Д.А. Давронбеков, У.Т. Алиев

БЕСПРОВОДНЫЕ СИСТЕМЫ IoT

МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ
РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Д.А. Давронбеков, У.Т. Алиев

БЕСПРОВОДНЫЕ СИСТЕМЫ IoT

Учебник для бакалавров по направлению образования 5350100 –
Телекоммуникационные технологии (Мобильные системы)

ТАШКЕНТ
"METODIST NASHRIYOTI"
2024

УДК: 004.7(075)
ББК: 32.973я7
Д 14

Д.А. Давронбеков

Беспроводные системы IoT / У.Т. Алиев /. Учебник. – Ташкент: "METODIST NASHRIYOTI", 2024. - 276 с.

В учебнике изложены принципы организации интернета вещей (IoT), современное состояние и перспективы развития, термины и понятия; базовые принципы IoT, стандарты и протоколы передачи данных в IoT; архитектура IoT, способы взаимодействия с интернет-вещами; взаимодействие IoT с перспективными инфокоммуникационными технологиями, IoT и технологии 5G; интернет вещей и беспроводные сенсорные сети; архитектура беспроводных сенсорных сетей, системы M2M, RFID

Учебник предназначается для студентов, изучающих одноименный курс, а также может быть полезен для инженерно-технических специалистов в области телекоммуникаций (мобильных систем).

Рецензенты

А.А.Ярмухамедов - к.т.н., доцент заведующий кафедрой «Радиоэлектронные устройства и системы», Ташкентский Государственный имени И. Каримова технический университет

А.Н. Пузий - PhD, доцент кафедры «Системы телерадиовещания», Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Рекомендовано для прозы по заказу Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми. (Приказ № 439 от 25.04.2023 г., квитанция № 203-004)

ISBN 978-9910-03-108-3

ВВЕДЕНИЕ

В настоящее время бурными темпами развиваются сети передачи данных различного типа и назначения. Широкое развитие получает интернет вещей, который представляет собой сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные извне. Интернет вещей (Internet of Things, IoT) получает широкое распространение во многих странах мира, в том числе в Республике Узбекистан.

Узбекистан, следуя мировым тенденциям развития, взял курс на строительство и реализацию проектов «Умный город» на основе технологий Интернета вещей в несколько этапов. В 2017 году Президент Республики Узбекистана Шавкат Мирзиёев утвердил программу мер по реализации проекта «Безопасный город» на 2017-2023 гг., охватывающего весь Узбекистан.

В соответствии с Постановлением Кабинета Министров Республики Узбекистан №48 от 18 января 2019 года утверждены Концепция внедрения технологий «Умный город» в Республике Узбекистан и план практических мер по ее реализации на 2019-2030 гг., который будет реализовываться в четыре этапа [1].

Первый этап (2019-2021 гг.) – определение базовых подходов строительства «умного» города – включает в себя: формирование профиля территории; оценка существующей инфраструктуры; определение индикаторов развития; анализ доступных активов, существующих вызовов и историй успеха.

Второй этап (2022-2024 гг.) – разработка стратегии внедрения концепции «умного» города: вовлечение заинтересованных сторон; определение направлений мероприятий и планов; оценка рисков; формирование финансовой стратегии; определение ключевых показателей эффективности и целей.

Третий этап (2025-2027 гг.) – детализированное планирование строительства: бюджетирование; прогноз эффективности; определение возможностей автоматизации и внедрения информационных систем.

Четвертый этап (2028-2030 гг.) – внедрение и оценка эффективности: совместное (со всеми заинтересованными сторонами) внедрение; мониторинг эффективности; оценка и переоценка (анализ трендов, инвестиционных параметров), обеспечение развертывания (экспансии).

Для развития и применения IoT используется широкий спектр радиотехнологий и соответствующих им полос радиочастот. В зависимости от предоставления услуг IoT эти технологии и полосы радиочастот могут существенно различаться. Технологии могут варьироваться от унифицированных на международном уровне устройств малого радиуса действия до стандартов систем мобильной связи, нацеленных на более специфические задачи [2].

Данный учебник позволяет самостоятельно изучить современное состояние и перспективы развития интернета вещей, который находит всё большое применение во всём мире.

Авторы выражают признательность к.т.н., доценту Р.Р. Ибраимову, к.т.н., доценту Ш.У. Пулатову, PhD Х.Х. Мадаминову, д.т.н., профессору Ю.В. Писецкому за оказанную методическую помощь в написании данного учебника. Также выражаем благодарность рецензентам PhD, доценту А.Н. Пузий и к.т.н., доценту А.А. Ярмухаммедову.

Глава 1. ПРИНЦИПЫ ОРГАНИЗАЦИИ И РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ

1.1. Концепция и принципы организации Интернета вещей

Идея Интернета вещей сама по себе очень проста. Представим, что все окружающие нас предметы и устройства (домашние приборы и утварь, одежда, продукты, автомобили, промышленное оборудование и др.) снабжены миниатюрными идентификационными и сенсорными (чувствительными) устройствами. Тогда при наличии необходимых каналов связи с ними можно не только отслеживать эти объекты и их параметры в пространстве и во времени, но и управлять ими, а также включать информацию о них в общую «умную планету». В самом общем виде с инфокоммуникационной точки зрения Интернет вещей можно записать в виде следующей символической формулы:

IoT = Сенсоры (датчики) + Данные + Сети + Услуги

Интернет вещей - это глобальная сеть компьютеров, датчиков (сенсоров) и исполнительных устройств (актуаторов), связывающихся между собой с использованием интернет протокола IP (Internet Protocol). Например, для решения определенной задачи компьютер связывается через публичный интернет с небольшим устройством, к которому подключен соответствующий датчик (например, температуры), как это показано на рис.1.1 [3].

Различные типы устройств образовывают различные типы сетей, которые взаимодействуют с различными приложениями через Интернет (рис.1.2). Эти приложения могут иметь несколько интерфейсов. Сети устройств соединяются с Интернетом, а затем взаимодействуют с приложениями через транзитную сеть. Это транзитная сеть является основой коммуникации Интернет-инфраструктуры.

Очевидно, что при внедрении Интернета вещей вся наша повседневная жизнь кардинально изменится. Уйдут в прошлое поиски нужных вещей, дефициты товаров или их перепроизводство, кражи автомобилей и мобильных телефонов,

поскольку будет точно известно, что, в каком месте и в каком количестве находится, производится и потребляется. Если все объекты (вещи) будут снабжены миниатюрными радиометками, то их можно будет дистанционно идентифицировать, а при наличии определенного «интеллекта» - и управлять ими [3].

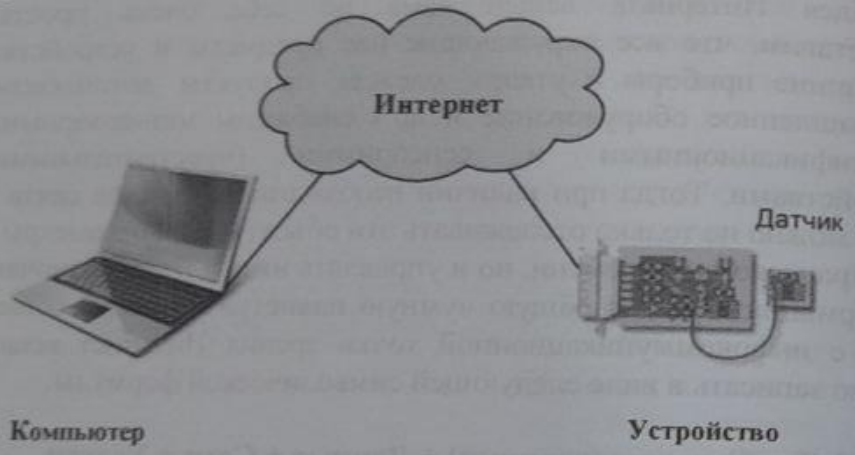


Рис. 1.1. Интернет-соединение компьютера и устройства, подключенного к датчику

Рис.1.2. Принципы организации связей в сети вещей

Концепция IoT играет определяющую роль в дальнейшем

развитии инфокоммуникационной отрасли. Это подтверждается как позицией Международного союза электросвязи (МСЭ) и Европейского Союза в данном вопросе, так и включением Интернета вещей в перечень прорывных технологий в США, Китае и других странах. И хотя на международном уровне данная концепция уже обретает черты сформировавшейся технологии, для нее ведутся активные работы в области стандартизации архитектуры, технических компонентов, приложений, но одновременно столь же велико количество мнений о том, как именно будет построен Интернет вещей [4].

В связи с бурным развитием сетей с пакетной коммутацией и прежде всего Интернета в начале 2000-х годов мировое телекоммуникационное сообщество сначала выработало, а затем и приступило к реализации новой парадигмы развития коммуникаций - сетей следующего поколения NGN (Next Generation Networks). Технологии NGN уже прошли эволюционный путь развития от гибких коммутаторов (Softswitch) до подсистем мультимедийной связи IMS (IP Multimedia Subsystem) и беспроводных сетей долговременной эволюции LTE (Long Term Evolution). При этом всегда предполагалось, что основными пользователями сетей NGN будут люди и, следовательно, максимальное число абонентов в таких сетях всегда будет ограничено численностью населения планеты Земля.

Однако в последнее время значительное развитие получили методы радиочастотной идентификации RFID (Radio Frequency IDentification), беспроводные сенсорные сети БСС (Wireless Sensor Network), коммуникации малого радиуса действия NFC (Near Field Communication) и межмашинные коммуникации M2M (Machine-to-Machine), которые, интегрируясь с интернет, позволяют обеспечить простую связь различных технических устройств («вещей»), число которых может быть огромным [6].

Рынок Интернета вещей продолжает расти. Ожидается, что к 2025 году будет более 30 миллиардов подключений к Интернету вещей (рис. 1.3) [5].

В общем случае под Интернетом вещей понимается совокупность разнообразных приборов, датчиков, устройств, объединённых в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия

между собой и единственный протокол доступа к глобальной сети. В роли глобальной сети для Интернет-вещей в настоящий момент используется сеть Интернет. Общим протоколом является IP.

Следует особо отметить, что Интернет вещей не исключает участие человека. IoT не полностью автоматизирует вещи, так как он ориентирован на человека и предоставляет ему возможность доступа к вещам. Но многие вещи смогут вести себя иначе, чем мы представляем себе сегодня. В IoT каждая вещь имеет свой уникальный идентификатор, которые совместно образуют континуум вещей, способных взаимодействовать друг с другом, создавая временные или постоянные сети.

Рис. 1.3. Временная шкала изменения количества людей и предметов, подключенных к интернет

Так вещи могут принимать участие в процессе их перемещения, делясь сведениями о текущей геопозиции, что позволяет полностью автоматизировать процесс логистики, а имея встроенный интеллект, вещи могут менять свои свойства и адаптироваться к окружающей среде, в том числе для уменьшения энергопотребления. Они могут обнаруживать другие, так или иначе связанные с ними вещи, и налаживать с ними взаимодействие. IoT позволяет создавать комбинацию из интеллектуальных устройств, объединенных сетями связи, и людей. Совместно они могут создавать самые разнообразные системы, например, для работы в средах, неудобных или недоступных для человека (в космосе, на большой глубине, на

ядерных установках, в трубопроводах и т.п.).

Считается, что первую в мире интернет-вещь создал один из отцов протокола TCP/IP Джон Ромки в 1990 году, когда он подключил к сети свой тостер [3]. Но только в 21 веке в связи с бурным развитием инфокоммуникационных технологий сформировалась концепция IoT и получила свое практическое воплощение. Процесс развития Интернета вещей проиллюстрирован технологической дорожной картой, приведенной на рис.1.4. Все началось с необходимости оптимизации системы логистики и управления системой снабжения предприятий. Вторая волна инноваций была обусловлена необходимостью сокращения затрат в системах наблюдения, безопасности, транспорта и др.

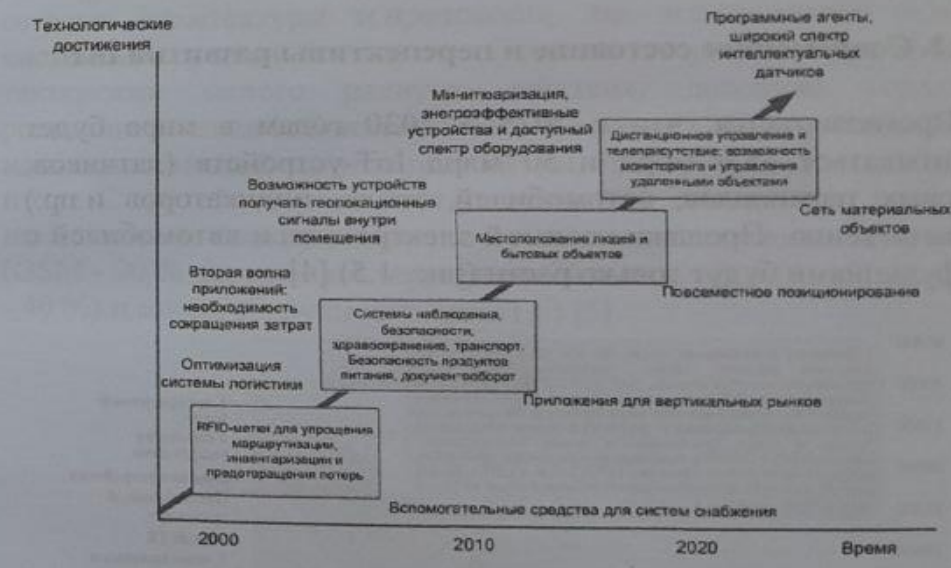


Рис. 1.4. Технологическая дорожная карта Интернета вещей

Третья была вызвана потребностью в геолокационных сервисах. Четвертая волна будет обусловлена необходимостью дистанционного присутствия человека на месте совершения требующего его внимания событий, которое станет возможным благодаря миниатюрным встроенным процессорам. А следующим

шагом будет возможность создания будущих сетей (Future Networks) с ячеистой топологией, включающих в себя метки, датчики, средства измерения и управляющие устройства [3].

С развитием Интернета вещей все больше предметов будут подключаться к глобальной сети, тем самым создавая новые возможности в сфере безопасности, аналитики и управления, открывая все новые и более широкие перспективы и способствуя повышению качества жизни населения.

