ВС/NW 2022 № 1 (39):2.3

АРХИТЕКТУРА, ТЕХНОЛОГИИ, ПРОТОКОЛЫ, ПРИМЕНЕНИЕ IOT

(Лекция курса «Интернет вещей»)

Широков В. Л.

Аннотация. Рассматриваются средства, архитектура, технологии, интерфейсы «вещей» (устройств), протоколы передачи данных, области применений одного из самых перспективных сетевых направлений в информационно-коммуникационных технологиях – «Интернета вещей».

Ключевые слова: «Интернет людей», RFID, «Интернет вещей», IoT, IPv6, SDN, WPAN, Wi-Fi, 3G, LTE, 5G, LoRaWAN, NB-IoT, Mesh, MQTT, M2M, Clouds, Edge & Fog computing.

I. Введение

1. Понятие «Интернета вещей»

«Интернет вещей» (Internet of Things, IoT, читается как «ай оу ти») — это общее название совокупности технологий, объединённых задачей построения систем автоматизированного мониторинга и сетевого управления.

Интернет вещей -концепция сети передачи данных между физическими объектами, оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. Предполагается, что организация таких сетей способна перестроить экономические и общественные процессы, исключить из части действий и операций необходимость участия человека.

Системы IoT (практически) могут:

- ✓ включать в себя различные, заранее неизвестные типы датчиков и исполнительных элементов (как проводные, так и беспроводные);
- ✓ работать как поверх сетей общего пользования, так и в изолированных инсталляциях;
- ✓ осуществлять управление как в автоматическом режиме по заранее заданному алгоритму, так и вручную;
- ✓ использовать различные типы клиентских устройств и интерфейсов (графический, телефонный, SMS и др.).

Также к IoT можно отнести многочисленные стандартные и фирменные системы управления, которые разрабатывались отдельными производителями и интеграторами ещё в прошлом веке. Проблема, однако, была в том, что такие решения создавались порознь, каждое под конкретную задачу. И они не имели ни общего взгляда на их архитектуру, ни стандартных протоколов для взаимодействия между различными компонентами этой архитектуры.

Разнообразие подобных решений чрезвычайно велико. Практика чаще ставит новые задачи, с новыми вариациями в каждом из аспектов, нежели стремится к клонированию типовых наработок. Вместе с тем, в середине 2010-х гг. в данной области стали проявляться некоторые общие тенденции и принципы построения этих систем. Именно эти подходы позволяют рассматривать объекты «Интернета вещей» как единообразную (более или менее) универсальную архитектуру.

Современное решение из класса «Интернета вещей» содержит, в том или ином виде, порознь или комбинированно, следующие компоненты:

1) датчики,
2) контроллеры, и
3) актуаторы (исполнительные элементы).

С вышестоящими контроллерами датчики связываются, как правило, по некоторому интерфейсу. На физическом уровне это могут быть проводные интерфейсы:

- RS-232 и RS-485 , Использование последовательной связи дает ряд преимуществ, включая простоту, легкость в использовании и требует всего нескольких контактов GPIO. RS-485 и RS-232

– это два стандарта последовательной передачи данных, которые были рождены давно. Они существовали задолго до USB, SPI, I2C и многих других протоколов, но все еще остаются актуальными и имеют свое место в сегодняшнюю эпоху. Хоть они в возрасте, но они все еще живы и работают. Сравнение RS-232 и RS-485 http://digitrode.ru/articles/3446-klyuchevye-razlichiya-mezhdu-protokolami-rs-485-i-rs-232.html

- 1-Wire, двунаправленная шина для устройств с низкоскоростной передачей данных, в которой данные передаются по цепи питания.
- USB, англ. Universal Serial Bus — «универсальная последовательная шина») — последовательный интерфейс для подключения периферийных устройств к вычислительной технике. Получил широчайшее распространение и стал основным интерфейсом подключения периферии к бытовой цифровой технике.
- CAN. шина – интерфейс, или система цифровой связи управления электрическими устройствами транспортного средства.

Также могут использоваться беспроводные системы малой дальности (Bluetooth, ZigBee и т.п.), Wi-Fi или протоколы сетей большой дальности, например, LPWAN (Low-Power WAN) с низким энергопотреблением.

К числу технологий, определяющих облик современных сетей IoT, относятся также:

- LoRaWAN (Long Range WAN большой дальности), и
- NB-IoT (Narrow Band – узкополосные).

Итак, IoT – это концепция сети передачи данных между физическими устройствами («вещами»), оснащёнными встроенными средствами взаимодействия друг с другом, с контроллерами, интернет и/или с внешней средой. Организация систем IoT позволяет перестроить экономические и общественные процессы, исключая из ряда операций необходимость участия человека.

Внедрение практических решений IoT считается устойчивой тенденцией в информационно-коммуникационных технологиях, начиная с 2010-х годов.

Прежде всего, это происходит благодаря:

- началу перехода на IPv6,
- развитию межмашинного взаимодействия (M2M),
- освоению программно-определяемых сетей (SDN),
- распространению беспроводных сетей (Wireless networks);
- развитию облачных (Clouds) и туманных вычислений (Fog computing).

2. История появления и развития «Интернета вещей»

Концепция и термин «Интернет вещей» были впервые сформулированы Кевином Эштоном, основателем фирмы Auto-ID Labs. В его презентации в 1999 году предсказано, как изменится логистика при массовом внедрении радиочастотных меток RFID (Radio Frequency ID).

А в журнале Scientific American в 2004 году была опубликована статья, посвящённая «Интернету вещей», показывающая возможности концепции в бытовом применении. В этой статье приведены иллюстрации, показывающие как бытовые приборы (будильник, кондиционер), домашние системы (освещение, охранная, садовый полив), датчики (освещённости, тепловые, движения) и «вещи» (например, лекарства, снабжённые RFID) взаимодействуют друг с другом посредством инфракрасной, беспроводной, слаботочной и/или по силовой сети. И обеспечивают полностью автоматическое выполнение ряда процессов: включают кофеварку, изменяют освещённость, напоминают о приёме лекарств, поддерживают температуру, обеспечивают полив сада, позволяют сберегать энергию, управляя её потреблением. Акцент делался на объединение устройств и «вещей» в единую сеть, обслуживаемую интернет-протоколами, на рассмотрение IoT как особого явления. Статья способствовала большей популярности концепции IoT.

В отчёте Национального разведывательного совета США (National Intelligence Council) 2008 года IoT фигурирует также как одна из шести подрывных технологий. Указывается, что повсеместное и незаметное для потребителей превращение в интернет-узлы таких распространённых вещей, как товарная упаковка,

мебель, бумажные документы могут повысить риски в сфере национальной информационной безопасности.

Аналитики корпорации Cisco считают настоящим рождением IoT период с 2008 по 2009 год. По их оценкам, именно в этот период количество устройств, подключённых к Сети, превысило численность населения Земли.

Именно в 2008-2009 гг **«Интернет людей» стал «Интернетом вещей»!**

И с 2009 года в Брюсселе при поддержке Еврокомиссии ежегодно проводится конференция «Internet of Things». На ней представляют доклады еврокомиссары и депутаты Европарламента, правительственные чиновники, руководители известных компаний, таких как **SAP, SAS Institute, Telefónica**, учёные университетов, исследовательских лабораторий.

С начала 2010-х годов платформа IoT становится также движущей силой ***парадигм*** «***облачных***» и ***«туманных вычислений»*** (clouds & fog computing), переносящих вычисления из центров обработки данных (ЦОД) на огромное количество распределённых интеллектуальных (smart) IoT устройств.

3. Технологии IoT

3.1. Средства идентификации

Задействование в IoT физических предметов, не обязательно оснащённых средствами подключения к сетям передачи данных, требует применения технологий идентификации этих предметов («вещей»).

Хотя толчком для появления концепции стала технология RFID, в качестве технологий IoT используются и другие средства идентификации:

- оптически распознаваемые идентификаторы (штрих-коды, QR-коды, Data Matrix),
- определения местонахождения в режиме реального времени.

Примечание. Data Matrix – двумерный матричный штрих-код, состоящий из чёрно-белых элементов или элементов нескольких различных степеней яркости, в форме квадрата или в прямоугольнике, предназначенном для кодирования текста или других типов данных.

