их также могут использовать как RFID-считыватели, так и считыватели штрих-кодов. Смарт-метки можно печатать по запросу с помощью настольных принтеров, где для RFID-меток требуется более современное оборудование.

Существует три основных типа RFID-систем: низкочастотные (НЧ), высокочастотные (ВЧ) и сверхвысокочастотные (СВЧ). Также доступны микроволновые RFID. Частоты сильно различаются в зависимости от страны и региона.

- Низкочастотные системы RFID. Диапазон составляет от 30 кГц до 500 кГц, хотя типичная частота составляет 125 кГц. LF RFID имеет короткие диапазоны передачи, как правило, от нескольких сантиметров до менее двух метров.
- Высокочастотные системы RFID Диапазон составляет от 3 МГц до 30 МГц, типичная частота HF составляет 13,56 МГц. Стандартный диапазон составляет от нескольких сантиметров до нескольких метров.
- Системы UHF RFID. Диапазон составляет от 300 МГц до 960 МГц, типичная частота составляет 433 МГц, и их обычно можно считывать с расстояния более 8 метров.
- Микроволновые системы RFID. Они работают на частоте 2,45 ГГц и могут считываться с расстояния более 10 метров.

RFID появилась в 1940-х годах; однако в 1970-х годах ее стали использовать чаще. Долгое время высокая стоимость меток и считывателей препятствовала широкому

коммерческому использованию. По мере снижения стоимости оборудования внедрение RFID также возросло.

Применение технологии RFID в IoT чрезвычайно широко и разнообразно. Метки RFID в основном используются для связи повседневных предметов друг с другом и с главным узлом и сообщения о своем состоянии. Розничная торговля, производство, логистика, интеллектуальное складирование и банковское дело входят в число основных отраслей, использующих решения RFID для Интернета вещей.

RFID подвержен двум основным проблемам:

- Коллизия считывателей. Коллизия считывателей, когда сигнал от одного считывателя RFID мешает второму считывателю, можно предотвратить с помощью протокола антиколлизии, чтобы метки RFID по очереди передавали данные соответствующему считывателю.
- Коллизия меток. Коллизия меток происходит, когда слишком много меток сбивают с толку считыватель RFID, передавая данные одновременно. Выбор считывателя, который собирает информацию о метках по одному за раз, предотвратит эту проблему.

NFC (Near-field communication – связь ближнего действия)

NFC – это технология беспроводной связи на коротком расстоянии, которая использует индукцию магнитного поля для обеспечения связи между устройствами, когда они соприкасаются или находятся на расстоянии нескольких сантиметров друг от друга. Это включает в себя аутентификацию кредитных карт, обеспечение физического доступа, передачу небольших файлов и запуск более эффективных беспроводных соединений. В целом, она основывается на существующих экосистемах и стандартах, связанных с радиочастотными идентификационными метками (RFID), и расширяет их.

NFC расширяет возможности RFID и бесконтактной связи с помощью более динамичных функций, поддерживаемых современными смартфонами. Все современные телефоны теперь поддерживают чипы и приложения NFC, такие как Apple Pay и Google Pay, чтобы использовать миллиарды уже развернутых RFID-меток и терминалов. NFC упрощает загрузку нескольких карт в один телефон для платежей, городского транспорта, доступа в здание, открытия дверей автомобиля и других вариантов использования. NFC поддерживает интерактивные приложения, основанные на базовых возможностях RFID, таких как автоматическое сопряжение наушников Bluetooth и подключений Wi-Fi. Он также может автоматически извлекать данные или приложение из постера или рекламы. Первоначально он предназначался для передачи файлов между телефонами с помощью Android Beam. Современные сервисы, такие как Google Nearby Share, используют NFC для настройки беспроводных сервисов в более быстрых сетях, таких как Bluetooth или Wi-Fi Direct.

NFC ограничен связью на коротких расстояниях, что имеет важные последствия для безопасности физического доступа. Пользователь должен находиться в пределах 10 см от терминала NFC, чтобы обработать платеж или открыть дверь. Другим важным аспектом является то, что для базовой механики прослушивания и ответа на запросы NFC не требуется питание. Это позволяет реализовать его в предметах, в которых отсутствует батарея, таких как кредитные карты.