Предполагается, что в будущем «вещи» станут активными участниками бизнеса, информационных и социальных процессов, где они смогут взаимодействовать и общаться между собой, обмениваясь информацией об окружающей среде, реагируя и влияя на процессы, происходящие в окружающем мире, без вмешательства человека.

1.2. Современное состояние и перспективы развития IoT

Прогнозируется, что к 2025 и 2030 годам в мире будет насчитываться 38,6 млрд и 50 млрд IoT-устройств (датчиков, торговых терминалов, автомобилей, табло, индикаторов и пр.) соответственно. Продажи носимой электроники и автомобилей с IoT-функциями будут только расти (рис. 1.5) [4].

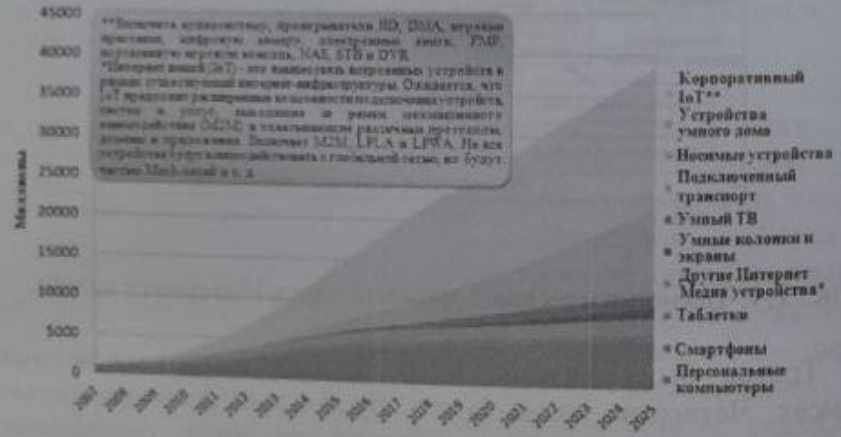


Рис. 1.5. Количество подключенных устройств в 2007-2025 гг.

Стремительный рост подключенных устройств в сегменте IoT и различные сценарии их использования диктуют определенные требования к сетевым технологиям - скорости передачи данных, задержки, надежность и пр. Эти параметры определяются особенностями конкретного применения, однако есть ряд общих целевых показателей, которые требуют внедрения инновационных сетевых технологий, предназначенных для IoT. К основным таким показателям, в частности, относятся:

- стоимость реализации сетевой технологии в конечном устройстве;
- энергопотребление и время автономной работы;
- покрытие сети.

Разработки последних лет в сфере беспроводной передачи данных связаны как со стремлением адаптировать имеющиеся сетевые архитектуры и протоколы, так и с созданием новых системных решений с нуля. С одной стороны, существуют технологии малого радиуса действия, довольно успешно решающие задачи IoT-коммуникаций в рамках одного помещения или ограниченной территории - Wi-Fi, Bluetooth, Z-Wave, Zigbee и т. д. С другой стороны, есть мобильные технологии, которые находятся вне конкуренции с точки зрения обеспечения покрытия (GSM - 90 % населенной территории Земли, WCDMA - 65 %, LTE - 40 %) и масштабируемости (рис.1.6) [5].

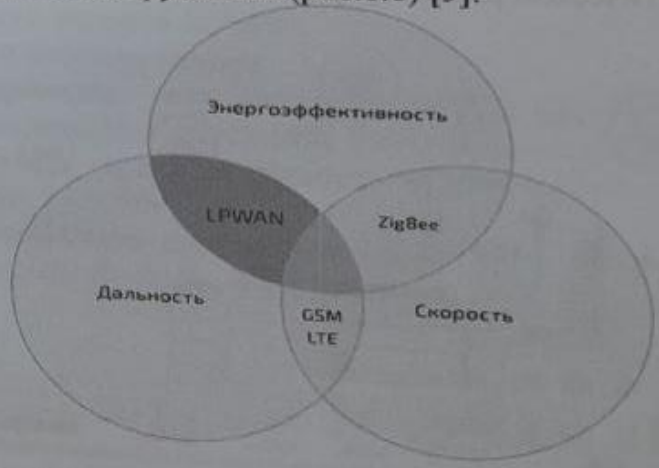


Рис.1.6. Сравнения технологий LPWAN, Zigbee , GSM/LTE по показателям

Однако основным недостатком как технологий малого радиуса действия, так и традиционных технологий мобильной связи является ограниченное время работы устройств от аккумулятора. Кроме того, технологии мобильной связи достаточно дороги в использовании, а Wi-Fi, Zigbee и другие технологии малого радиуса действия не обеспечивают достаточного сетевого покрытия и плохо управляемы.

Шаги, предпринятые в рамках развития стандартов мобильной связи, в частности спецификации 3GPP Release 15, направлены, в том числе, на достижение целевых показателей для IoT при сохранении преимуществ использования глобальной экосистемы. Предполагается, что эволюция этих технологий станет основой будущих модификаций стандартов мобильной связи, включая стандарты 5G.

С другой стороны, активно развиваются энергоэффективные технологии низкой мощности для нелицензируемого частотного спектра, такие как LoRa, Sigfox, «Стриж» и другие.

На рис. 1.7. приведен пример экосистемы IoT в масштабах населенного пункта или целой страны, благодаря которым у локальных систем появляются новые возможности, например, заказа товара в магазине или бронирования мест при поездке на отдых в автоматическом режиме [7].

Рис. 1.7. Концепция умного города

1.3. Основные термины и понятия

Интернет вещей (IoT) - Объединение уникально идентифицируемых встроенных вычислительных устройств в рамках развернутой интернет инфраструктуры [3].

Уровень управления доступом к среде передачи данных - MAC-уровень часть протокола передачи данных, которая контролирует доступ к физической среде передачи в сетях IEEE 802 (LAN).

Система на чипе SoC - интегральная схема (ИС), которая объединяет все компоненты компьютера или другой электронной системы в один чип.

Синхронизованный временной mesh-протокол (TSMP) - сетевой протокол, являющийся центральным элементом беспроводной сенсорной сети с низким энергопотреблением.

Беспроводная локальная сеть (WLAN) - локальная сеть, в которой данные передаются без использования проводов.

Беспроводная городская сеть (WMAN) - другое название – беспроводной абонентский доступ (WLL). В основу WMAN положен стандарт IEEE 802.16. Эффективная скорость беспроводного абонентского доступа составляет от 1 до 10 Мбит /секунду на удалении от 4 до 10 километров.

Беспроводная персональная сеть (WPAN) - беспроводная сеть малого радиуса действия, которая занимает площадь всего несколько десятков метров

Беспроводная сенсорная сеть (WSN) - самоорганизующиеся сети с множеством переходов беспроводных сенсорных узлов, используемых для мониторинга и управления физическими явлениями

Беспроводная глобальная сеть (WWAN) - беспроводная сеть, обеспечивающая коммуникационные услуги в пределах географической области большей, чем территория одного города. Этот вид сетей является наиболее распространенным из всех беспроводных сетей.

Контрольные вопросы

1. Особенность концепции Интернет вещей.
2. Какие сети относится к Интернету вещей?
3. В чём заключается формирование и практическая реализация концепции IoT?
4. Расскажите о дорожной карте Интернета вещей.
5. Какие общие показатели требуют внедрения инновационных сетевых технологий, предназначенных для IoT.
6. Сравните технологии LPWAN, Zigbee, GSM/LTE по показателям.

Глава 2. СТАНДАРТЫ И ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ В IoT

2.1. Базовые принципы IoT

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и, в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен.

Наиболее важными отличиями Интернета вещей от существующего интернета являются [3]:

- фокус на вещах, а не на человеке;
- существенно большее число подключенных объектов;
- существенно меньшие размеры объектов и невысокие скорости передачи данных;
- фокус на считывании информации, а не на коммуникациях;
- необходимость создания новой инфраструктуры и альтернативных стандартов.

Концепция сетей следующего поколения NGN предполагала возможность коммуникаций людей (непосредственно или через компьютеры) в любое время и в любой точке пространства. Концепция Интернета вещей включает еще одно направление - коммуникация любых устройств или вещей (рис. 2.1) [8].

Официальное определение Интернета вещей приведено в Рекомендации МСЭ-Т Y.2060, согласно которому IoT - глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий.

Под «вещами» (things) здесь понимается физический объект (физическая вещь) или объект виртуального (информационного) мира (виртуальная вещь, например, мультимедийный контент или прикладная программа), которые могут быть идентифицированы и объединены через коммуникационные сети.

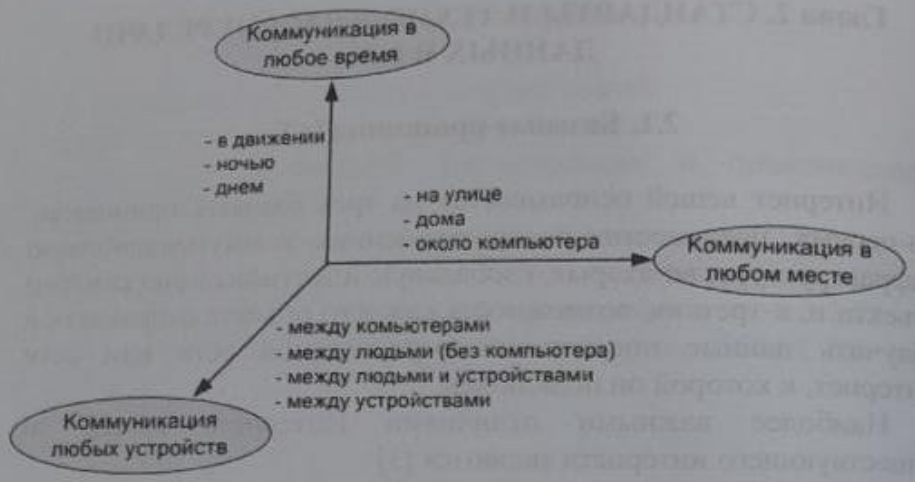


Рис. 2.1. Новое направление коммуникаций, реализуемое Интернетом вещей

Кроме понятия «вещь», МСЭ-Т также использует понятие «устройство» (device), под которым понимается часть оборудования с обязательными возможностями по коммуникации и необязательными возможностями по сенсорингу/зондированию, приведению в действие вещи, сбору, обработке и хранению данных. Отсюда следует, что МСЭ-Т в большей степени уделяет вниманию аспектам коммуникаций и межсоединений, нежели приложениям IoT [8].

Схема отображения физических и виртуальных вещей представлена на рис. 2.2. Из рисунка следует, что виртуальные вещи могут существовать без их физических воплощений, в то время как физическим объектам/вещам обязательно соответствует минимум один виртуальный объект. При этом ведущую роль играют именно устройства, которые могут собирать различную информацию и распространять её по коммуникационным сетям различными способами: через шлюзы и через сеть; без шлюзов, но через сеть; напрямую между собой.

Рекомендация Y.2060 описывает различное сочетание перечисленных способов соединений [8]. Это указывает на то, что МСЭ-Т предусматривает использование для IoT множества

сетевых технологий - глобальных сетей, локальных сетей, беспроводных самоорганизующихся (ad-hoc) и ячеистых (mesh) сетей. Указанные сети связи переносят данные, собранные устройствами, к соответствующим программным приложениям, а также передают команды от программных приложений к устройствам.

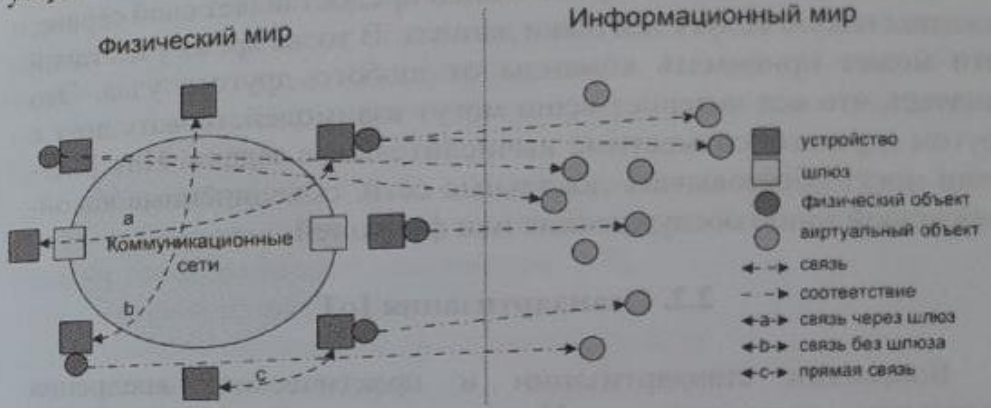


Рис. 2.2. Схема отображения физических и виртуальных вещей

Следует отметить, что вещи и связанные с ними устройства могут обладать полноценными управляющими процессорами для обработки данных в виде «системы-на-кристалле», в том числе с собственной операционной системой, блоком сенсоринга/зондирования окружающей среды и блоком коммуникации.

Следует различать понятия «Интернет вещей» и «интернет-вещь». Под интернет-вещью понимается любое устройство, которое:

- имеет доступ к сети Интернет с целью передачи или запроса каких-либо данных,
- имеет конкретный адрес в глобальной сети или идентификатор, по которому можно осуществить обратную связь с вещью,
- имеет интерфейс для взаимодействия с пользователем.

Интернет-вещи имеют единый протокол взаимодействия, согласно которому любой узел сети равноправен в предоставлении

своих сервисов. На пути перехода к воплощению идеи Интернета вещей стояла проблема, связанная с протоколом IPv4, ресурс свободных сетевых адресов которого уже практически исчерпал себя. Однако подготовка к повсеместному внедрению версии протокола IPv6 позволяет решить эту проблему и приближает идею Интернета вещей к реальности.

Каждый узел сети интернет-вещей предоставляет свой сервис, оказывая некую услугу поставки данных. В то же время узел такой сети может принимать команды от любого другого узла. Это означает, что все интернет-вещи могут взаимодействовать друг с другом и решать совместные вычислительные задачи. Интернет-вещи могут образовывать локальные сети, объединённые какой-либо одной зоной обслуживания или функцией.

2.2. Стандартизация IoT

Вопросами стандартизации и практического внедрения отдельных составляющих Интернета вещей (M2M, RFID, всепроникающие сенсорные сети и др.) занимаются многие международные организации, неправительственные ассоциации, альянсы производителей и операторов, партнерские проекты. В целом для Интернета вещей, как нового направления развития инфокоммуникаций, в настоящее время определены самые общие концептуальные и архитектурные решения. В ближайшее время основной проблемой будет гармонизации различных стандартов с целью формирования единой и непротиворечивой нормативной базы для практической реализации Интернета вещей [9, 10].