При всеобъемлющем распространении IoT принципиально обеспечить уникальность идентификаторов.

Для объектов, подключённых к интернет, канальный MAC-адрес, позволяющий идентифицировать устройство, для приложений не подходит. Хотя диапазон доступных MAC-адресов практически неисчерпаем (для MAC-48 – это 2^{48} адресов). Бо́льшие возможности даёт IPv6, обеспечивающий до 300 млн уникальных адресов сетевого уровня на каждого жителя Земли.

3.2. Средства измерений

Особую роль в IoT играют средства измерений, обеспечивающие преобразование сведений о внешней среде в «читаемые» данные, и тем самым наполняющие вычислительную среду значимой информацией. Используется большой класс средств измерений, от элементарных датчиков (например, температуры, давления, освещённости), приборов учёта потребления (таких, как интеллектуальные счётчики) до интегрированных измерительных систем. В концепции IoT принципиально объединение средств измерений в сети (такие, как измерительные комплексы или сети беспроводных датчиков). За счёт этого возможно межмашинное взаимодействие (M2M).

Особая проблема внедрения IoT – необходимость обеспечения автономности средств измерений. И прежде всего, это проблема энергоснабжения датчиков.

Решения, обеспечивающие автономное питание сенсоров:

- использование фотоэлементов,
- преобразование энергии вибрации,
- преобразование воздушных потоков,
- использование беспроводной передачи электричества.

Эти решения позволяют масштабировать сенсорные сети без повышения затрат на обслуживание:

- смена батареек, или
- подзарядка аккумуляторов.

3.3. Средства передачи данных

Спектр возможных технологий передачи данных охватывает все возможные средства проводных и беспроводных сетей.

Для беспроводной передачи данных особо важную роль в построении IoT играют такие качества, как эффективность в условиях низких скоростей, отказоустойчивость, адаптивность, возможность самоорганизации. Основной интерес в этом представляет стандарт IEEE 802.15.4, определяющий физический слой и управление доступом в персональных сетях, являющийся основой протоколов ZigBee, WirelessHart, MiWi, LPWAN, 6LoWPAN.

Примечания:

1. WirelessHART (IEC 62591) – сетевая технология для беспроводных устройств на базе протокола HART (Highway Addressable Remote Transducer Protocol, разработчик HART Communication Foundation). Использует синхронизированную во времени, самоорганизующуюся и самовосстанавливающуюся ячеистую архитектуру (Mesh) на основе TSMP (Time Synchronized Mesh Protocol) – синхронизированного по времени ячеистого протокола. Работает в Wi-Fi диапазоне 2400-2483,5 МГц для научной, промышленной, медицинской аппаратуры (ISM) стандарта IEEE 802.15.4.
2. MiWi – проприетарный (фирменный) беспроводной протокол Microchip Technology для соединения в структуру звезда. Использует маломощные радиомодули на основе IEEE 802.15.4 для промышленного мониторинга, автоматизации домов и зданий, беспроводные датчики, дистанционное управление, контроль, освещение, считывание показаний счетчиков.
3. 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks, RFC 4944) – стандарт взаимодействия по IPv6 поверх маломощных сетей IEEE 802.15.4. Цель разработки –обеспечение взаимодействия WPANs 802.15 с другими IP-сетями.

В проводных технологиях IoT большую роль играют решения PLC – передача данных по электросетям, поскольку к ним часто имеется доступ (банкоматы, контроллеры освещения, торговые автоматы, интеллектуальные счётчики).

4. Области и направления применения IoT

Применения IoT делятся на следующие направления:

- потребительское,
- инфраструктурное,
- промышленное,
- коммерческое,
- логистика,
- военное.

4.1. Потребительское направление

В с ё большая часть устройств IoT создаётся для использования потребителями, включая (подключенные) транспортные средства, домашнюю автоматизацию, умную одежду, (подключённое) здравоохранение, приборы с возможностями удалённого мониторинга.

4.1.1. Умный дом

Устройства IoT являются частью более широкой концепции домашней автоматизации, которая может включать кондиционирование воздуха, медиа-системы, освещение, отопление, видеонаблюдение, системы безопасности. Долговременную выгоду в этом обеспечит экономия электроэнергии за счет автоматического отключения света, электроники, информирование жителей дома об их использовании.

Умный или интеллектуальный дом делается на концентраторах или платформе, которая управляет

умными устройствами и приборами. Например, используя Apple HomeKit, можно управлять своими домашними аксессуарами с помощью приложения на устройствах iOS, таких как iPhone и Apple Watch. Это может быть специальное приложение в iOS, такое как Siri. В случае Lenovo это будет Smart HomeEssentials – линейка устройств для умного дома, которые управляются через приложение Apple Home или Siri (без необходимости использования Wi-Fi). Существуют специализированные концентраторы умного дома, которые предлагаются в качестве автономных платформ для подключения различных продуктов умного дома, в том числе Amazon Echo, Google Home, Apple HomePod и Samsung SmartThings Hub. Также существуют непатентованные системы с открытым исходным кодом, например, Domoticz, OpenHAB, Home Assistant.

4.1.2. Уход за пожилыми людьми

Одним из ключевых применений умного дома является оказание помощи людям с ограниченными возможностями и пожилым людям. Эти домашние системы используют вспомогательные технологии для удовлетворения особых потребностей владельца. Голосовое управление может помочь пользователям с ограничениями зрения и подвижности, а системы оповещения могут быть подключены непосредственно к кохлеарным имплантатам, которые носят пользователи с нарушениями слуха.

Примечание. Кохлеарные импланты представляют собой биомедицинские электронные устройства, обеспечивающие преобразование звука в электрические импульсы.

Они также могут быть оснащены дополнительными функциями безопасности. Эти функции могут включать датчики, которые отслеживают экстренные медицинские ситуации, такие как падения или судороги. Технология умного дома, применяемая таким образом, может предоставить пользователям больше свободы и более высокое качество жизни.

4.2. Инфраструктурное направление

Мониторинг и контроль функционирования устойчивой городской и сельской инфраструктуры, такой как мосты, железнодорожные пути, ветряные электростанции на суше и в море, является ключевым приложением IoT. Инфраструктура IoT может использоваться для мониторинга любых событий или изменений в структурных условиях, которые могут поставить под угрозу безопасность и увеличить риск. IoT может принести пользу строительной отрасли за счет экономии затрат, сокращения времени, повышения качества рабочего дня, безбумажного рабочего процесса и повышения производительности. Это может помочь в принятии более быстрых решений и сэкономить деньги благодаря анализу данных в режиме реального времени. Он также может быть использован для эффективного планирования работ по ремонту и техническому обслуживанию путем координации задач между различными поставщиками услуг и пользователями этих объектов. Устройства IoT также могут использоваться для управления критически важной инфраструктурой, такой как мосты, для обеспечения доступа к судам. Использование устройств IoT для мониторинга и эксплуатации инфраструктуры, улучшит управление инцидентами и координацию реагирования на чрезвычайные ситуации, а также качество обслуживания, время безотказной работы и снизит затраты на эксплуатацию во всех областях, связанных с инфраструктурой. Например, управление отходами, может дать выгоду из автоматизации и оптимизации, которые могут быть реализованы с помощью IoT.

4.2.1. Управление энергопотреблением

Значительное количество энергопотребляющих устройств (например, лампы, бытовая техника, двигатели, насосы и т.д.) уже интегрируют подключение к Интернету, что позволяет им взаимодействовать с коммунальными службами не только для балансировки выработки электроэнергии, но и помогает оптимизировать потребление энергии в целом. Эти устройства обеспечивают удаленное управление пользователями или централизованное управление через облачный интерфейс и позволяют выполнять такие функции, как планирование (например, удаленное включение или выключение систем отопления, управление духовками, изменение условий освещения и т.д.). Интеллектуальная сеть – это приложение IoT на стороне утилиты. Системы собирают и обрабатывают информацию, связанную с энергией и электроэнергией, для повышения эффективности производства и распределения электроэнергии. Используя устройства, подключенные к Интернету с помощью усовершенствованной измерительной инфраструктуры (AMI), предприятия электроэнергетики не только собирают данные от конечных пользователей, но и управляют устройствами автоматизации распределения, такими как трансформаторы.