NFC также дополняет беспроводные технологии, такие как Bluetooth, Ultrawideband (UWB), Wi-Fi direct и QR-коды. Его наиболее существенное преимущество заключается в том, что это самая простая беспроводная технология для настройки соединения, что делает ее полезной для устройств IoT. Однако она не так хороша для поддержания соединения на расстоянии или в течение длительного времени.

NFC работает на основе трех важнейших инноваций в области беспроводных считывателей меток, криптографической обработки кредитных карт и одноранговой (P2P) соединения для обеспечения различных приложений.

NFC основывается на работе набора стандартов и спецификаций RFID, таких как ISO/IEC 14443 и ISO/IEC 15963. Они используют преимущества беспроводной технологии связи, использующей другие физические принципы, чем большинство беспроводных радиоустройств. В то время как большинство радиоустройств передают данные посредством распространения радиоволн, NFC передает данные посредством индукции магнитного поля. Данные NFC передаются на частоте 13,56 МГц, что соответствует длине волны 22 метра.

Одним из важнейших аспектов передачи данных посредством индукционной связи, а не радиоволн, является то, что поле затухает гораздо быстрее, чем радиоволны. Это полезно для предотвращения прослушивания людьми конфиденциальных разговоров о транзакциях по кредитным картам, кодах доступа к дверям или другой конфиденциальной информации.

Второе значимое новшество NFC включает криптографическую обработку кредитных карт, используемую для бесконтактных платежей. Криптография с открытым ключом позволяет карте генерировать новый код аутентификации для каждой транзакции, не раскрывая необработанные данные карты или трехзначный код на обороте. Это гарантирует, что даже если кто-то подслушает или хакер запросит карту в оживленном метро, он никогда не узнает оригинальные данные карты. Форум NFC, некоммерческая отраслевая ассоциация, взял эти два строительных блока и добавил P2P-подключение поверх стандарта ISO/IEC 18092. Классические случаи использования RFID и кредитных карт включают активный считыватель карт, который запрашивает пассивную метку или карту, что является односторонним взаимодействием. Форум NFC представил спецификации, которые позволили более мощным устройствам, таким как смартфоны, наушники, маршрутизаторы, бытовая техника и промышленное оборудование, инициировать или реагировать на запросы NFC. Это открыло широкий спектр шаблонов взаимодействия и подключения. Также потребовалось много работы, чтобы упростить обмен информацией, минимизируя уязвимости безопасности. Например, вы можете приложить два телефона друг к другу, чтобы обмениваться контактными данными с помощью Android Beam, но не случайно обмениваться исполняемым кодом, который может распространять вирус.

Поставщики смартфонов начинают создавать некоторые базовые возможности выполнения приложений поверх этого. В экосистеме Google смарт-тег может запускать прогрессивное веб-приложение, работающее в браузере. Apple недавно запустила Apple App Clips, в котором тег NFC или QR-код может запускать приложения с базовой функциональностью для таких вещей, как заказ в ресторане или разблокировка киоска проката скутеров без загрузки полноценного приложения. Эти приложения ограничены в доступе к конфиденциальным данным на телефоне.

Вот несколько примеров использования NFC:

- мобильные платежи, такие как Apple Pay и Google Pay;
- платежи по транспортным картам;
- выкуп билетов на концерте или в театре;
- аутентификация доступа к дверям или офисам;
- разблокировка дверей автомобиля или арендованного скутера;
- регистрация на месте или в месте для оповещения друзей в социальных сетях;
- сопряжение смартфонов и гарнитур путем их соприкосновения;
- автоматическая настройка подключения по Wi-Fi путем соприкосновения телефона с маршрутизатором или интернет-шлюзом;
- подключение через смартфон к радиатору для настройки его температурных параметров и графика;
- подключение через смартфон или планшет к промышленному оборудованию для доступа к более сложной панели управления.

Контрольные вопросы:

1. В чем различия между Low Power Short Range Networks (LPSRN) и Low Power Wide Area Networks (LPWAN)?
2. Какие основные протоколы используются в беспроводных сенсорных сетях, и какую роль они играют в IoT?
3. Как аналитика больших данных поддерживает функциональность IoT?
4. Опишите ключевые этапы анализа данных.
5. Что такое облачные вычисления, и как они взаимодействуют с IoT для улучшения обработки данных?
6. Как работают технологии RFID и NFC, и в каких случаях они наиболее эффективны в контексте IoT?
7. Приведите примеры реальных приложений IoT в различных отраслях и объясните их влияние на производительность и инновации.