В рамках деятельности сектора стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) имеются три глобальных инициативы GSI (Global Standards Initiative). Под глобальной инициативой понимается комплекс работ, выполняемых параллельно разными исследовательскими комиссиями МСЭ в соответствии со скоординированным планом работы. Одна из таких инициатив посвящена стандартизации Интернета вещей - IoT-GSI (Global Standards Initiative on Internet of Things). Две другие глобальные инициативы - по стандартизации сетей последующих поколений NGN-GSI и систем телевидения на основе протокола Интернет IPTV-GSI - также базируются на

использовании IP-технологий, как и IoT-GSI.

IoT-GSI строит свою работу на основе усилий МСЭ-Т в таких областях, как сетевые аспекты идентификационных систем (Network Identificator, NID), всепроникающие сенсорные сети (Ubiquitous Sensor Networks, USN), межмашинная связь (M2M), WEB вещей (WoT) и т.п. В рамках серии МСЭ-Т Y.xx, посвященной сетям следующего поколения NGN, уже утверждены первые рекомендации, посвященные специально Интернету вещей: Y.2060 «Обзор Интернета вещей», Y.2063 «Основа WEB вещей» и Y.2069 «Термины и определения Интернета вещей» и др. [11].

В Рекомендации Y.2060 приведена эталонная модель IoT, которая очень похожа на модель NGN и также включает четыре базовых горизонтальных уровня (рис. 2.3):

- уровень приложений IoT;
- уровень поддержки приложений и услуг;
- сетевой уровень;
- уровень устройств.

Уровень приложений IoT в Рекомендации Y.2060 детально не рассматривается. Уровень поддержки приложений и услуг включает общие возможности для различных объектов IoT по обработке и хранению данных, а также возможности, необходимые для некоторых приложений IoT или групп таких приложений.

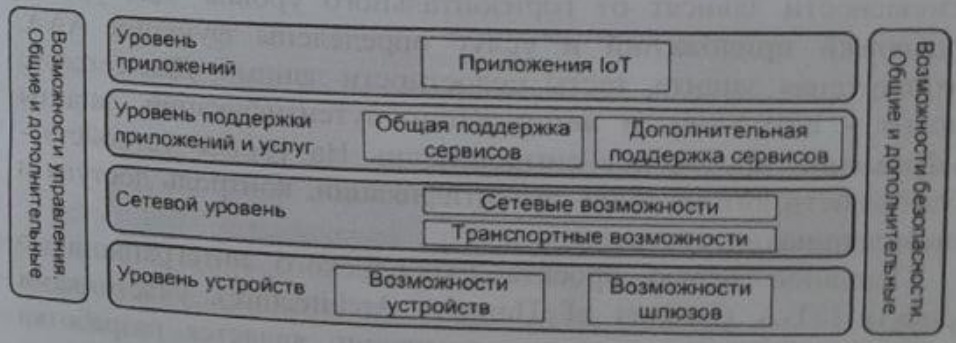


Рис. 2.3. Эталонная модель IoT согласно МСЭ-Т Y.2060

Сетевой уровень включает сетевые возможности (функция

управления ресурсами сети доступа и транспортной сети, управления мобильностью, функции авторизации, аутентификации и расчетов, AAA) и транспортные возможности (обеспечение связности сети для передачи информации приложений и услуг IoT). Наконец, уровень устройств включает возможности устройства и возможности шлюза. Возможности устройства предполагают прямой обмен с сетью связи, обмен через шлюз, обмен через беспроводную динамическую ad-hoc сеть, а также временный останов и возобновление работы устройства для энергосбережения. Возможности шлюза предполагают поддержку множества интерфейсов для устройств (шина CAN, ZigBee, Bluetooth, Wi-Fi и др.) и для сетей доступа/транспортных сетей (2G/3G, LTE, DSL и др.). Другой возможностью шлюза является поддержка конверсии протоколов, в случае, если протоколы интерфейсов устройств и сетей отличаются друг от друга [12-15].

Существует также два вертикальных уровня - уровень управления и уровень безопасности, охватывающие все четыре горизонтальных уровня. Возможности вертикального уровня эксплуатационного управления предусматривают управление последствиями отказов, возможностями сети, конфигурацией, безопасностью и данными для биллинга. Основными объектами управления являются устройства, локальные сети и их топология, трафик и перегрузки на сетях. Возможности вертикального уровня безопасности зависят от горизонтального уровня. Для уровня поддержки приложений и услуг определены функции AAA, антивирусная защита, тесты целостности данных. Для сетевого уровня - возможности авторизации, аутентификации, защиты информации протоколов сигнализации. На уровне устройств - возможности авторизации, аутентификации, контроль доступа и конфиденциальность данных.

Основной целью проекта Европейского интеграционного проекта IoT-A (Internet of Things - Architecture), участниками которого являются различные компании, является разработка эталонной архитектурной модели Интернета вещей с описанием основных составляющих компонентов, которая бы позволила интегрировать разнородные технологии IoT в единую взаимосвязанную архитектуру.

Функциональная модель IoT-A (рис. 2.4) несколько отличается от модели МСЭ (рис. 2.3), хотя она тоже является иерархической, но состоит уже из семи горизонтальных уровней, дополняемых двумя вертикальными (управление и безопасность), которые участвуют во всех процессах.

Если обратиться к техническим особенностям модели на рис. 2.5, то можно сказать, что модель передачи данных в Интернете вещей IoT-A будет отличаться от существующей модели передачи данных через Интернет. В модели архитектуры IoT-A фигурируют два важных понятия. Сеть с ограничениями характеризуется относительно низкими скоростями передачи - менее 1 Мбит (например, стандарт IEEE 802.15.4) и достаточно высокими задержками.

Рис. 2.4. Функциональная модель архитектуры IoT-A

Сеть без ограничений соответственно характеризуется высокими скоростями передачи данных (десятки Мбит/с и более) и похожа на существующую сеть Интернет. Различие данных моделей сетей показано на рис. 2.5.

Рис. 2.5. Сравнение моделей передачи данных в Интернете и в IoT

2.3. Стандарты и технологии передачи данных в 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 [16]:

- 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 том числе 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) [17]

Сравнение беспроводных технологий IoT по дальности действия и полосе пропускания представлено на рис. 2.6. На рис. 2.7 приведен обзор и позиционирование основных технологий Short Range и LPWAN.

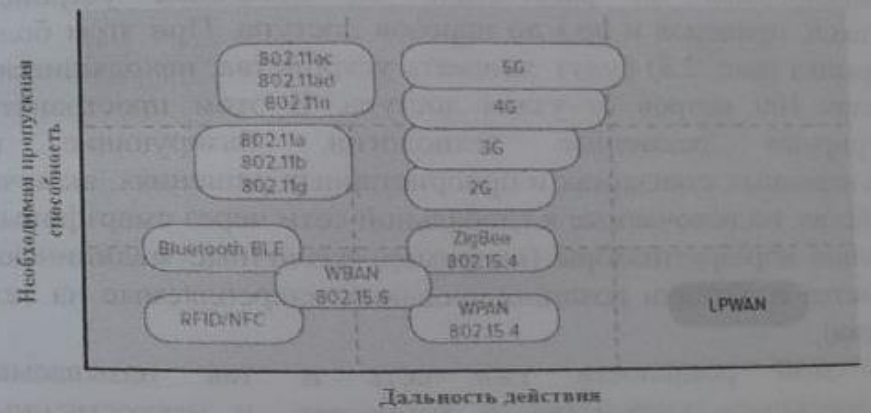


Рис. 2.6. Сравнение беспроводных технологий IoT по дальности действия и полосе пропускания

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.

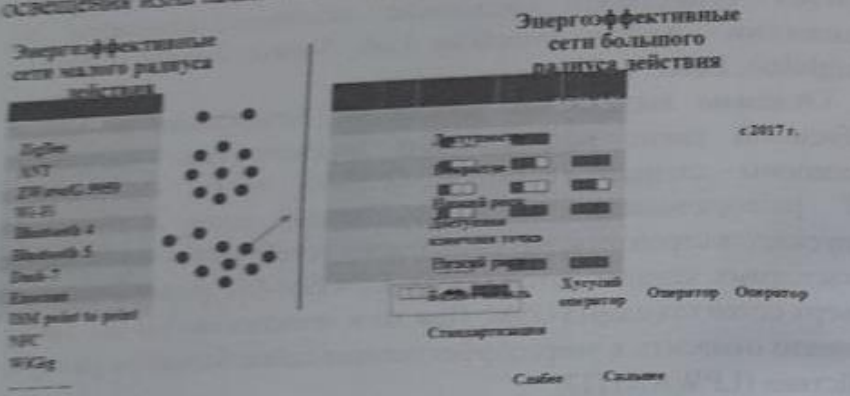


Рис. 2.7. Обзор и позиционирование основных технологий Short Range и LPWAN

Технологии реализации Интернета вещей могут быть также проранжированы по расстоянию от конечных устройств (датчиков, приводов и пр.) до шлюзов доступа. При этом более 90% рынка (рис. 2.8) будут занимать устройства, находящиеся в пределах 100 метров от узлов доступа. В этом пространстве конкурируют различные технологии, базирующие на международных стандартах и проприетарных решениях, включая устройства, подключаемые к глобальной сети через смартфоны и домашние маршрутизаторы (например, различные медицинские устройства и датчики позиционирования, закрепляемые на теле человека).

В этой реальности уже есть и так называемые «подключенные» устройства, и нейросети, и искусственный интеллект со всеми его достоинствами и рисками, и даже информационные облака, как называют «облачные» серверы с мультидоступом для хранения и обработки данных. Типовые примеры построения сетей IoT приведены на рис. 2.9 и 2.10 [19]. Они помогают понять всю глубину внедрения технологии IoT в нашу повседневную жизнь и оценить то, что ждет нас уже в самом ближайшем будущем.

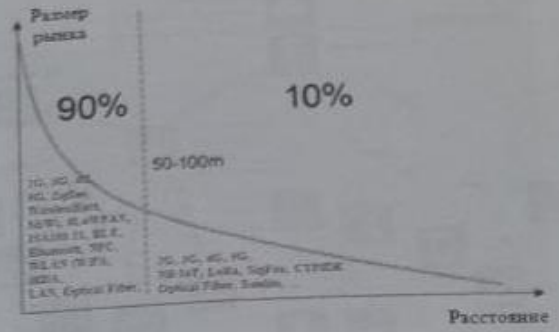


Рис 2.8. Разделение Интернет вещей по расстоянию от конечных устройств (датчиков) до шлюзов подключения

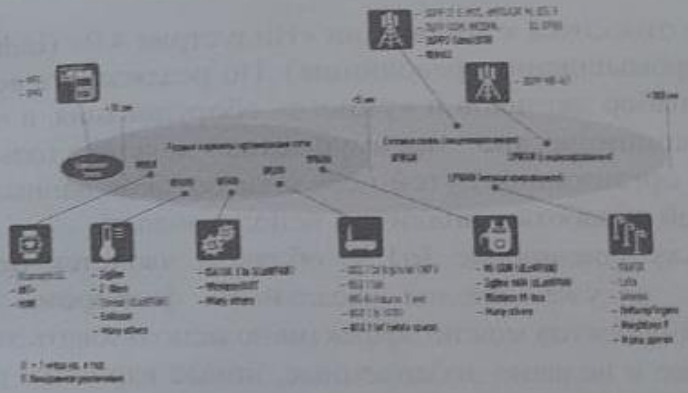


Рис. 2.9. Технологии IoT, сгруппированные по рабочему диапазону покрытия

IoT - это технология, революционизирующая производственные процессы. Как уже говорилось, ее внедрение позволяет собирать данные и в режиме реального времени сообщать о текущем состоянии оборудования, более эффективно контролировать функционирование производства. Применительно к предприятиям IoT трансформировался в «Индустриальный Интернет вещей» (Industrial Internet of Things, IIoT), то есть относящийся к индустрии, а также в «Корпоративный Интернет вещей» (Enterprise IoT, EIoT).

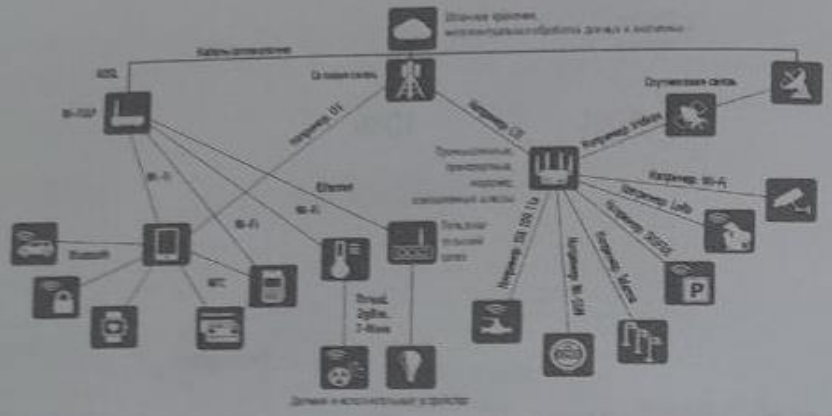


Рис. 2.10. Пути и шлюзы для доступа к облаку

Все это относится к концепции «Индустрия 4.0» (Industry 4.0, четвертая промышленная революция). Но реализовать все это не просто как набор датчиков и «умного» оборудования, а получить весомые экономические преимущества можно только при правильной организации путей передачи потоков данных для их последующей обработки, анализа и использования.

Поскольку соединение IoT с облаком является не только ожидаемым, а уже вполне реальным фактором, то для реализуемых проектов можно эффективно использовать эти, недоступные ранее и недавно добавленные, новые варианты решений для предложений беспроводной связи.

Распределение частот для протоколов беспроводной связи IoT приведена в таблице 2.1.

Технологии, основанные на стандартах мобильной связи

Типовой элемент IoT является, как правило, компактным устройством с низкой скоростью передачи данных и малым собственным энергопотреблением. Одним из основных требований к нему является минимальная стоимость организации канала связи [20].