4.2.2. Мониторинг окружающей среды

Приложения IoT для экологического мониторинга обычно используют датчики охраны окружающей среды путем мониторинга качества воздуха или воды, атмосферных или почвенных условий и могут даже включать такие области, как мониторинг перемещений диких животных и мест их обитания. Разработка устройств с ограниченными ресурсами, подключенных к Интернету, также означает, что другие приложения, такие как системы раннего предупреждения о землетрясениях или цунами, также могут

использоваться экстренными службами для оказания более эффективной помощи. Устройства IoT в этом приложении обычно охватывают большую географическую область и также могут быть мобильными. Утверждалось, что стандартизация, которую IoT привносит в беспроводное зондирование, произведет революцию в этой области.

4.2.3. Живая лаборатория

Другим примером интеграции IoT является «Живая лаборатория», которая объединяет исследовательские и инновационные процессы, создаваемые в рамках государственно-частного партнерства людей. В настоящее время существуют сотни живых лабораторий, которые используют IoT для сотрудничества и обмена знаниями между заинтересованными сторонами для совместного создания инновационных и технологических продуктов. Для внедрения и развития сервисов IoT в умных городах, у компаний должны быть стимулы. Ключевую роль в проектах "умных городов" играют правительства, поскольку изменения в политике помогут городам внедрить IoT, которые обеспечивают эффективность, результативность и точность используемых ресурсов. Например, правительство предоставляет налоговые льготы и дешевую арендную плату, улучшает общественный транспорт и предлагает среду, в которой компании, творческие объединения и транснациональные корпорации могут совместно создавать, использовать общую инфраструктуру и рынки труда, а также использовать преимущества местных технологий, производственных процессов, логистических и транзакционных издержек. Взаимоотношения между разработчиками технологий и правительствами, которые управляют активами городов, являются ключевыми для эффективного предоставления пользователям открытого доступа к ресурсам.

4.3. Промышленное направление

Промышленный IoT, также известный как IIoT, получает и анализирует данные от подключенного оборудования, операционных технологий (OT), местоположений и людей. IIoT в сочетании с устройствами мониторинга OT помогает регулировать и контролировать промышленные системы. Кроме того, такая же реализация может быть реализована для автоматического обновления записей о размещении активов в промышленных хранилищах, поскольку размер активов может варьироваться от небольшого винта до всей запасной части двигателя, и неправильное размещение таких активов может привести к потерям рабочего времени и денег.

4.3.1. Производство

IoT позволяет подключать различные производственные устройства, оснащенные функциями обнаружения, идентификации, обработки, связи, приведения в действие и создания сетей. Сетевой контроль и управление производственным оборудованием, управление активами и ситуациями или управление производственными процессами позволяют использовать IoT для промышленных приложений и интеллектуального производства. Интеллектуальные системы IoT позволяют быстро производить и оптимизировать новые продукты, а также быстро реагировать на потребности в продуктах.

Цифровые системы управления для автоматизации управления технологическими процессами, инструменты оператора и системы служебной информации для оптимизации безопасности и охраны оборудования входят в компетенцию IIoT. Так же можно применить IoT для управления активами с помощью прогнозного обслуживания, статистической оценки и измерений для обеспечения максимальной надежности. Промышленные системы управления могут быть интегрированы с интеллектуальными сетями, что позволяет оптимизировать энергопотребление. Измерения, автоматизированное управление, оптимизация установок, управление охраной труда и безопасностью и другие функции обеспечиваются сетевыми датчиками.

В дополнение к общему производству, IoT также используется для процессов индустриализации строительства.

4.3.2. Сельское хозяйство

Существует множество приложений IoT в сельском хозяйстве, таких как сбор данных о температуре, количестве осадков, влажности, скорости ветра, зараженности вредителями и составе почвы. Эти данные могут быть использованы для автоматизации методов ведения сельского хозяйства, принятия обоснованных решений по улучшению качества и количества, минимизации рисков и отходов, а также для сокращения усилий, необходимых для управления посевами. Например, фермеры теперь могут контролировать температуру и влажность почвы удаленно с помощью IoT, составлять точную программу внесения удобрений. Цель состоит в том, чтобы данные с датчиков в сочетании с интуицией и знаниями крестьян помогли снизить затраты и повысить производительность ферм.

В августе 2018 года компания Toyota Tsusho начала партнерство с Microsoft по созданию инструментов для рыбоводства с использованием пакета приложений Microsoft Azure для технологий IoT, связанных с управлением водными ресурсами. Так, например, разработанные исследователями механизмы

водяного насоса используют искусственный интеллект для подсчета количества рыбы на конвейерной ленте, анализа количества рыбы и определения эффективности потока воды.

4.3.3. Продовольствие

В последние годы широко изучалось использование приложений на основе IoT для улучшения деятельности в цепочке поставок продовольствия. Внедрение технологии RFID в цепочку поставок продуктов питания привело к видимости запасов и их перемещения в режиме реального времени, автоматизированному подтверждению доставки, повышению эффективности логистики продуктов с коротким сроком годности, мониторингу окружающей среды, животноводства и холодильной цепи, эффективной отслеживаемости. Исследователи на основе технологии IoT разработали инновационную систему отслеживания пищевых отходов, которая поддерживает принятие решений в режиме реального времени для борьбы с проблемами отходов в производстве продуктов питания и сокращения их количества. Они также разработали полностью автоматизированную систему, основанную на обработке изображений, для отслеживания отходов картофеля на фабрике по упаковке картофеля. В настоящее время IoT внедряется в пищевой промышленности для повышения безопасности пищевых продуктов, улучшения логистики, повышения прозрачности цепочки поставок и сокращения потерь.

4.4. Коммерческие направления

4.4.1. Медицина и здравоохранение

Устройства IoT можно использовать для обеспечения удаленного мониторинга и оповещения о состоянии здоровья в чрезвычайных ситуациях. Эти устройства мониторинга состояния здоровья могут варьироваться от мониторов артериального давления и сердечного ритма до современных устройств, способных контролировать специализированные имплантаты, такие как кардиостимуляторы, электронные браслеты, усовершенствованные слуховые аппараты. Внедряются "умные кровати", которые могут определять, когда они заняты и когда пациент пытается встать. Они даже могут автоматически настраиваться для обеспечения надлежащего давления и поддержки пациента без ручной помощи медсестер.

В жилых помещениях также могут быть установлены специализированные датчики для мониторинга здоровья и общего благополучия пожилых людей, для обеспечения надлежащего лечения и оказания помощи людям в восстановлении утраченной подвижности с помощью терапии. Для мониторинга пациента создают сеть интеллектуальных датчиков, которые способны собирать, обрабатывать, передавать и анализировать информацию в различных средах, например, таких как подключение домашних устройств мониторинга к больничным системам. Другие потребительские устройства для поощрения здорового образа жизни, такие как подключенные весы или носимые кардиомониторы, также доступны с IoT. Платформы IoT для комплексного мониторинга состояния здоровья также доступны для дородовых и хронических пациентов, помогая управлять жизненно важными показателями здоровья и повторяющимися потребностями в лекарствах.

Достижения в области методов изготовления электроники из пластика и ткани позволили создать сверхнизкие по стоимости, удобные в использовании датчики IoMT (интернета медицинских вещей). Эти датчики, наряду с необходимой электроникой RFID, могут быть изготовлены на бумаге или электронном текстиле для одноразовых сенсорных устройств с беспроводным питанием. Созданы приложения для диагностики на месте оказания медицинской помощи, где важна низкая сложность и мобильность системы.

IoMT в отрасли здравоохранения в настоящее время позволяет врачам, пациентам и другим лицам, таким как опекуны пациентов, медсестры, семьи и т.д., быть частью системы, в которой записи пациентов сохраняются в базе данных, позволяя врачам и остальному медицинскому персоналу иметь доступ к информации о пациентах. Кроме того, системы, основанные на IoMT, ориентированы на пациента, что предполагает гибкость в отношении медицинских условий пациента. В страховой отрасли IoT обеспечивает доступ к динамической информации, которая включает в себя решения на основе датчиков, такие как биосенсоры, носимые устройства, подключенные медицинские устройства и мобильные приложения для отслеживания поведения пациентов.

Применение IoT в здравоохранении играет фундаментальную роль в лечении хронических заболеваний, а также в профилактике заболеваний и борьбе с ними. Удаленный мониторинг становится возможным благодаря беспроводным подключениям, которые позволяют практикующим врачам дистанционно собирать данные о пациентах, применяя сложные алгоритмы анализа состояния их здоровья.

4.4.2. Транспорт

IoT может помочь в интеграции коммуникаций, управления и обработки информации в различных

транспортных системах. Применение IoT относится ко всем компонентам транспортной системы (инфраструктура, транспортное средство, водитель и пользователь). Динамическое взаимодействие между компонентами обеспечивает связь между транспортными средствами и внутри них, интеллектуальное управление движением, парковкой, взиманием платы, логистикой и автопарком, транспортными средствами, безопасностью, помощью на дорогах.

4.5. Военное направление

Интернет военных вещей (IoMT) – это применение технологий IoT в военной области дляцелей разведки, наблюдения и других целей, связанных с боевыми действиями. Это в значительной степени зависит от будущих перспектив ведения боевых действий в городской среде и предполагает использование датчиков, боеприпасов, транспортных средств, роботов, биометрических данных, пригодных для ношения человеком, и других интеллектуальных технологий, которые актуальны на поле боя.

4.5.1. IoT на поле боя

I o T на поле боя (IoBT) – это проект, инициированный и выполняемый Исследовательской лабораторией армии США (ARL), который фокусируется на фундаментальных науках,связанных с IoT, которые расширяют возможности солдат армии. В 2017 году ARL запустила Альянс совместных исследований IoT на поле боя (IoBT-CRA),устанавливающий рабочее сотрудничество между промышленностью, университетами и армейскими исследователями для продвижения теоретических основ технологий IoT и их применения в армейских операциях.

4.5.2. Океан вещей

Проект "Океан вещей" – это программа, возглавляемая Агентством перспективных исследовательских проектов Министерства обороны США DARPA (Defense AdvancedResearch Projects Agency), предназначенная для создания IoT на больших акваториях океана в целях сбора, мониторинга и анализа данных об окружающей среде и деятельности судов. Проект предусматривает развертывание около 50 000 поплавков, в которых размещен набор пассивных датчиков, которые автономно обнаруживают и отслеживают военные и коммерческие суда в рамках облачной сети.

4.6. Логистика

Существует несколько приложений умной или активной упаковки, в которых QR-код или NFC-метка прикрепляются к продукту или его упаковке. Сам тег является пассивным, однако он содержит уникальный идентификатор (обычно URL-адрес),который позволяет пользователю получать доступ к цифровому контенту о продукте с помощью смартфона. Строго говоря, такие пассивные предметы не являются частью IoT, но их можно рассматривать как средства, способствующие цифровому взаимодействию. Термин "Интернет упаковки" был придуман для описания приложений, в которых используются уникальные идентификаторы, для автоматизации цепочек поставок и масштабного сканирования потребителями для доступа к цифровому контенту. Аутентификация уникальных идентификаторов, и, следовательно, самого продукта, возможна с помощью чувствительного к копированию цифрового водяного знака или шаблона обнаружения копирования при сканировании QR-кода, в то время как метки NFC могут шифровать связь.

5. Тенденции и характеристики

Основной значимой тенденцией IoT в последние годы является взрывной рост устройств, подключенных и контролируемых интернетом. Широкий спектр приложений для IoT означает, что особенности могут сильно отличаться от одного устройства к другому, но есть основные характеристики, общие для большинства.

IoT создает возможности для более прямой интеграции физического мира в компьютерные системы, что приводит к повышению эффективности, экономическим выгодам и снижению нагрузки на человека.

5.1. Интеллект

Окружающий интеллект и автономное управление не являются частью первоначальной концепции IoT, и они не обязательно требуют интернет-структур. Однако в исследованиях (таких компаний, как Intel) наблюдается сдвиг в направлении интеграции концепций IoT и автономного управления. При этом первоначальные результаты в этом направлении рассматривают объекты как движущую силу автономного IoT. Перспективным подходом в этом контексте является глубокое обучение с подкреплением, в котором большинство систем IoT обеспечивают динамичную и интерактивную среду. Обучение агента (т.е. устройства IoT) разумному поведению в такой среде не может быть решено с помощью обычных алгоритмов машинного обучения, таких как обучение под наблюдением. С помощью подхода к обучению с подкреплением обучающийся агент может определять состояние окружающей среды (например,

определять температуру в доме), выполнять действия (например, включать или выключать кондиционер) и учиться за счет максимизации накопительной экономии, которая получается в долгосрочной перспективе.

Интеллект IoT может быть расположен на трех уровнях:

- устройства IoT,
- пограничные/туманные узлы, и
- облачные вычисления.

Необходимость интеллектуального управления и принятия решений на каждом уровне зависит от чувствительности приложения IoT ко времени. Например, камера автономного транспортного средства должна обнаруживать препятствия в режиме реального времени, чтобы избежать аварии. Такое быстрое принятие решений было бы невозможно за счет передачи данных с транспортного средства в облачные экземпляры и возврата прогнозов обратно в транспортное средство. Вместо этого все операции выполняются локально в автомобиле. Интеграция передовых алгоритмов машинного обучения, включая глубокое обучение, в устройства IoT – активная область исследований, направленная на то, чтобы сделать интеллектуальные объекты ближе к реальности. Более того, можно извлечь максимальную выгоду из развертывания IoT за счет анализа данных IoT, извлечения скрытой информации и прогнозирования решений по управлению. В области IoT используется широкий спектр методов машинного обучения:

- традиционные методы (такие как регрессия, метод опорных векторов и random forest), и
- продвинутые методы (такие как свёрточные нейронные сети, LSTM и вариационный автокодировщик).

Примечание. LSTM (Long Short-Term Memory) – нейронная сеть с длительной краткосрочной памятью.

В перспективе IoT может стать недетерминированной и открытой сетью, в которой автоматически организованные или интеллектуальные объекты (веб-службы, компоненты SOA, Service-Oriented Architecture) и виртуальные объекты (аватары) будут взаимодействовать и смогут работать (преследуя свои собственные или общие цели) в зависимости от контекста, обстоятельств или среды. Автономное поведение посредством сбора и анализа контекстной информации, а также способность объектов обнаруживать изменения в окружающей среде (неисправности, влияющие на датчики), вводить подходящие меры по смягчению последствий, представляет собой важную тенденцию, которая явно необходима для обеспечения доверия к IoT.

Современные продукты и решения IoT уже используют ряд технологий для поддержки контекстно-зависимой автоматизации. Однако требуется более сложный интеллект, позволяющий развертывать сенсорные устройства и интеллектуальные киберфизические системы в реальных средах.

6. Архитектура систем IoT

Архитектура системы IoT в упрощенном виде состоит из трех уровней:

- Уровень 1: устройства,
- Уровень 2: пограничные шлюзы, и
- Уровень 3: облака.

Первый (верхний) уровень устройств включают в себя оконечные датчики и актуаторы (исполнительные механизмы), используемые в оборудовании IoT, особенно те, которые работают по таким протоколам, как Modbus, Bluetooth, Zigbee, или по собственным (проприетарным) протоколам, для подключения к пограничному шлюзу.

Второй уровень пограничного шлюза состоит из систем агрегирования данных от датчиков, которые (пограничные шлюзы, или контроллеры), обеспечивают функциональность, такую как предварительная обработка данных, обеспечение подключения к облаку, использование таких систем, как WebSockets, концентратор событий, а в некоторых случаях, обеспечивают пограничную аналитику, или туманные вычисления (Fog Computing). Для облегчения управления уровень пограничных шлюзов необходим также для общего представления об устройствах верхнего уровня.

Третий облачный уровень включает приложение, создаваемое для системы IoT на основе архитектуры микросервисов, которые обычно являются многоязычными и по своей сути безопасными с использованием HTTPS / OAuth. Он включает в себя различные системыуправления базами данных, которые хранят данные от датчиков, такие как БД временных рядов или внутренние хранилища подсистем

управления БД (например, Cassandra, PostgreSQL). Этот уровень в большинстве облачных систем IoT включает систему организации очередей событий и обмена сообщениями, которая обрабатывает связи, происходящие между всеми тремя уровнями.