Использование существующих сотовых сетей для целей IoT принято считать избыточным и дорогим, сложные протоколы и повышенная скорость обмена информацией приводят к чрезмерному энергопотреблению и быстрой разрядке батарей

датчиков и других устройств. Поэтому для повышения эффективности работы IoT-приборов и одновременного уменьшения затрат консорциумом 3GPP (The 3rd Generation Partnership Project) было принято решение о модернизации стандартных мобильных сетей. К основным таким модернизированным сетям можно отнести:

- EC-GSM (также носит названия EC-GPRS, EC-GSM-IoT);
- eMTC (то же, что и LTE-M, LTE Cat.M1);
- NB-IoT (таблица 2.2).

Таблица 2.1

Распределение частот для протоколов беспроводной связи IoT

Основное наименование	Частота, МГц															Альтернативное название
	13,56	169	220	315	426	433	470	779	868	915	920	2400	5800	5900		
NFC/EMV	♦															ISO14443
Wireless M-Bus		♦				♦			♦							EN13757
China WMPNET						♦	♦									WMBNET I, II, III, IV
LoRa						♦	♦		♦	♦						
SIGFOX									♦	♦						
Telensa									♦	♦						
OnRamp												♦				802.15.4k
Wi-SUN											♦					802.15.4g/e/6LoWPAN
ZigBee								♦	♦	♦	♦	♦				802.15.4-2003, c d
Thread												♦				802.15.4-2003/6LoWPAN
WirelessHART												♦				802.15.4e
ISA100.11a												♦				802.15.4e/6LoWPAN
Z-Wave									♦	♦	♦					ITU G9959
EnOcean				♦						♦	♦					ISO14543-3-10
ANT+												♦				
Bluetooth												♦				802.15.1
802.11/a/b/g/n/ac												♦	♦			Wi-Fi
802.11ah (HaLow)								♦	♦	♦	♦					Wi-Fi HaLow
802.11p														♦		V2X
802.11af				♦												White Space
Positive Train Ctrl			♦													802.15.4p

Отличительные характеристики технологий EC-GSM, eMTC и NB-IoT Таблица 2.2

Характеристики	EC-GSM	GMTC	NB-IoT
Используемый частотный спектр	Ширина канала 200 кГц в рамках полосы GSM (частотные диапазоны 900 и 1800 МГц)	Ширина канала 1.08 МГц в рамках полосы LTE. Любой из диапазонов, определенных для использования FDD и TDD LTE	Ширина канала 200 кГц в одном из трех вариантов размещения: 1) отдельно; 2) внутри полосы LTE; 3) внутри защитного интервала LTE. Любой из диапазонов, определенных для использования FDD LTE
Бюджет канала связи, дБ	154-164	155.7	до 164
Тип множественного доступа и модуляция (DownLink)	TDMA/FDMA. GMSK/8PSK	OFDMA. 16QAM	OFDMA
Тип множественного доступа и модуляция (UpLink)	TDMA/FDMA. GMSK/8PSK	SC-FDMA. 16QAM	SC-FDMA и FDMA/GMSK
Максимальная скорость передачи данных	При использовании 4 таймслотов (из 8 доступных в GSM): 70 кбит/с (GMSK) и 240 кбит/с (8PSK)	1 Мбит/с	до 250 кбит/с
Количество узлов сети	50 000 на одну БС	-	50 000 на одну БС

Технология EC-GSM предусматривает сравнительно небольшие изменения относительно базового GSM/GPRS/EDGE, что позволяет использовать подавляющее большинство установленных базовых станций (БС) этого стандарта без замены или модернизации аппаратной части [21].

В этом и заключается ключевое преимущество EC-GSM - сетевая инфраструктура существующей мобильной сети GSM, распространенной по всему миру, практически готова для внедрения IoT, во многих случаях требуется только обновить программное обеспечение (ПО) на узлах сети.

Пакет расширенных программных функций позволяет увеличить бюджет канала связи и включает в себя следующие изменения:

– уменьшение периодичности обязательных сигнальных сообщений, оптимизацию интервалов приема и получения информации, поддержку длительных (до 52 мин) периодов «молчания», в течение которых устройство остается подключенным к сети, не передавая и не получая информацию;

– адаптацию канального уровня сети для улучшения покрытия на 20 дБ по сравнению с базовой системой;

– упрощение сетевой сигнализации (отказ от поддержки совместимости с WCDMA/ LTE сетями), расширение механизмов аутентификации и безопасности соединения.

При помощи аналогичных программных изменений получена технология eMTC, являющаяся адаптацией сетей LTE для целей IoT. Этот стандарт также сфокусирован на достижении целевых показателей массового IoT (стоимость, покрытие, срок автономной работы) при одновременном обеспечении максимальной совместимости с имеющейся у мобильных операторов сетевой инфраструктурой.

Технология eMTC призвана снизить стоимость конечных элементов сети за счет отказа от функциональности LTE, избыточной при массовом подключении устройств. При этом, зачастую, сети LTE и eMTC могут сосуществовать и динамически перераспределять используемые ресурсы (частотный спектр, вычислительную мощность базовой станции и др.) в зависимости от типа и количества подключенных устройств и

создаваемого ими трафика. Важное отличие технологии eMTC - высокая пропускная способность, скорость передачи данных в исходящем и входящем каналах составляет 1 Мбит/с, что востребовано при определенных сценариях.

NB-IoT (Narrowband IoT, узкополосный ИВ) - это относительно новое направление развития сетевых технологий. Несмотря на то, что его использование предусматривает тесное взаимодействие и интеграцию с LTE, речь все же идет о создании нового типа радиодоступа, характеристики которого имеют больше отличий, чем сходств с имеющимися технологиями.

О поддержке технологии NB-IoT в своих продуктах уже заявили многие производители сетевого оборудования и абонентских модулей: Ericsson, Huawei, Nokia, Intel, Qualcomm, а также ведущие операторы связи, среди которых можно отметить Vodafone, Deutsche Telekom и China Unicom.

Сети NB-IoT предоставляют множество серьезных преимуществ, среди которых:

- поддержка более 100 тыс. соединений на соту;
- десятилетняя гарантия срока службы аккумулятора4
- повышенная безопасность за счет двусторонней аутентификации и усиленного шифрования интерфейса.

Таким образом, принятие финальных версий спецификаций EC-GSM, eMTC и NB- IoT позволяет получить три эффективных инструмента развития сетей IoT. К преимуществам каждой из рассмотренных сетей можно отнести:

- использование инфраструктуры существующих мобильных операторов;
- поддержку роуминга;
- высокие скорости передачи данных для мультимедийного оборудования и устройств, которым необходимо функционировать в режиме реального времени.

Недостатки состоят в том, что:

- для их функционирования необходим лицензируемый спектр;
- тарифы на передачу данных могут быть высокими для нетребовательного к скоростям оборудования;
- стоимость устройств, работающих в этих сетях, все еще достаточно высока. Кроме того, остается открытым вопрос

стандартизации.

Стандарты технологий LPWAN

Для оконечных устройств сети, обычно выполняющих функции сбора данных, не так важны скорость и объем передаваемой информации; определяющими характеристиками являются длительность работы без дополнительного обслуживания и зарядки аккумуляторов (измеряемая месяцами и годами). Для соответствия данному требованию активно внедряются новые типы маломощных сетей LPWAN, отличающихся низким энергопотреблением и одновременно большим радиусом действия [22].

К типовым элементам сетей данного типа относятся:

- автономные счетчики потребления ресурсов (воды, газа, электричества), установленные в подвалах жилых домов;
- модули управления уличным освещением;
- датчики систем безопасности и т. д.

В настоящее время существует несколько распространенных LPWAN-технологий для IoT, которые работают в нелицензируемых субгигагерцовых частотных диапазонах. Наибольшую популярность имеют конкурирующие технологии для сетей IoT большой дальности - Sigfox, LoRaWAN и «СТРИЖ», в таблице 2.3 приведены их основные отличительные особенности [22].

Компанией Sigfox (Франция) разработана одноименная технология сверхузкополосной (Ultra Narrow Band, UNB) беспроводной связи для передачи данных в диапазонах 868 и 902 МГц. Сеть развернута во многих странах (во Франции, Италии, Великобритании, Испании, Бельгии, Ирландии, США и странах Латинской Америки). Решения разработаны для «умных городов», интеллектуальных зданий, дистанционного мониторинга, контроля и учета энергоресурсов и множества других приложений.

Сеть «СТРИЖ» реализуется компанией «СТРИЖ Телематика», для построения используется узкополосная модуляция и собственный протокол связи Marcato 2.0.

Таблица 2.3

Отличительные особенности технологий Sigfox, LoRaWAN и «СТРИЖ»

Характеристики	LoRaWAN	Slgfox	Стриж
Модуляция	Широкополосная LoRa	Узкополосная DPSK	Узкополосная
Ширина полосы	125 кГц	100 Гц	100 Гц
Разделение	CDMA,TDMA	FDMA	FDMA,TDMA
Симметричность канала	Полная	Ограниченная	Ограниченная
Классы оконечных	A, B, C	A	A
Скорость передачи	От 300 до 50 000	100	100
Сложность базовой	От низкой до средней	Высокая	Высокая
Помехоустойчивость	Средняя	Высокая	Высокая
Степень проприетарност	Низкая	Высокая	Абсолютная
Глобальные сети LPWAN	Да	Да	Да
Локальные сети масштаба	Да	Нет	С ограничениями

В основе сетей LoRaWAN (Long Range Wide Area Networks) лежит использование запатентованного компанией Semtech метода модуляции LoRa, реализуемого в «железе» и обеспечивающего хорошие показатели бюджета канала связи (до 168 дБ). Разработкой и стандартизацией LoRaWAN занимается некоммерческая организация LoRa Alliance [23].

Помимо основателей альянса, компаний IBM и Semtech, в это объединение входят известные производители электроники, такие как Cisco, Kerlink, IMST, Microchip Technology, а также лидирующие телекоммуникационные операторы (Bouygues Telecom, Inmarsat, SingTel, Proximus, Swisscom), при этом количество зарегистрированных членов постоянно увеличивается.

Общая черта всех перечисленных технологий в том, что они позволяют организовать низкоскоростную беспроводную передачу данных на дальностях в единицы или десятки километров, не выходя при этом за ограничения безлицензионных радиодиапазонов (как правило, такие системы работают на частотах 864-869 МГц с мощностью до 25 мВт). Однако в том, как именно происходит использование радиочастотного спектра, они достаточно существенно различаются: у широкополосных (UWB) LoRaWAN сетей один канал занимает полосу 125 или 250 кГц, в то время как у узкополосных Sigfox или «Стриж» его ширина составляет 100 Гц (рис. 2.11). У каждого из способов есть свои плюсы и минусы.

В UNB-системах, использующих частотное разделение каналов, приемник базовой станции (БС) в один момент времени может принимать данные только от одного узла сети. В сетях LoRaWAN используется не только частотное и временное, но и кодовое разделение каналов, БС способна разделять потоки данных от нескольких устройств, одновременно работающих с разными схемами модуляции на одном частотном канале.

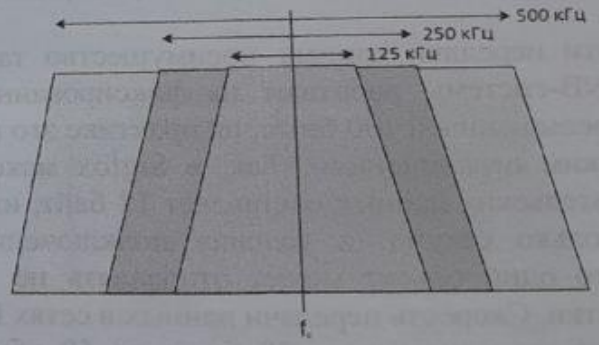


Рис. 2.11. Типовые значения ширины радиоканала для сети LoRa

Кроме того, UNB-системы крайне чувствительны к точности установки частоты. Например, хороший кварцевый резонатор имеет погрешность 10 ppm (0,001%) при комнатной температуре, также можно добавить еще 15 ppm (0,0015%) сверху при изменении температуры в диапазоне -40.. .+85 °С. Даже такое

малое изменение может значительно превысить номинальную ширину 100 Гц канала и выбросить рабочую частоту оконечного устройства за пределы заданной ему полосы. Частично эта проблема решается при помощи термостабилизированных генераторов (ТСГ), позволяющих уменьшить погрешность примерно в 10 раз, но стоимость узлов сети при этом значительно возрастает.

Более продвинутый вариант, применяемый в современных БС, подразумевает оцифровку, спектральный анализ радиоэфира и поиск абонентских устройств. Такая система действительно эффективна, но цифровая обработка сигналов в режиме реального времени является сложной вычислительной задачей, требующей от БС весьма серьезных аппаратных и программных ресурсов. К тому же, реализовать такие же алгоритмы на уровне маленького, дешевого и экономичного оконечного устройства проблематично, поэтому двунаправленность связи в UNB-системах присутствует не всегда и не везде. В отличие от них, сеть LoRaWAN гарантирует симметричный канал связи. Благодаря полосе шириной в сотни кГц, обеспечивается симметричная связь при уходе частоты на 25% от ширины канала (31,25 кГц при ширине 125 кГц), что в диапазоне 868 МГц означает допустимую погрешность резонатора в 35 ppm.

По скорости передачи данных преимущество также имеет LoRaWAN. UNB-системы работают на фиксированной низкой скорости, не превышающей 100 бит/с, на практике это приводит к довольно жестким ограничениям. Так, в Sigfox максимальный объем пользовательских данных составляет 12 байт, их передача занимает несколько секунд, а условия подключения к сети определяют, что один объект может отправлять не более 140 сообщений в сутки. Скорость передачи данных в сетях LoRaWAN - адаптивная, может меняться от 30 бит/с до 50 кбит/с. Из-за сложной системы модуляции длина сетевого пакета больше, чем у UNB-систем (длиннее преамбула), но это с лихвой компенсируется большей пропускной способностью.

Отдельного внимания заслуживает вопрос помехозащищенности, здесь в более выгодном положении находятся узкополосные системы, обладающие возможностью перестройки частоты на десятки кГц в любую сторону. БС, анализирующая широкий диапазон, все равно поймает сигнал от

абонентского устройства. С другой стороны, каждый узел сети может перед отправкой сообщения прослушать эфир и переключиться в другую полосу, если на его полосе слишком шумно. Устройства LoRaWAN достаточно чувствительны к помехам, но на практике избыточность кодирования позволяет им спокойно функционировать, например, по соседству с узкополосными системами.