Некоторые эксперты различают в системе IoT три уровня: пограничный, платформенный и корпоративный, – которые связаны:

- сетью близости,
- сетью доступа, и
- сетью обслуживания, соответственно.

Сеть вещей, web of things – это архитектура прикладного уровня, ориентированная на конвергенцию данных с устройств IoT в веб-приложения для создания инновационных вариантов использования.

Для программирования и управления потоками информации в IoT используется архитектура, называемая BPM (Business Process Management) Everywhere. Она представляет собой сочетание традиционного управления процессами с интеллектуальным их анализом и специальными возможностями автоматизации при управлении большим количеством устройств.

7. Прогнозы и распространение технологии

В 2011 году общее количество устройств в мире, подключенных к сетям IoT превысило количество людей, имеющих подключение к интернету, и составило 4,6 млрд штук.

К концу 2021 года в мире уже насчитывалось 12,2 млрд находящихся в эксплуатации устройств IoT, что почти в 3 раза больше, чем 10 лет назад.

Наибольшую скорость развития IoT демонстрируют промышленность, транспорт и логистика, ЖКХ, «Умный дом», а также здравоохранение.

Прогнозируется глобальный рост общего объёма корпоративного и пользовательского рынка IoT. Основными сферами применения технологии IoT станут ЖКХ, промышленность, технологии «умной недвижимости». По прогнозам доходы глобального рынка промышленного IoT достигнут в 2025 году 500 млрд €, в 2030 году – 4 трлн €.

II. Архитектура и протоколы IoT

II.1. Архитектура IoT

Система IoT состоит из набора инфокоммуникационных технологий, которые обеспечивают её работу. Общая упрощенная архитектура IoT показана на рис.1.

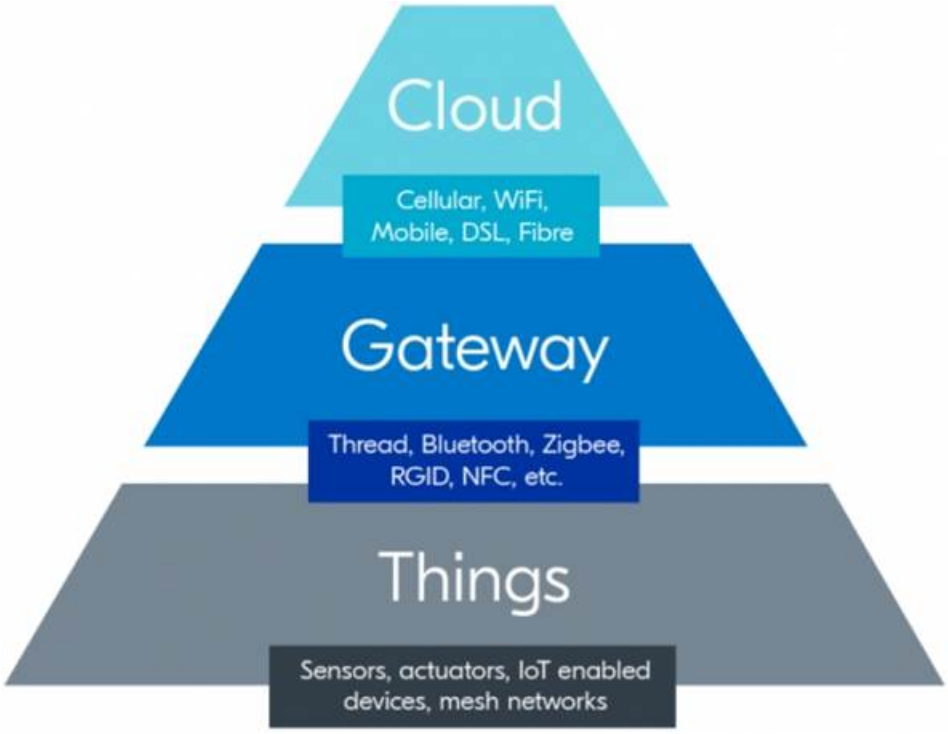

Рис.1. Общая архитектура IoT

Архитектура системы IoT показывает, как разные технологии связаны между собой.

IoT – концепция технологий Интернета для автоматизации, т.е. исключения участия человека из большинства рутинных процессов работы IT-инфраструктуры.

Технологии IoT связывают также с объединением интеллектуальных устройств в единую систему. Согласно рекомендации МСЭ-Т Y.2060, IoT обеспечивает коммуникацию между любыми «вещами», как виртуальными объектами, в режиме реального времени.

Как правило устройства IoT имеют соединение со шлюзами, подключаемыми к локальной или глобальной вычислительной сети. Есть и самодостаточные устройства, которые могут подключаться к сетям с помощью интерфейсов Ethernet, Wi-Fi, WiMAX, LTE и 5G.

Сами шлюзы являются концентраторами, поддерживающими определенный стандарт или протокол, обеспечивающий связь с IoT-"вещами".

В качестве примера IoT-системы без шлюза на рис.2 приведена схема работы GPS/GLONAS-трекера с модулем NB-IoT.

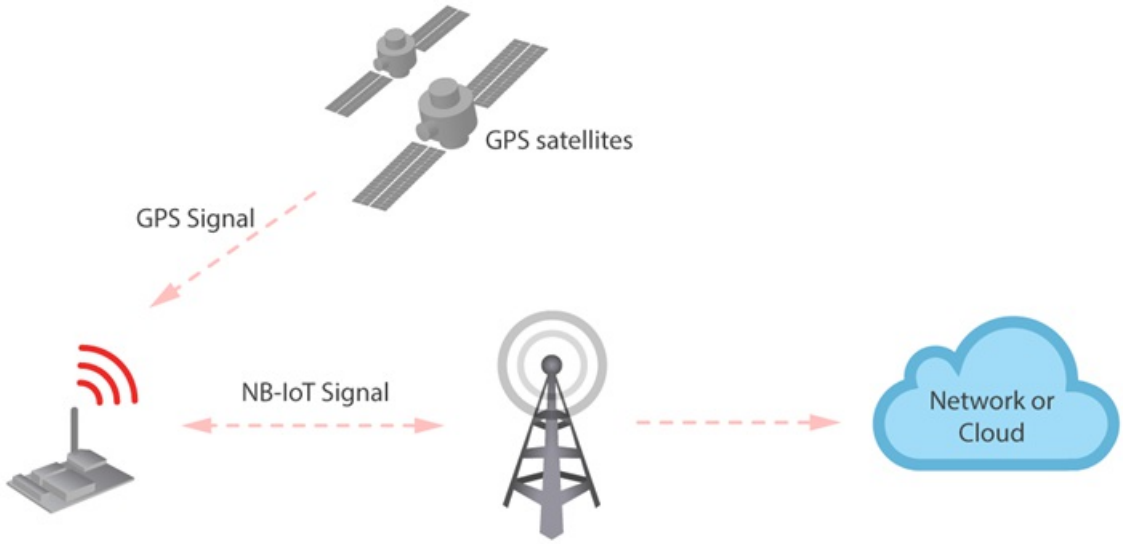

Рис.2. Схема IoT-системы без шлюза

Таким образом, есть устройства, которым не нужен шлюз, и они обладают стандартным интерфейсом связи. Они самодостаточны и для координации с облаком им хватает доступа в интернет через провод, GSM/3G/LTE, NB-IoT, Wi-Fi и т.д.

В примере с GPS/GLONAS-трекером на рис.2 оператор присваивает устройству IP-адрес (либо использует технологию без IP) и через NB-IoT (L1, L2) «выпускает» устройство в интернет. Сам трекер может поддерживать протоколы CoAP, MQTT и др. или просто отправлять свой payload в UDP-пакетах на указанный в настройках адрес приложения через публичную сеть.

Примечания: CoAP (Constrained Application Protocol) – протокол прикладного уровня для межмашинного взаимодействия M2M (Machine-to-Machine) устройств с ограниченными ресурсами, таких как микроконтроллеры и др.

MQTT (Message Queuing Telemetry Transport) – протокол передачи сообщений телеметрии с очередями.