Энергопотребление конечных устройств определяется технологическим совершенством чипов передатчиков и временем, в течение которого они находятся в активном режиме. Во всех перечисленных технологиях обеспечивается работа на одной батарейки в течение 5 лет и более (рис. 2.12). UWB-сети имеют преимущество над UNB при работе на небольших дистанциях, когда их скорость может превышать 1 кбит/с, а время активности и энергопотребление передатчика значительно сокращается вследствие быстрой передачи данных.

Дальность связи - примерно одинаковая и сильно зависит от условий на местности, в целом можно считать, что все перечисленные технологии обеспечивают радиус действия 1-3 км в городской застройке и 15-20 км на открытой местности (рис. 2.13).

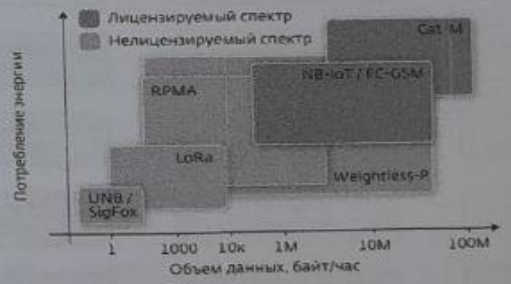


Рис.2.12. Сравнительная оценка энергопотребления технологии LoRa и других радиотехнологий

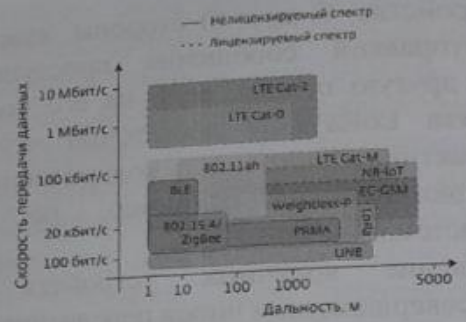


Рис. 2.13. Характеристики сетей радиодоступа IoT в нелицензируемых и лицензируемых участках спектра

Отдельно стоит упомянуть об открытости сравниваемых систем, являющейся немаловажным фактором при выборе конкретной технологии IoT. Любая реализованная сеть содержит несколько типовых уровней, изображенных на рис. 2.14 [24].

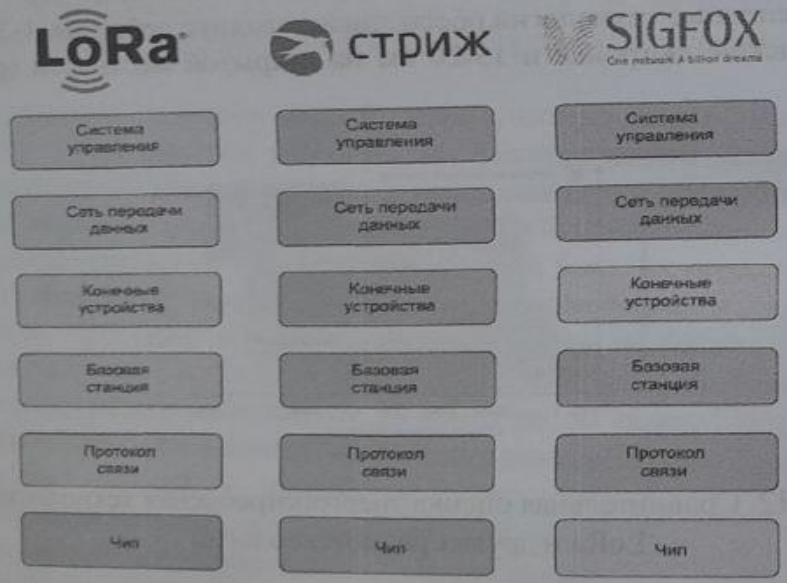


Рис. 2.14. Сравнение открытости технологий Sigfox, LoRaWAN и «СТРИЖ» (розовым цветом отмечены закрытые уровни, зеленым - открытые)

Как видно, Sigfox представляет собой довольно закрытую систему. Для ее использования необходимо приобрести у компании БС и заключить с ней договор на разворачивание сети, к которой будет предоставляться платный доступ сторонним абонентам.

Серверы Sigfox с программным обеспечением верхнего уровня также принадлежат компании. Положительным моментом является доступность чипов и оконечных устройств, их производят компании Texas Instruments, SiLabs и ряд других изготовителей.

Технология «Стриж» отличается абсолютной закрытостью. Компания «Стриж Телематика» сама производит и устанавливает БС и конечные устройства, предоставляет сервер сети и с каждого подключенного устройства взимает абонентскую плату.

Некоторым преимуществом LoRaWAN является то, что на фоне конкурентов это довольно открытая технология, в мире есть много занимающихся ей компаний. Чипы LoRaWAN для конечных устройств присутствуют в свободной продаже, документация на них открыта, делать устройства на них могут все желающие.

Архитектура сети LoRaWAN

Типичная сеть LoRaWAN имеет базовую топологию «звезда» и состоит из оконечных узлов, шлюзов, сетевого сервера и сервера приложений [24]. Принцип работа прост: БС (шлюзы) передают зашифрованные данные, полученные от оконечных устройств, на центральный сервер сети провайдера и далее - на сервер приложений сервис-провайдера, с которого информация поступает пользователям (рис. 2.15).

Центральный сервер LoRaWAN осуществляет общее управление сетью, в частности, принимает решение о необходимости адаптации скорости передачи данных, изменения мощности передатчика, выборе канала передачи, начале сессии и продолжительности ее по времени, измеряет заряд батарей конечных узлов, т. е. полностью контролирует каждое абонентское устройство в отдельности.

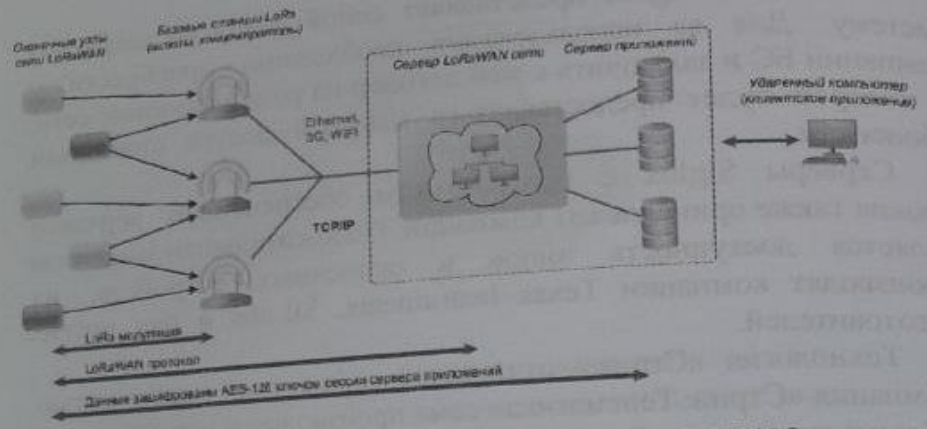


Рис. 2.15. Типовая архитектура сети LoRaWAN

Каждый LoRaWAN пакет данных, отправляемых конечным узлом, имеет в своем составе уникальный идентификатор приложения, соответствующий определенному приложению на сервере провайдера и используемый для его дальнейшей маршрутизации.

На рис. 2.16 приведена упрощенная модель сети LoRaWAN.

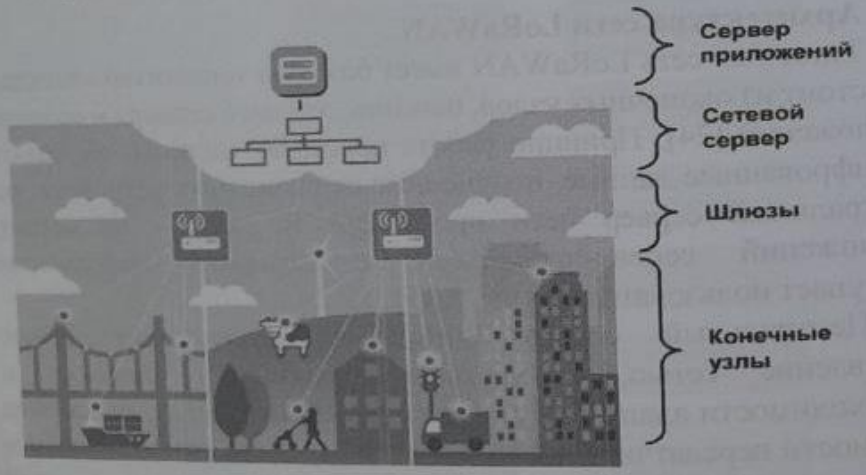


Рис. 2.16. Упрощенная модель сети LoRaWAN

Таким образом, технология LoRaWAN основана на следующих двух ключевых элементах:

- для радиоинтерфейса физического уровня он идентифицирует все аспекты передачи радиосигнала между сетевыми шлюзами LoRaWAN и конечными устройствами. Радиоинтерфейс LoRaWAN устанавливает обмен сигналами между рабочими частотами, типом модуляции, уровнем мощности, сигнализацией и устройствами передачи и приема в сети LoRaWAN;
- к сетевой архитектуре включает абонентские устройства IoT/M2M, шлюзы LoRaWAN (базовые станции), сетевые серверы, подключенные к сети Интернет по транспортной сети, и серверы приложений (рис. 2.17).

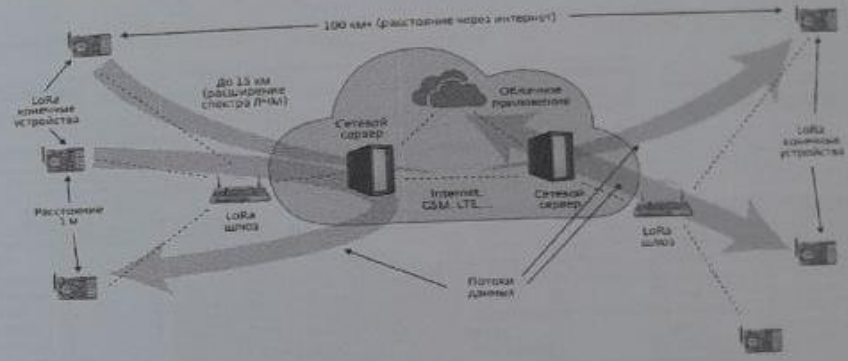


Рис. 2.17. Архитектура сети LoRaWAN

Контрольные вопросы

1. Каковы основные принципы, на которых основаны интернет-вещи?
2. Каковы наиболее важные отличия Интернета от существующего Интернета?
3. Какое новое направление связи используется в интернет-объектах?
4. Что подразумевается под «вещами»?
5. Что подразумевается под «устройством»?

6. Что подразумевается под «интернет вещью» и «интернетом вещей»?

7. Объясните эталонную модель IoT и ее уровни.

8. Объясните функциональную модель архитектуры IoT-A.

9. Сравните модели передачи данных в Интернете и IoT?

10. Перечислите беспроводные технологии IoT?

11. Какие технологии входят в технологии IoT на основе стандартов сотовой связи? Их основные характеристики.

12. Какие технологии включены в технологии IoT в стандарты технологии LPWAN? Их основные характеристики.

Глава 3. АРХИТЕКТУРА IOT И СПОСОБЫ ВЗАИМОДЕЙСТВИЯ С ИНТЕРНЕТ-ВЕЩАМИ

3.1. Архитектура IoT

Интернет вещей концептуально принадлежит к сетям следующего поколения, поэтому его архитектура во многом схожа с известной четырехслойной архитектурой NGN. IoT состоит из набора различных инфокоммуникационных технологий, обеспечивающих функционирование Интернета вещей, и его архитектура показывает, как эти технологии связаны друг с другом. Архитектура IoT включает четыре функциональных уровня (рис. 3.1) [3].

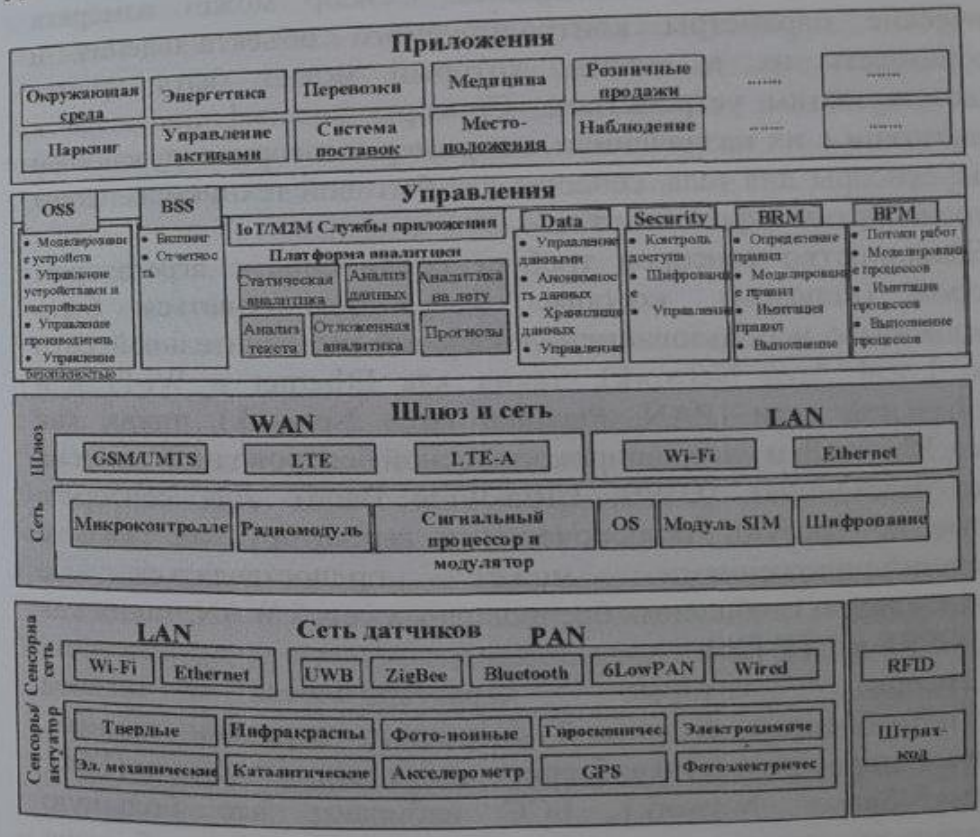


Рис. 3.1. Архитектура IoT

1. *Уровень сенсоров и сенсорных сетей*

Самый нижний уровень архитектуры IoT состоит из «умных» (smart) объектов, интегрированных с сенсорами (датчиками). Сенсоры реализуют соединение физического и виртуального (цифрового) миров, обеспечивая сбор и обработку информации в реальном масштабе времени. Миниатюризация, приведшая к сокращению физических размеров аппаратных сенсоров, позволила интегрировать их непосредственно в объекты физического мира.

Существуют различные типы сенсоров для соответствующих целей, например, для измерения температуры, давления, скорости движения, местоположения и др. Сенсоры могут иметь небольшую память, давая возможность записывать некоторое количество результатов измерений. Сенсор может измерять физические параметры контролируемого объекта/явления и преобразовать их в сигнал, который может быть принят соответствующим устройством. Сенсоры классифицируются в соответствии с их назначением, например, сенсоры окружающей среды, сенсоры для тела, сенсоры для бытовой техники, сенсоры для транспортных средств и т.д.

Большинство сенсоров требует соединения с агрегатором сенсоров (шлюзом), которые могут реализоваться быть реализованы с использованием локальной вычислительной сети (LAN, Local Area Network), таких как Ethernet и Wi-Fi или персональной сети (PAN, Personal Area Network), таких как ZigBee, Bluetooth и ультраширокополосной беспроводной связи на малых расстояниях (UWB, Ultra-Wide Band). Для сенсоров, которые не требуют подключения к агрегатору, их связь с серверами/приложениями может предоставляться с использованием глобальных беспроводных сетей WAN, таких как GSM, GPRS и LTE [20].

Сенсоры, которые характеризуются низким энергопотреблением и низкой скоростью передачи данных, образуют широко известные беспроводные сенсорные сети (БСС, Wireless Sensor Network). БСС набирают все большую популярность, поскольку они могут содержать гораздо больше сенсоров с поддержкой работы от батарей и охватывают большие площади.

2. *Уровень шлюзов и сетей*

Большой объем данных, создаваемых на первом уровне IoT многочисленными миниатюрными сенсорами, требует надежной и высокопроизводительной проводной или беспроводной сетевой инфраструктуры в качестве транспортной среды. Существующие сети связи, использующие различные протоколы, могут быть использованы для поддержки межмашинных коммуникаций M2M и их приложений. Для реализации широкого спектра услуг и приложений в IoT необходимо обеспечить совместную работу множества сетей различных технологий и протоколов доступа в гетерогенной конфигурации.

Эти сети должны обеспечивать требуемые значения качества передачи информации, и прежде всего по задержке, пропускной способности и безопасности. Данный уровень состоит из конвергентной сетевой инфраструктуры, которая создается путем интеграции разнородных сетей в единую сетевую платформу. Конвергентный абстрактный сетевой уровень в IoT позволяет через соответствующие шлюзы нескольким пользователям использовать ресурсы в одной сети независимо и совместно без ущерба для конфиденциальности, безопасности и производительности.

3. *Сервисный уровень*

Сервисный уровень содержит набор информационных услуг, призванных автоматизировать технологические и бизнес операции в IoT: поддержки операционной и бизнес деятельности (OSS/BSS, Operation Support System/Business Support System), различной аналитической обработки информации (статистической, интеллектуального анализа данных и текстов, прогностическая аналитика и др.), хранения данных, обеспечения информационной безопасности, управления бизнес-правилами (BRM, Business Rule Management), управления бизнес-процессами (BPM, Business Process Management) и др.

4. *Уровень приложений*

На четвертом уровне архитектуры IoT существуют различные типы приложений для соответствующих промышленных секторов и сфер деятельности (энергетика, транспорт, торговля, медицина, образование и др.). Приложения могут быть «вертикальными», когда они являются специфическими для конкретной отрасли

промышленности, а также «горизонтальными», (например, управление автопарком, отслеживание активов и др.), которые могут использоваться в различных секторах экономики.

3.2. Способы взаимодействия с интернет-вещами

Используются три способа взаимодействия с интернет-вещами:

1) прямой доступ;
2) доступ через шлюз;
3) доступ через сервер.

В случае прямого доступа интернет-вещи должны иметь собственный IP-адрес или сетевой псевдоним, по которому к ним можно обратиться из любого клиентского приложения и они должны выполнять функции веб-сервера. Интерфейс с такими вещами обычно выполнен в виде web-ресурса с графическим интерфейсом для управления посредством веб-браузера. Возможно использование специализированного программного обеспечения [26].

В такие веб-устройства должен быть интегрирован прикладной программный интерфейс RESTful API для прямого доступа к ним через Интернет. Соответствующая архитектура WEB of Things (WoT) показана на рис. 3.2. Каждое устройство имеет собственный IP-адрес, работает как веб-сервер и использует интерфейс RESTful API для реализации веб-приложения, объединяющего данные из нескольких источников в один интегрированный сервис. При таком объединении получается новый уникальный веб-сервис, изначально не предлагаемый ни одним из источников данных.

Недостатками такого способа являются:

- необходимость иметь фиксированный адрес в сети, что зависит от провайдера услуги связи с Интернетом таких вещей; другим выходом из ситуации является использование сетевого псевдонима IP-адреса (alias), что требует постоянного обращения интернет-вещи к специальному серверу с запросом об обновлении сетевого адреса по псевдониму;
- лимит подключений к устройству - вызвано низким качеством связи интернет-вещей, а также их слабыми

вычислительными ресурсами. Такая проблема решается путем включения в состав интернет-вещи высокопроизводительного оборудования и подключения вещей к стабильному источнику связи с Интернетом. Это вызывает необходимость в большем потреблении энергии такой вещью и часто вынуждает делать такие вещи стационарными, питающимися от постоянных источников электроэнергии.

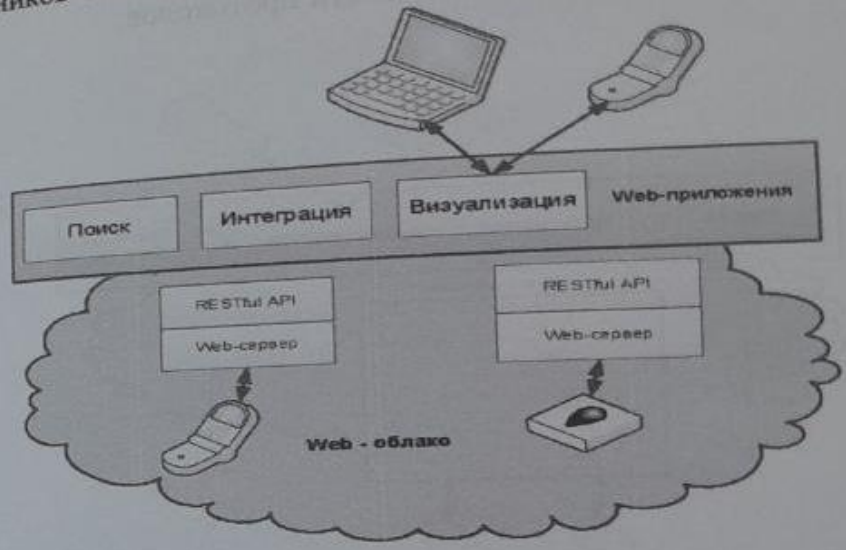


Рис. 3.2. Прямой доступ к IP-устройствам через API

Если интерент-вещи не имеют встроенной поддержки протоколов IP и HTTP, а поддерживают частные протоколы, например Bluetooth или ZigBee, то для взаимодействия с ними можно использовать специальный Интернет-шлюз (рис. 3.3). Он является веб-сервером, который через интерфейс REST-API взаимодействует с IP-устройствами, и преобразует поступающие от них запросы в запрос к специфическому API устройства, подключенного к этому шлюзу. Основное преимущество использования Интернет шлюза в том, что он может поддерживать несколько типов устройств, использующих собственные протоколы для связи [26].

Доступ к интернет-вещам через шлюз является более рациональным способом организации взаимодействия и

полностью вытесняет метод прямого доступа в случае необходимости организации связи беспроводных сенсорных сетей или сети Интернет-вещей с глобальной сетью Интернет. Большинство стандартов беспроводных сенсорных сетей не поддерживают протокол IP, используя собственные протоколы взаимодействия. Такая особенность вызывает необходимость наличия устройства для ретрансляции сообщений из сенсорной сети в сеть Интернет для совместимости протоколов.

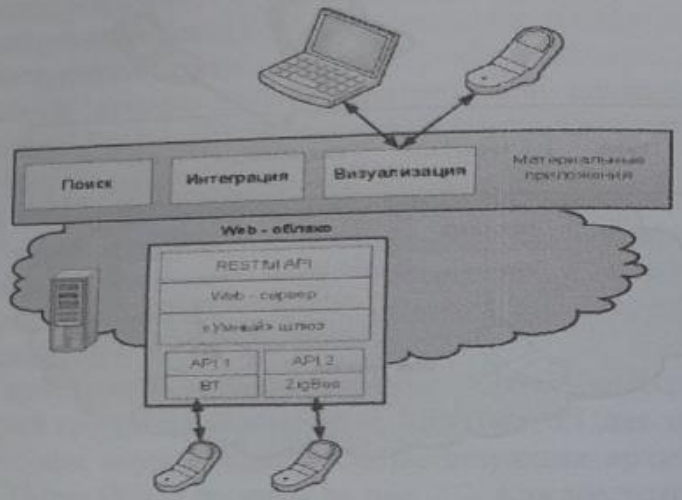


Рис. 3.3. Доступ к не IP-устройствам через интеллектуальный шлюз

Недостатки такого подхода те же, что и в случае прямого доступа, но распространяются они уже на шлюз.

Третья форма взаимодействия устройств в IoT через сервер подразумевает наличие посредника между интернет-вещами и пользователем и может быть реализована с помощью посреднической платформы данных. Данный подход предполагает наличие централизованного сервера или группы серверов, в основные функции которых входит:

- приём сообщений от интернет-вещей и передача их пользователям;
- хранение принятой информации и её обработка;

- обеспечение пользовательского интерфейса с возможностью двустороннего обмена между пользователем и интернет-вещью.

Основной целью использования посреднических платформ данных является упрощение поиска, контроля, визуализации и обмена данными с разными «вещами». В основе данного подхода лежит централизованное хранилище данных. Каждое устройство, имеющее доступ в сеть Интернет (прямой или через интернет-шлюз), должно быть зарегистрировано в системе, прежде чем оно сможет начать передачу данных. При этом существенно снижаются требования к производительности устройств, так как от них не требуется выполнение функций web-сервера. Набор инструментов, предоставляемых платформами, существенно упрощает разработку новых приложений для взаимодействия и управления объектами WoT.

Такой способ доступа является наиболее рациональным и часто используемым, поскольку позволяет перенести нагрузку обработки запросов пользователей с интернет-вещей на централизованный сервер, тем самым разгружая слабый радиоканал связи интернет-вещей, перенося нагрузку на проводные каналы связи между сервером и пользователями.

Метод централизованного сервера также предоставляет надёжные средства хранения и обработки информации, позволяет интернет-вещам взаимодействовать друг с другом и пользоваться облачными вычислениями. Данный подход может использовать также метод шлюза для соединения локальных беспроводных сетей с сервером.

В Интернете вещей шлюз используется не только для прямой связи интернет-вещей с пользователем, но и при использовании централизованного сервера. Шлюзы служат средством для объединения локальных сетей интернет-вещей с глобальной сетью и связью с сервером управления или конечным пользователем. Поскольку локальные сети интернет-вещей представляют собой в основном беспроводные сенсорные сети, то шлюзы, используемые в Интернете вещей, аналогичны используемым в территориально-распределённых сенсорных сетях. Существует несколько способов организации шлюзов.

Первый способ заключается в использовании компьютеров, которые имеют точку доступа к глобальной сети Интернет, и

каждая из объединяемых сетей подключена к такому компьютеру. Основными недостатками такого подхода являются стоимость и громоздкость. Сенсорные сети состоят из миниатюрных датчиков и должны работать автономно, однако территориально-распределённая сенсорная сеть при таком подходе теряет свойство автономности, поскольку теперь она зависит от наличия электричества и точки доступа в Интернет на компьютере.

Второй способ заключается в использовании устройства-шлюза, позволяющего соединить сенсорную сеть с ближайшей проводной сетью, имеющей выход в Интернет. Такой проводной сетью, как правило, является Ethernet-сеть. Устройство имеет в себе приёмопередатчик, совместимый с объединяемой сенсорной сетью, порт для подключения к сети Ethernet и микроконтроллер, выполняющий функции преобразования пакетов одной сети в формат другой. Такой способ отличается меньшей стоимостью, чем первый и размер такого устройства небольшой, но оно нуждается в относительно высоком энергопотреблении из-за того, что стандартные проводные сети не рассчитаны на низкий уровень сигнала и потребления энергии. Также такое устройство не может гарантировать наличие точки доступа в ближайшей проводной сети.

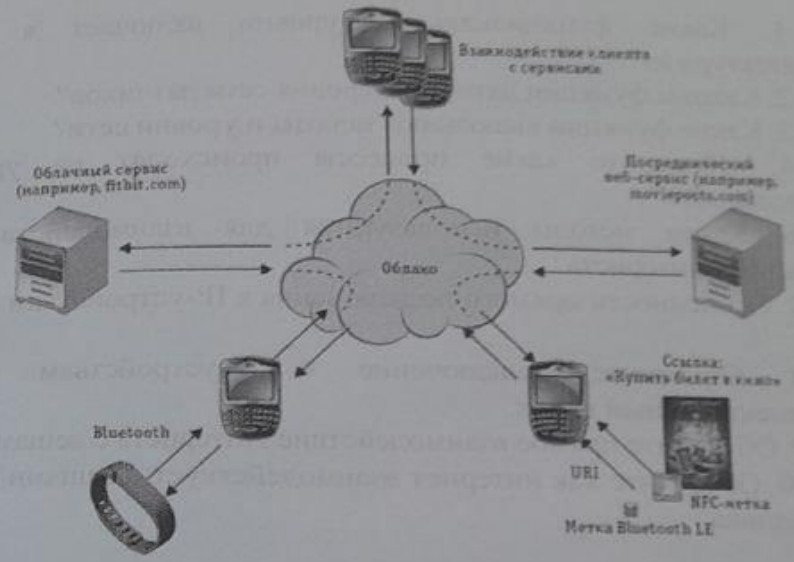
Третий способ заключается в использовании устройства-шлюза, которое является полностью автономным и само предоставляет точку доступа к сети Интернет. Это возможно при использовании беспроводных технологий передачи данных. Устройство состоит из одного приёмопередатчика, совместимого с сенсорной сетью и второго - совместимого с той или иной глобальной беспроводной сетью, в область действия которой попадает сенсорная сеть. Такими сетями могут служить GSM или WiMAX. Использование сети GSM является более экономичным в плане энергопотребления.