Сенсоры, которые характеризуются низким энергопотреблением и низкой скоростью передачи данных, образуют беспроводную сенсорную сеть WSN (Wireless Sensor Network). Онаможет содержать множество датчиков с поддержкой работы от батарей и охватывать большие площади. Достигается это путем применения топологии mesh-сети.

В качестве примера можно привести стандарт ZigBee (IEEE 802.15.4), применяемый всистемах "Умный Дом".

II.2. Протоколы передачи данных IoT

Определение. Протоколы передачи данных IoT – это правила, определяющие способы обмена данными между объектами сети IoT.

При построении IoT-систем используются специальные протоколы передачи данных. Основные из этих протоколов следующие:

- CoAP (Constrained Application Protocol);
- AMQP (Advanced Message Queuing Protocol);
- MQTT (Message Queuing Telemetry Transport);
- XMPP (eXtensible Messaging and Presence Protocol);
- DDS (Data Distribution Service) – сервис распределения данных;
- JMS (Java Message Service) – сервис промежуточного ПО на Java для рассылки сообщений.

Также могут использоваться и другие, фирменные протоколы, а также стандартные протоколы интернета, например, HTTP.

Выбор протокола зависит от решаемой задачи. Протоколы IoT различаются между собой по принципам работы и сценариям использования.

При выборе протокола нужно ориентироваться на:

- количество устройств,
- потребление ресурсов,
- объем передаваемых данных, и
- расстояние, на которое нужно передавать данные.

Разработчики также используют собственные протоколы (фирменные, проприетарные). Однако использование стандартных протоколов на IoT-платформах значительно ускоряет внедрение и разработку новых систем и приложений Интернета вещей.

II.2.1. *Стандартные протоколы* IoT

К стандартным относятся протоколы MQTT, XMPP, AMQP и JMS.

В их основе лежит идея переноса ресурсозатратной части системы на элементы с бо́льшим количеством ресурсов.

При этом сообщения передаются не напрямую, а через специальный программный сервер, или брокер протоколов, иногда называемый шлюзом, который берёт на себя обработку сообщений.

Брокер протокола может быть развернут:

- в дата-центре на аппаратном сервере, или
- виртуально в облаке.

Из протоколов стандартного типа наиболее популярен MQTT, разработанный специально для IoT ещё в 1999 году.

MQTT не перегружает каналы связи и не требует постоянного и стабильного интернет-соединения. Он подходит для сред с очередями и высокой задержкой, поэтому годится для межмашинного обмена сообщениями (M2M).

В 2002 году была сформирована рабочая группа XMPP, для разработки протокола мгновенного обмена сообщениями на основе Jabber (Cisco).

Примечание. Протокол XMPP – расширяемый для (мгновенного) обмена сообщениями и информацией о присутствии на основе Jabber [ʤˈæbə(r] (джáббер, трёп, тарабарщина, болтовня) – открытый протокол обмена сообщениями и информацией о присутствии в режиме реального времени, основанный на XML. Помимотекстовых сообщений, поддерживает передачу по сети файлов, голоса и видео. Пример использования – IM WhatsApp.

Рабочая группа XMPP сформировалачетыре спецификации, которые были оформлены в качестве стандартов в 2004 году. Помимо XMPP, к ним относятся:

- MQTT,
- AMQP, и
- JMS.

Протокол MQTT используют в том числе с маломощными устройствами,т.к. он позволяет отправлять данные с минимальными затратами энергии.

Упрощённая схема работы MQTT показана на нижеследующем рис.3.

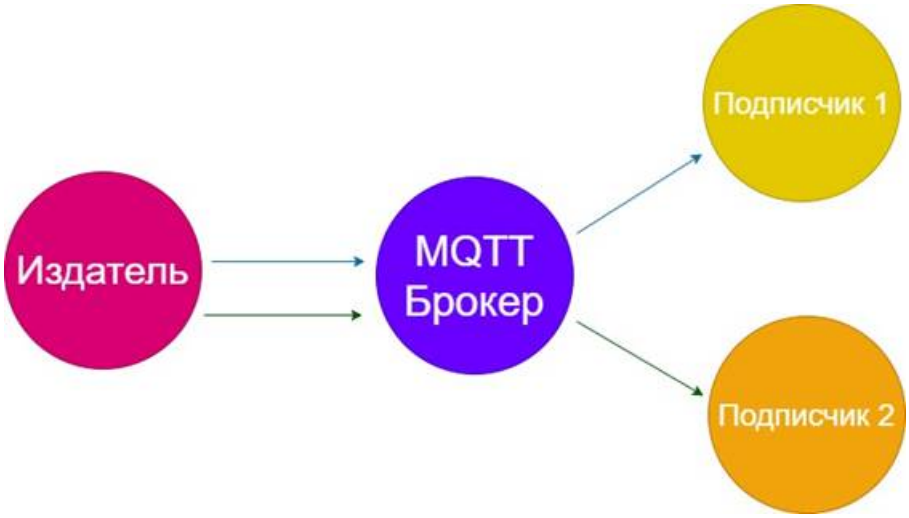

Рис.3. Схема работы протокола MQTT

MQTT Брокер (посредник) – это серверная часть протокола MQTT, выполняющаяклиент-серверные (C2S) и межсерверные коммуникации (S2S).

Семейство протоколов XMPP принято группой IETF как стандарты RFCs 6120, 6121, 7395, 7590, 7622. Типовой порт XMPP – 5222. При проблемах с файерволом также можно использовать порты 80 и/или 443.

Протокол AMQP

Протокол AMQP (Advanced Message Queuing Protocol) – это открытыйпротокол прикладного уровня для передачи сообщений между компонентами системы.

Его идея состоит в том, что отдельные подсистемы (или независимые приложения) могут обмениваться произвольным образом сообщениями через AMQP-брокер, который осуществляет маршрутизацию, возможно гарантирует доставку, распределение потоков данных, подписку на нужные типы сообщений.

Протокол JMS

Протокол JMS (Java Message Service) – стандарт промежуточного ПОдля рассылки сообщений, позволяющий приложениям, выполненным на платформе Java EE (Enterprise Edition), создавать, посылать, получать и читать сообщения.

Java EE – платформа, построенная на основе Java SE (StandardEdition), которая предоставляет API (Application Programming Interface)«программный интерфейс приложения» и среду выполнения для разработки и запуска крупномасштабных, многоуровневых, масштабируемых, безопасных и надежных

сетевых приложений.

II.2.2. *Специализированные протоколы* IoT

К специализированным протоколам относятся Modbus, CoAP, DDS.

Протокол Modbus

Данный протокол поддерживается производителями промышленного оборудования. Используется такой протокол для мониторинга, сбора данных с датчиков, управления контроллерами.

В сети одно устройство назначают ведущим, которое передает запросы другим, подчиненным устройствам. Modbus – открытый коммуникационный протокол, основанный на архитектуре ведущий – ведомый (master-slave; в стандарте Modbus используются термины client-server). Широко применяется в промышленности для организации связи между электронными устройствами. Может использоваться для передачи данных через последовательные линии связи RS-485, RS-422, RS-232 исети TCP/IP (Modbus TCP). Также существуют нестандартные реализации, использующие UDP.

Примечание. В облачной платформе IoT компании VK Cloud Solutions (бывшая MCS) реализована встроенная поддержка протоколов интернета вещей MQTT и Modbus. По запросу можно интегрировать в это облако также любые протоколы IoT, используемые заказчиком.

Протокол CoAP

Это аналог HTTP, но предназначен специально для IoT-оборудования. Принцип работы простой: он ориентирован на взаимодействие точка-точка (клиент-сервер). Клиент обращается к серверу и посылает ему простые команды, как это происходит и в HTTP. Схема взаимодействия по CoAP показана на рис.4:

Рис.4. Схема взаимодействия по CoAP

CoAP ориентирован на взаимодействие между точками клиент-сервер.

Когда нужна двусторонняя коммуникация с устройствами, подходят протоколы, позволяющие оборудованию обмениваться сообщениями в реальном времени. Одним из них является протокол DDS.

Протокол DDS

Протокол DDS (Data Distribution Service) – это службараспространения данных в системах реального времени и стандарт межмашинного взаимодействия.