Существуют также шлюзы, предоставляющие доступ сенсорным сетям к ближайшим сетям Wi-Fi для поиска точки доступа к сети интернет.

Таким образом, если необходимо организовать полностью автономную территориально-распределённую сенсорную сеть, то следует использовать третий способ. Если же сенсорная сеть используется как часть какой-либо крупной проводной сети, то нет

необходимости в её полной автономности и возможно использование первых двух способов.

На рис 3.4 приведена два способа взаимодействия с Интернетом вещей: а) прямой; б) через посредника.



а) б)

Рис. 3.4. Способы взаимодействия с Интернетом вещей: а) прямой; б) через посредника

При прямом взаимодействии смартфон может опрашивать состояние устройства вблизи себя, и выполнит роль моста между низкоуровневыми одноранговыми протоколами, такими как Bluetooth или Wi-Fi, и протоколами Интернета вроде HTTP и TCP. Один из примеров - фитнес-трекер, который загружает число пройденных шагов через смартфон пользователя по 4G-сети в него облачный аккаунт.

Через веб-сервис на своих смартфонах мобильные пользователи, находящиеся поблизости от объекта Интернета вещей, могут поискать связанную с ним информацию, опубликованную заинтересованными сторонами, например, постер кинофильма, который позволяет проходящим мимо него

людям автоматически обратиться к веб-странице картины и купить электронные билеты.

Контрольные вопросы

1. Какие функциональные уровни включает в себя архитектура IoT.
2. Каковы функции датчика и уровня сети датчиков?
3. Какие функции выполняют шлюзы и уровни сети?
4. Объясните какие процессы происходят на уровне приложений?
6. Какие методы используются для взаимодействия с объектами интернета?
7. Особенности прямого подключения к IP-устройствам через API.
8. Объясните подключение к IP-устройствам через интеллектуальный шлюз.
9. Объясните прямое взаимодействие Интернета с вещами.
10. Объясните как интернет взаимодействует с вещами через посредника?

Глава 4. ВЗАИМОДЕЙСТВИЕ IoT С ПЕРСПЕКТИВНЫМИ ИНФОКОММУНИКАЦИОННЫМИ ТЕХНОЛОГИЯМИ

4.1. Взаимодействие IoT с перспективными инфокоммуникационными технологиями

Так как базовые составляющие Интернета вещей, такие как беспроводные сенсорные сети (Wireless Sensor Network, БСС), коммуникации малого радиуса действия (NFC, Near Field Communication) и межмашинные коммуникации (M2M, Machine-to-Machine), уже прошли пик завышенных ожиданий и находятся на третьем этапе - избавления от иллюзий, для того чтобы концепция IoT получила стабильное развитие в будущем, необходима ее практическая востребованность. А это случиться, если Интернет вещей продемонстрирует на практике новые, более широкие возможности коммуникаций любых вещей в различных областях человеческой деятельности [3].

На рис. 4.1 приведен цикл зрелости для технологий, составляющих основу IoT.

Важную роль в становлении и успешном внедрении Интернета вещей играют различные перспективные инфокоммуникационные технологии, такие как большие данные, облачные технологии и повсеместная компьютеризация, с которыми IoT активно взаимодействует. Эволюция Интернета вещей и сопутствующих инфокоммуникационных технологий на ближайшую перспективу показана на рис. 4.2. В настоящее время IoT находит свое практическое воплощение в основном в виде систем M2M, в ближайшей перспективе на базе чипсетов с ультранизким энергопотреблением и миниатюрных RFID-меток будут созданы интегральные сенсорные сети, а затем и когнитивные сети («умные» сети на основе знаний) [9].

Большие данные (Big Data)

До начала XX века объем знаний удваивался каждое столетие, сегодня объем знаний человечества удваивается каждые 2-3 года. 70% всей доступной информации появилось после изобретения Интернета. Интернет вещей радикальным образом увеличивает объем собираемых данных, что является следствием огромного количества источников информации (прежде всего различные

сенсоры). Гигантские сенсорные сети уже сейчас производят огромные потоки данных, которые надо уметь не только хранить, но и обрабатывать, делать по ним выводы, принимать решения - и все это с учетом неточности как оригинальных данных, так и процедур обработки [27].

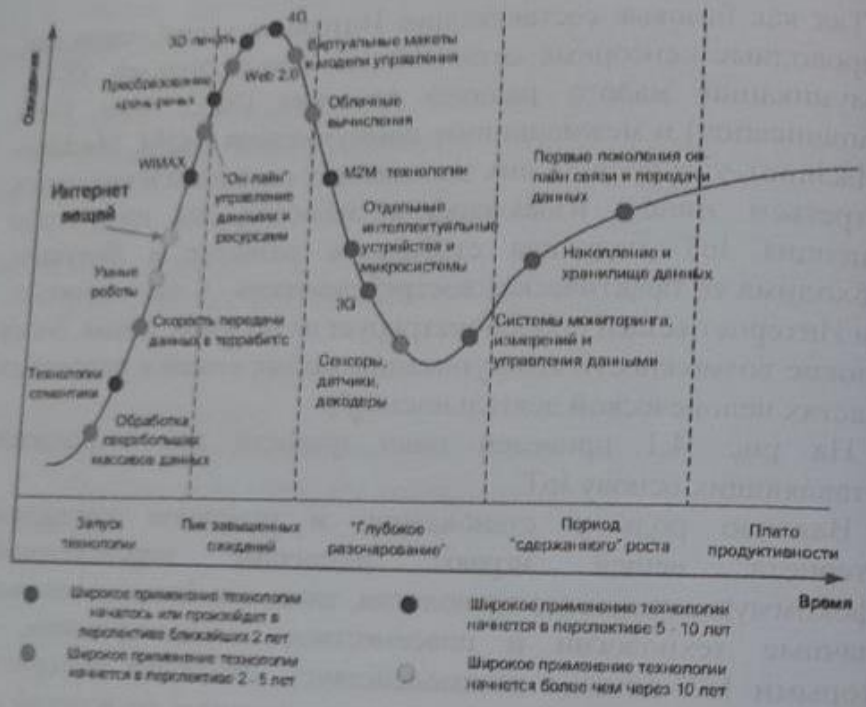


Рис. 4.1. Цикл зрелости технологий IoT

В конце 2000-х годов для обработки большого объема данных сформировался подход, который называется «большие данные» (англ. Big Data) - это серия инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения необходимых результатов обработки.

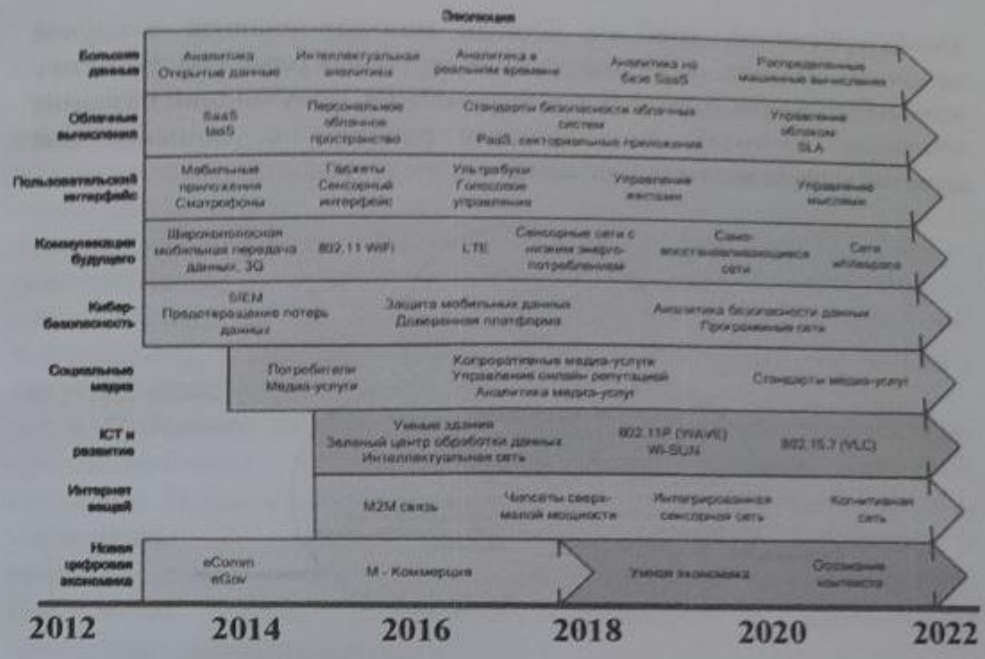


Рис. 4.2. Эволюция Интернета вещей и сопутствующих инфокоммуникационных технологий

В качестве определяющих характеристик для больших данных отмечают «три V»: объём (англ. volume, в смысле величины физического объёма), скорость (англ. Velocity, в смыслах как скорости прироста, так и необходимости высокоскоростной обработки и получения результатов), многообразие (англ. variety, в смысле возможности одновременной обработки различных типов структурированных и неструктурированных данных) (рис. 4.3) [27].

Основное отличие больших данных от «обычных» заключается в том, что эти данные невозможно обработать традиционными системами управления базами данных (СУБД) и решениями класса Business Intelligence из-за их большого объема и разнообразного состава. Другое важное их свойство - феноменальное ускорение накопления данных и постоянное изменение. Такие популярные задачи, как сведение данных, полученных из разных источников (Data Cleaning, Data Merging,

De-deduplication), требуют особых методов анализа в случае неточных данных, особенно данных огромных размеров. В связи с этим и был разработан набор инструментов, получивший название «большие данные», позволяющих работать с данными вне зависимости от их типа и объема.

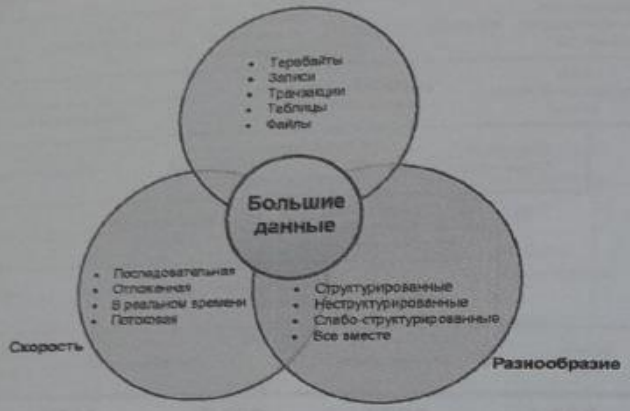


Рис. 4.3. Три основные характеристики больших данных

Прогнозируется, что внедрение технологий больших данных наибольшее влияние окажет на информационные технологии в производстве, здравоохранении, торговле, государственном управлении, а также в сферах и отраслях, где регистрируются индивидуальные перемещения ресурсов и где потенциально могут быть использованы технологии Интернета вещей.

Облачные вычисления (Cloud Computing)

Так как Интернет вещей порождает «большие данные», поэтому возникает закономерный вопрос: где их хранить и чем обрабатывать? Ответом этот вопрос является инфокоммуникационная технология - *облачные вычисления* (CC, Cloud Computing). Облачные вычисления подразумевают аренду услуг и ресурсов для хранения и обработки данных в глобальной сети вместо собственной инфраструктуры. У систем CC должны быть пять основных характеристик: самообслуживание по требованию, широкополосный сетевой доступ, пул ресурсов, возможность быстрой перенастройки или расширения и измеряемое обслуживание.

Существуют следующие модели развёртывания облачной инфраструктуры (так называемых «облаков»):

1. *Частное облако* (англ. private cloud) - инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации, как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

2. *Публичное облако* (англ. public cloud) - инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца - поставщика услуг.

3. *Гибридное облако* (англ. hybrid cloud) - это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений.

4. *Общественное облако* (англ. community cloud) - вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики, и соответствия различным требованиям). Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Различные услуги *облачных вычислений*, обозначаемые в общем случае как XaaS (X as a Service), можно отнести к трем основным классам (рис. 4.4):

- «инфраструктура, как услуга» (IaaS, Infrastructure as a Service) - аренда мощности серверов и емкости систем хранения

центров обработки данных (ЦОД);

- «программное обеспечение, как услуга» (SaaS, Software as a Service) - аренда программного обеспечения (ПО), которое запускается «из облака»;

- «платформа, как услуга» (PaaS, Platform as a Service) - аренда платформы разработки ПО коллективными или индивидуальными разработчиками.

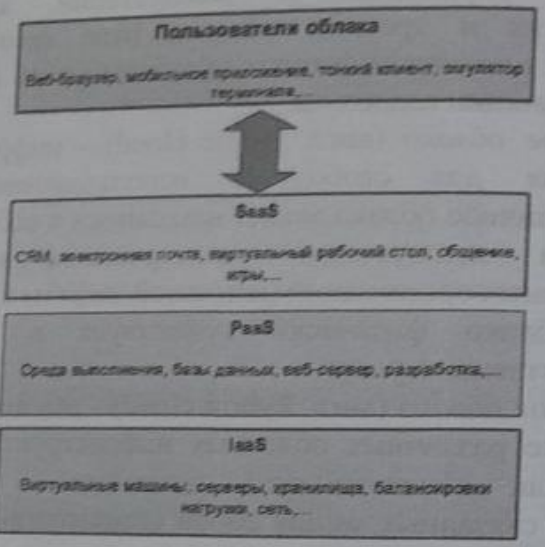


Рис. 4.4. Классы услуг облачных вычислений

Все остальные услуги систем *облачных вычислений* (например, BPaaS - «бизнес-процесс, как услуга» или VSaaS - «видеонаблюдение, как услуга»), можно, так или иначе, отнести к трем вышеуказанным классам облачных услуг.

Для работы технологий Интернета вещей можно использовать и *туманные вычисления* (Fog Computing). Под «туманом» подразумевается приближение «облака» к земле, в данном случае «туман» — это разновидность облачных сервисов, расположенных не где-то в недоступных высотах, а в окружающей нас среде. Иначе говоря, Fog Computing не альтернатива, а дополнение к Cloud Computing, и могут возникнуть ситуации их совместного действия (например, выполнение аналитического приложения), и в таком случае Cloud окажет услугу Fog.