Принцип его работы построен на обмене сообщениями напрямую, а не через специальный брокер-посредник, то есть не используя сервер.

https://nag.ru/material/38920

https://iotas.ru/files/documents/wg/T-REC-Y.2060-201206-I!!PDF-R.pdf

https://mcs.mail.ru/blog/protokoly-interneta-veschej

https://mcs.mail.ru/iot/

III. Технологии IoT

К числу технологий, определяющих облик современных сетей IoT, относят две основные:

- LoRaWAN (Long Range WAN большой дальности), и

- NB-IoT (Narrow Band – узкополосные).

Рассмотрим их подробнее.

III.1. Технология LoRaWAN

LoRaWAN (Long Range) – технология передачи данных для IoT большой дальности. Принцип её действия заключается в том, что в режиме онлайн smart-датчики осуществляют мониторинг показателей, анализируют их и передают на сервер. Данные от датчиков отображаются на мониторе через специальное приложение. При этом система способна самостоятельно оценивать сотни показателей.

Некоторые датчики могут работать автономно до 10 лет. Это актуально для объектов, где нет электричества, а также там, где оно может являться источником потенциальной опасности, например, возгорания. Отсутствие проводов делает процесс внедрения максимально простым и удобным.

Параметры LoRaWAN

За российским стандартом LoRaWAN закреплены и используются частоты в диапазоне 864-870МГц. Эти параметры подтверждены российскими членами LoRa Alliance.

Возможные варианты ширины канала, SF (Spreading Factor) фактора и скорости представлены ниже в таблице 1.

Таблица 1. Параметры каналов LoRaWAN

DataRate	Configuration	Indicative physical bit rate [bit/s]
0	LoRa: SF12 / 125 kHz	250
1	LoRa: SF11 / 125 kHz	440
2	LoRa: SF10 / 125 kHz	980
3	LoRa: SF9 / 125 kHz	1760
4	LoRa: SF8 / 125 kHz	3125
5	LoRa: SF7 / 125 kHz	5470
6	LoRa: SF7 / 250 kHz	11000
7	FSK: 50 kbps	50000

Из таблицы 1 видно, что LoRaWAN может использовать каналы различной ширины от 125 кГц до 250 кГц и даже 0,5 МГц, хотя в наших реалиях это большая роскошь. Ширина меньше 125 кГц спецификацией не предусмотрена, но схемотехнически чип реализовать её тоже может. Однако в России прижились каналы шириной 125 кГц. Причём Минсвязь разрешает работать только в двух поддиапазонах, указанных в табл.2.

В стандарте SF – это целое число от 12 до 7. Чем больше SF, тем выше помехозащищенность, но тем ниже скорость, и тем больше времени в эфире будет занимать передача. Для примера, максимальная помехозащищенность достигается при SF=12. При этом время пакета в эфире составляет 2,466 с, а скорость – 292 бит/с (индикативно считается, что скорость 250 бит/с).

Вид модуляции FSK (Frequency Shift Keying) – частотная фазовая манипуляция радиосигналов в эфире.

Таблица 2. Разрешённые поддиапазоны и ограничения LoRaWAN

Диапазон частот	Максимальная мощность	Время нахождения в эфире
864 - 865	25 мВт	0,1 % или LBT (listen before talk)
868.7 – 869.2	25 мВт	Нет ограничений

На практике нужно обращать внимание, что 25 мВт — это не мощность передатчика, а ЭИИМ — эффективная изотропно-излучаемая мощность, т.е мощность передатчика, минус потери в кабеле и разъемах, плюс коэффициент усиления антенны. Формально, при хорошей антенне, можно немного превысить допустимый уровень. По факту, замеры на месте на таких мощностях дают слишком большую погрешность, а расчеты могут не отразить всей картины. Поэтому обычно считают, что кабель и разъемы компенсируются антенной. И в результате отправной точкой будет мощность передатчика и два поддиапазона — 1 МГц и 0,5 МГц. Туда поместятся 7 каналов по 125 кГц, т. к. между ними еще должен быть зазор, или защитный интервал, шириной 75 кГц (согласно рекомендаций Semtech).

***Работа* LoRaWAN**

Итак, базовая станция-шлюз LoRaWAN «слушает» эфир на частотах датчиков. Когда от какого-то сенсора она «слышит» сигнал, то отправляет его на сервер. При этом шлюз не обрабатывает информацию – он служит «посредником» между датчиками и сервером.

Сервер необходим для передачи данных, управлением устройств, которые подключены к датчикам. Если датчик сработал, когда концентрация пыли в воздухе возросла или изменилась влажность в помещении, сервер отправит приказ включить вытяжку или запустит отопление.

В технологии есть еще одно звено – серверы приложений, компьютеры, планшеты, смартфоны и ноутбуки. Они переводят информацию с датчиков в цифры, графические схемы, текстовые сообщения.

LoRaWAN *подходит для:*

- *подключения «умного» дома, офиса, магазина, производства;*
- *потребляет при этом меньше энергии.*

Сети Wi-Fi и 4G дороже эксплуатировать, так как они потребляют больше энергии. Беспроводные каналы LoRa рассчитаны на передачу большого объема данных, например, фото или видео, требуют меньше энергии, так как с датчиков поступает небольшой объем данных. Также датчики передают сообщения по сети не постоянно, а только если сработало какое-то условие.

Например, для ЖКХ условие сработает, если многоквартирный дом потребит воды больше суточной нормы. Датчик в подвале дома зафиксирует это событие и передаст на компьютер сотрудника ЖКХ. Такая передача может произойти не чаще, чем раз в сутки. Это очень небольшой объем информации, и мощные беспроводные сети для этого не к чему.

- *Подключает большее количество устройств.*

Количество устройств, которые можно подключать к LoRaWAN, достегает несколько десятков тысяч. Ни одна другая сеть не выдержит такого количества подключений без потери скорости передачи данных.

- *Продлевает срок жизни батарей.*

Чтобы датчики работали, их необходимо подключить к источнику питания. Если «умные» электросчетчики можно подключить к электросети, то к счетчику воды кабель не протянешь. В таких ситуациях питание происходит от батарейки или аккумулятора.

III.2. Технология NB-IoT

NB-IoT(Narrow Band Internet of Things) — стандарт сотовой связи для устройствтелеметрии с небольшими объёмами обмена данными.

Предназначен для подключения к цифровым сетям связи широкого спектра автономных устройств.

Например, медицинских датчиков, счетчиков потребления ресурсов, устройств умного дома и т.п. NB-IoT является одним из трех стандартов IoT, разработанных 3GPP для сотовых сетей связи: eMTC (enhanced Machine-Type Communication), NB-IoT иEC-GSM-IoT. eMTC обладает наибольшей пропускной способностью и разворачивается на оборудовании LTE. NB-IoT сеть может быть развернута как на оборудовании сотовых сетей LTE, так и отдельно, в том числе поверх GSM. EC-GSM-IoTпредоставляет наименьшую пропускную способность и разворачивается поверх сетей стандарта GSM.

Достоинства стандарта NB-IoT:

- гибкое управление энергопотреблением устройств (вплоть до 10 лет в сети от батареи емкостью 5 Вт*ч);
- огромная емкость сети (десятки-сотни тысяч подключенных устройств на одну базовую станцию);
- низкая стоимость устройств.

Разработан NB-IoT консорциумом 3GPP в рамках работ над стандартами сотовых сетей нового поколения. Первая рабочая версия спецификации была представлена в июне 2016 года.

Обзор решений NB-IoT и их параметры представлены в табл.

	LTE Cat 1	LTE Cat 0	LTE Cat M1 (eMTC)	LTE Cat NB1 (NB-IoT)	EC-GSM-IoT
3GPP Release	Release 8	Release 12	Release 13	Release 13	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s	474 kbit/s (EDGE), 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s (multi-tone), 20 kbit/s (single-tone)	474 kbit/s (EDGE), 2 Mbit/s (EGPRS2B)
Latency	50-100 ms	not deployed	10-15 ms	1.6-10 s	700 ms - 2 s
Number of Antennas	2	1	1	1	1-2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex
Device Receive Bandwidth	1.4 — 20 MHz	1.4 — 20 MHz	1.4 MHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)	1 (SISO)	1-2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	23 / 33 dBm

SIM карта

Поскольку прогнозируется массовое распространение устройств IoT с возможностью мобильной связи, то вопросы себестоимости и затрат на обслуживание становятся критически важными. Один из путей экономии — отказ от установки физической SIM-карты. Для этого консорциум GSMA в 2016 году принял спецификацию Embedded SIM (eSIM) /Remote SIM Provisioning (RSP). Стандарт eSIM позволяет интегрировать функциональность SIM карты в электронику модема, а RSP описывает инфраструктуруи алгоритмы взаимодействия доверенных центров эмиссии параметров SIM, оператора сотовой связи и потребителя услуг связи.

Внедрение NB-IoT

Первые тестовые сети NB-IoT были развернуты в Европе компанией Vodafone в 2015 году. Микросхемы сделал Huawei, модемы разработал u-Blox. Коммерческую эксплуатацию технологии Vodafone начал в 2017 году.

В декабре 2017 года в России принято решение ГКРЧ по выделению частот для систем NB-IoT Комиссия разрешила использование полос радиочастот 453-457,4 МГц и 463-467,4 МГц, 791-820 МГц, 832-

862 МГц, 880-890 МГц, 890-915 МГц, 925-935 МГц, 935-960МГц, 1710-1785 МГц, 1805-1880 МГц, 1920-980 МГц, 2110-2170 МГц, 2500-2570 МГц и 2620-2690 МГц.

III.3. Российский стандарт NB-Fi

Отечественный стандарт IoT NB-Fi утвержден Приказом Федерального агентства по техническому регулированию и метрологии (Росстандарта) как национальный ГОСТ Р 70036-2022 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)» по итогам трёхлетней апробации вступил в силу 1 апреля 2022 г.

Разработка стандарта NB-Fi началась в 2017 году. Инициатива создания национального стандарта принадлежит Ассоциации интернета вещей. Подготовку и публикацию NB-Fiвыполнил технический комитет 194 «Кибер-физические системы», созданный на базе РВК.

В основе стандарта NB-Fi так же как и в NBIoT, лежит использование узкополосных (Narrow Band) фазоманипулированных сигналов, которые в сочетании с помехоустойчивым кодированием позволяют достигать очень высокой чувствительности приема (до -150 дБм). При этом суммарная полоса частот для одновременного размещения большого количества каналов является достаточно узкой. Это позволяет обеспечивать связь с устройствами на очень больших расстояниях от 10 км в городе до 50 км в прямой видимости при скорости передачи от 0.3 кбит/с до 50 кбит/с на канал шириной 100 кГц.

В России NB-Fi разрешён для свободного и бесплатного использования при реализации передачи на частоте 868 МГц и ограничении мощности до 25 мВт для оконечных устройств.

Сеть NB-Fi использует топологию «звезда», где каждое устройство взаимодействует с базовой станцией напрямую.

Устройство или модем с NB-Fi модулем передает данные по радиоканалу на базовую станцию. Базовая станция принимает сигналы от всех устройств в радиусе своего действия, оцифровывает и передаёт на удалённый сервер, используя доступный канал связи (Ethernet или сотовая связь).

Для приема восходящих (Uplink) пакетов данных со стороны базовой станции применяется принцип SDR-системы (Software DefinedRadio, программно-определяемой радиосистемы), которая оцифровывает входной радиосигнал во всей полосе частот, подвергая его программной обработке.

Данный подход позволяет выполнять демодуляцию и декодирование входных пакетов одновременно по всем каналам. По сути, в данной системе не существует сетки каналов, а пакеты данных принимаются базовой станцией вне зависимости от частоты, на которой выполнена отправка. Это является ключевым свойством стандарта, позволяющим использовать недорогие генераторы частоты для формирования радиосигнала, что ранее было ограничивающим фактором при использовании узкополосных сигналов.

Ввиду применения простых видов модуляции Uplink-пакеты могут быть сформированы практически при помощи любого серийного интегрального радиотрансивера. Прием Uplink-пакетов возможен только базовой станцией. В этой связи для реализации передачи пакетов данных в обратном, нисходящем (Downlink) направлении, применяются виды модуляции и скорости передачи, поддерживаемые конкретным радиотрансивером, который используется в конечных устройствах.

Сети NB-Fi могут функционировать в любой части нелицензируемого диапазона промышленных, научных и медицинских частот (ISM).

По своим характеристикам протокол NB-Fi наиболее сопоставим с протоколом SigFox, чем с широко используемым протоколом LoRa, и кардинально отличается от протокола NB-IoT.

Примечание. SigFox – технология беспроводной низкоскоростной связи устройств в сетях с низким потреблением энергии. Изобретена в 2009 году французской компанией SigFox. Использует ультра-узкую полосу частот (Ultra- Narrow Band, UNB) с двоично-фазовой манипуляцией (BPSK), для кодирования данных меняет фазу несущей радиоволны. В РФ не используется.

Криптографический анализ предварительного стандарта ПНСТ 354-2019 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)» выявил уязвимости протокола NB-Fi. В новойверсии протокола эти уязвимости были устранены.

Реализация стандарта NB-Fi

По состоянию на февраль 2019 года, была доступна единственная реализация NB-Fi, выполненная компанией «ВАВИОТ» на микроконтроллере семейства STM32(производитель: STMicroelectronics) с радиотрансивером AX5043 (производитель: ON Semiconductor).

IV. Программирование IoT

Настройка, установка и проверка брокера и клиента Mosquitto

IV.1. Брокер и клиентская библиотека Mosquitto

Брокер-клиент Mosquitto – это специальное прикладное программное обеспечение (ПО), реализующее технологию MQTT.

Eclipse Mosquitto — брокер сообщений с открытым исходным кодом (лицензии EPL/EDL), который реализует протоколы MQTT версий 5.0, 3.1.1 и 3.1. Mosquitto подходит для использования на всех устройствах: от маломощных одноплатных компьютеров до полноценных серверов.

MQTT.js – это клиентская библиотека для протокола MQTT, написанная на языке JavaScript для Node.js и браузера.

Пример отправки сообщения с помощью MQTT.js:

```
var mqtt = require('mqtt')
var client  = mqtt.connect('mqtt://test.mosquitto.org')
client.on('connect', function () {
  client.subscribe('presence', function (err) {
    if (!err) {
      client.publish('presence', 'Hello mqtt')
    }
  })
})
client.on('message', function (topic, message) {
  // message is Buffer
  console.log(message.toString())
  client.end()
})
```

IV.2. Установка и настройка брокера и клиента Mosquitto

Сетевая библиотека MQTTnet

MQTTnet — это высокопроизводительная библиотека .NET, которая предоставляет и клиент, и сервер MQTT (брокер).

Установка клиента MQTT Mosquitto:

```
// Create a new MQTT client.
var factory = new MqttFactory();
var mqttClient = factory.CreateMqttClient();
```

После настройки параметров клиента MQTT можно установить соединение.

Подключение клиента к серверу:

```
// Use WebSocket connection.
var options = new MqttClientOptionsBuilder()
    .WithWebSocketServer("broker.hivemq.com:8000/mqtt")
    .Build();

await client.ConnectAsync(options);
```

Приём входящих сообщений:

```
client.UseApplicationMessageReceivedHandler(e =>
{
    Console.WriteLine("### RECEIVED APPLICATION MESSAGE ###");
    Console.WriteLine($"+ Topic = {e.ApplicationMessage.Topic}");
    Console.WriteLine($"+ Payload = {Encoding.UTF8.GetString(e.ApplicationMessage.Payload)}");
    Console.WriteLine($"+ QoS = {e.ApplicationMessage.QualityOfServiceLevel}");
    Console.WriteLine($"+ Retain = {e.ApplicationMessage.Retain}");
    Console.WriteLine();
    Task.Run(() => client.PublishAsync("hello/world"));
});
```

Публикация сообщения:

```
var message = new MqttApplicationMessageBuilder()
    .WithTopic("MyTopic")
    .WithPayload("Hello World")
    .WithExactlyOnceQoS()
    .WithRetainFlag()
    .Build();
await client.PublishAsync(message);
```

Больше примеров можно найти в документации и на wiki:

https://github.com/dotnet/MQTTnet/wiki/Client