Туманные вычисления дополняют облачные вычисления и обеспечивают взаимодействие умных вещей между собой и облачными ЦОД в виде трехуровневой иерархической структуры. Верхний уровень занимают тысячи облачных ЦОД, предоставляющих ресурсы, необходимые для выполнения серьезных, например аналитических, программных приложений IoT. Уровнем ниже располагаются десятки тысяч распределенных управляющих ЦОД, в которых содержится «интеллект» Fog Computing, а на нижнем уровне находятся миллионы вычислительных устройств умных вещей [27].

Fog Computing можно определить как в максимальной степени виртуализированную платформу, поддерживающую три основных типа сервисов, образующих межмашинные коммуникации M2M: вычисления, хранение и сеть. Задача Fog Computing заключается в обеспечении взаимодействия миллиардов устройств между собой и с облачными центрами обработки данных (ЦОД).

Парадигма Fog Computing отличается от Cloud Computing по целому ряду параметров.

1. *Распределение вычислительной мощности и реальное время.*

Значительные вычислительные ресурсы могут быть размещены на периферии сети, причем не должно быть зависимости от координат того места, где находится устройство, и при этом работа в режиме реального времени предполагает низкий уровень задержек при обмене данными, к тому же в Fog Computing может произойти конвергенция двух существовавших долгое время автономно друг от друга систем - управления бизнесом и технологическими системами.

2. *Географическое распределение компонентов.*

Модель распределения сервисов в Fog Computing менее централизована, чем для облаков, а отдельные устройства могут быть связаны между собой потоками данных и предоставлять друг другу «тяжелые» сервисы.

3. *Большой объем внешних данных.*

Устройства, экипированные многочисленными сенсорами, могут в реальном времени генерировать гигантские объемы данных.

4. *Сложная топология.*

Миллионы географически распределенных узлов могут создавать разнообразные и не детерминированные заранее связи.

5. Мобильность и гетерогенность.

Мобильность устройств потребует использования альтернативных протоколов, например протокола маршрутизации LISP (Locator/ID Separation Protocol), который позволяет разделить функциональность IP-адресов на две части: идентификаторы хостов и локаторы маршрутизации. Концепция предусматривает установку туннельных маршрутизаторов, которые будут добавлять LISP-заголовки в информационные пакеты по мере их движения по сети.

Повсеместная компьютеризация (Ubiquitous Computing)

Повсеместный (вездесущий, всепроникающий, тотальный) компьютинг, фигурирующий в специальной литературе под терминами «ubiquitous computing» и «pervasive computing», попросту означает создание вездесущих интеллектуальных информационных систем, помогающих в ежедневной человеческой рутине - дома, в офисе, в больнице, на работе, в дороге (рис. 4.5).

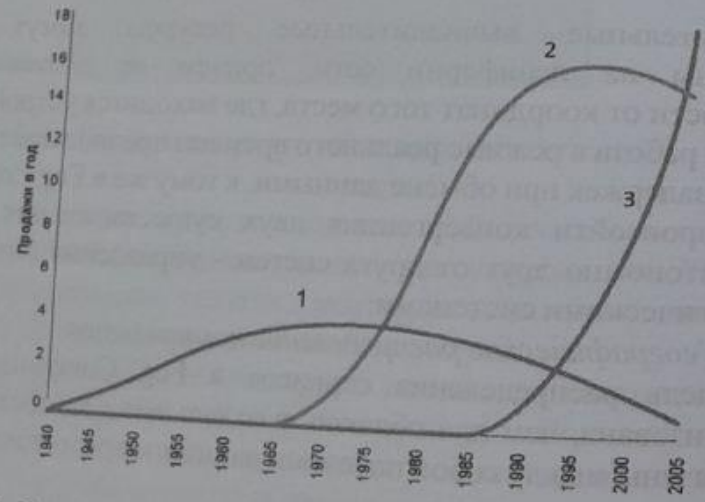


Рис. 4.5. Эволюция вычислительных систем: мейнфреймы (кривая 1) - один компьютер, много пользователей; персональные компьютеры (кривая 2) – один компьютер, один пользователь; повсеместный компьютинг (кривая 3) – один пользователь, много компьютеров

Можно выделить четыре основные характеристики тотального компьютинга:

1) *эффективное использование персонального умного пространства,* имея в виду окружающие нас на работе, в транспорте, дома устройства с компьютерным управлением, необходимыми датчиками и исполнительными механизмами;

2) *невидимость* (умного пространства) - минимальное отвлечение внимания пользователя на управление окружающими вещами;

3) *местная масштабируемость* - любая точка персонального умного пространства должна быть сделана настолько вычислительно "мощной", насколько это необходимо пользователю;

4) *маскирование неоднородностей* - под неоднородностью понимаются различия как в техническом плане (называемые, обычно, гетерогенностью), так и не технические - организационные структуры, бизнес-процессы, экономические факторы.

К этому можно еще добавить знание контекста, т.е. пользователь существует в персональном умном пространстве не "вслепую", а представляя себе, сознавая контекст.

4.2. IoT и технологии 5G

Сегодня мир находится в преддверии новой технологической революции в беспроводных сетях. Запуск пятого поколения сотовой связи (fifth generation, или 5G) тесно связан с развитием не мене прорывного явления последних лет - Интернета вещей (IoT). Обе эти концепции способны кардинально изменить бизнес и социум, предоставив им уникальные возможности взаимодействия «умных» устройств [28].

В ближайшее время ожидается, что в сетях мобильной связи 3,5 млрд IoT-подключений и 20% мирового мобильного трафика данных придется на сети 5G в 2023 году.

IoT способен совершить революционные изменения в бизнесе, социуме и системе управления практически любыми технологическими процессами. Интернет вещей, свяжет в одну глобальную систему всех, кто причастен к изготовлению и

использованию «умного» оборудования. Однако на пути к этому пока что есть немало препятствий. Одной из них является недостаточность сетевой емкости, что не позволяет использовать все возможности IoT.

Прорыв в этом вопросе может дать новое поколения мобильной связи - 5G. Главное ее отличие от предыдущих - огромная (свыше 10 Гбит/с) скорость передачи данных, а соответственно, и отклика. Задержка сигнала в 5G будет снижена всего до 1 мс, притом, что в 4G она составляет 10 мс, а в 3G - все 100 мс.

Но в контексте использования 5G IoT-устройствами скорость, все же, не является определяющим фактором. На первое место здесь выходит надежность сети, минимальная задержка сигнала и возможность массового подключения различных «умных» устройств со своими конкретными задачами и бесперебойность их взаимодействия.

Для повышения качества обслуживания своих пользователей гетерогенные беспроводные сети все более тесно интегрируют между собой существующие, а также перспективные технологии радиодоступа, что приводит к возникновению принципиально новых научно-технических задач. Помимо услуг мобильного доступа, которые предполагают передачу разнородного пользовательского трафика, гетерогенные сети 5G обеспечат поддержку множества приложений Интернета вещей, основанных на принципе межмашинного взаимодействия, а также реализуют технологии программно-определяемых сетей и облачных вычислений.

Необходим комплексный подход, учитывающий основные особенности современного этапа развития гетерогенных беспроводных систем мобильного доступа, такие как высокая плотность размещения пользовательских устройств и узлов сетевой инфраструктуры, тесная интеграция разнородных технологий радиодоступа и использование прямых соединений между устройствами, а также применение крайне высоких частот и обеспечение поддержки приложений Интернета вещей с учетом особенностей носимых устройств.

Сети 5G представляют собой архитектуру систем беспроводного доступа (рис. 4.6), основанную на использовании

различных малых сот и предназначенную для удовлетворения новых требований по емкости и качеству покрытия сети.

Рис. 4.6. Особенности гетерогенных сетей 5G

Соответственно, базовая станция макросети служит для обеспечения сетевого подключения и поддержки мобильности терминалов на обширных площадях, тогда как недорогие малые соты применяются для повышения качества и емкости сотового покрытия. Мобильные устройства, снабженные возможностями для установления прямого соединения [28], могут также рассматриваться в качестве одного из слоев в рамках такой иерархической гетерогенной структуры.

Возрастающая распространенность мультимедиа-приложений и сервисов, порождающих объемные потоки данных, а также более высокая сложность конструкции абонентских терминалов, поддерживающих несколько технологий радиодоступа, в совокупности приводят к значительному энергопотреблению пользовательских устройств. Более того, существует целый ряд сценариев, включающих в себя широкое множество приложений Интернета вещей, в которых тысячи устройств подключаются к одной и той же соте, где высокая энергетическая эффективность работы оконечного оборудования является определяющей.

По мере того как технологии 5G готовятся к обслуживанию многочисленных IoT-приложений с повышенными требованиями [28], возникает все более существенное различие между потребительскими и индустриальными сценариями их работы.

Действительно, потребительский сегмент Интернета вещей развивался уже значительное время (например, в области автоматизации домашнего хозяйства) с целью улучшения качества жизни людей и общества в целом. При этом индустриальный сегмент Интернета вещей представляет собой относительно недавнее направление, нацеленное на улучшение бизнес-связей между предприятиями.

При помощи средств связи 5G промышленные пользователи стремятся достичь повсеместного и надежного взаимодействия, превышающего возможности технологий 4G по обеспечению мобильного широкополосного доступа (рис. 4.7). Однако множеству индустриальных сценариев IoT присущи такие требования, которые не могут быть удовлетворены имеющимися сетями 3G и 4G, например, в системах контроля промышленного производства и обеспечения безопасности дорожного транспорта, при взаимодействии между машинами и их операторами, в сферах материально-технического снабжения и отслеживания перемещения объектов, а также в автомобилестроении, энергетике и т.д.

Как отмечалось выше, ограничения по емкости и качеству соединения в мобильных сетях по сравнению с требованиями 5G обусловливают необходимость более тесной интеграции сотовых и локальных сетей доступа.

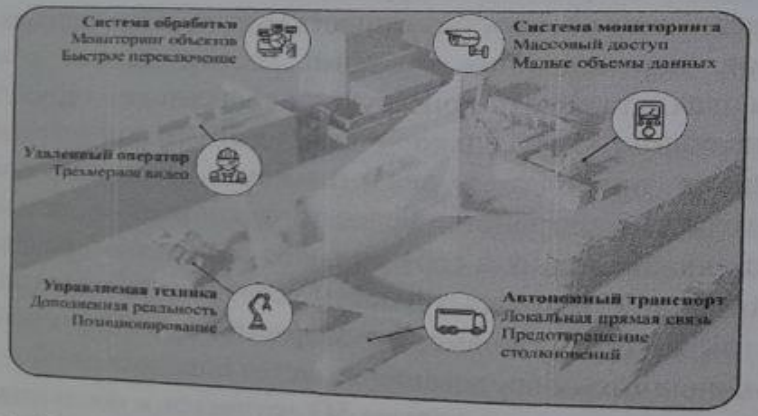


Рис. 4.7. Примеры 5G-приложений Индустриального Интернета для автоматизации производства

На рис. 4.8 схематически показана современная гетерогенная сеть HetNet сотового оператора. Система HetNet включает в себя иерархическую структуру сот различного размера, включая макросоты для обеспечения бесшовного покрытия, базового доступа и мобильности, а также различные малые соты (пикосоты, фемтосоты, точки доступа WiFi, совмещенные LTE-WiFi модули и др.).

Соответствующее оборудование доступа имеет более низкую мощность передачи и стоимость, позволяя повысить емкость системы за счет сокращения расстояния между сетевой инфраструктурой и абонентом в областях с высокой потребностью в обслуживании.

Последующее изложение сосредоточено на рассмотрении различных вариантов интеграции сетей LTE и Wi-Fi как показано на рис. 4.9. Данные опции отличаются, прежде всего, специфичными механизмами обеспечения взаимодействия технологий радиодоступа, включающими в себя обнаружение радиотехнологии, ее выбор или назначение, управление радиоресурсами RRM, обеспечение мобильности и перенаправления потока данных между технологиями радиодоступа и т.д.

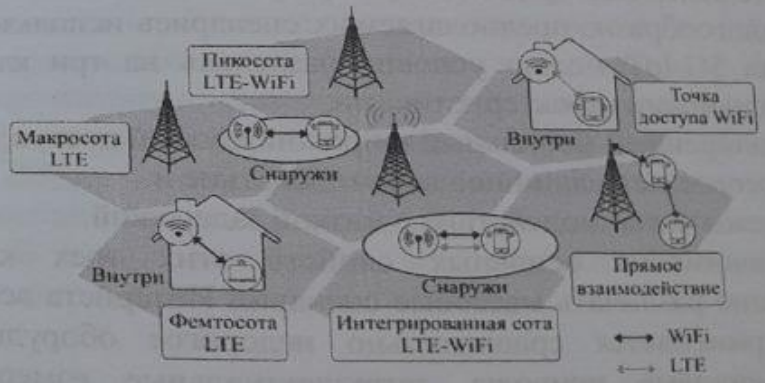


Рис. 4.8. Топология типовой гетерогенной сети

Интеграция на прикладном уровне.

На рис. 4.8 Вариант A соответствует архитектуре гетерогенной сети, которая подразумевает интеграцию на

прикладном уровне. Соответственно, предполагается наличие специализированного интерфейса верхнего уровня, который позволяет абонентскому терминалу взаимодействовать напрямую с поставщиком услуги, обмениваясь информацией по различным технологиям радиодоступа [28].

Интеграция на уровне ядра сети

Вариант Б облегчает интеграцию сотовых и WLAN систем при помощи взаимодействия на уровне опорной сети. Соответственно, механизм обнаружения и выбора сети доступа ANDSF обеспечивает выявление подходящих точек доступа WiFi, а также может задавать рекомендации по выбору сети [28].

Интеграция на уровне сети радиодоступа

Вариант В описывает передовую архитектуру гетерогенной системы связи, которая интегрирует технологии 3GPP и WLAN на уровне сети радиодоступа RAN. Данная опция предполагает, что содействие со стороны абонентского терминала позволяет упростить обмен информацией между сотовой и локальной сетью доступа, что может потребовать создания соответствующих управляющих интерфейсов. Доступные в этом случае возможности по взаимодействию на уровне RAN ограничены емкостью транзитных (backhaul) каналов между различными сотами и технологиями радиодоступа [28].

Всё многообразие предполагаемых сценариев использования технологии 5G-IoT можно условно разделить на три класса с крайне различными характеристиками:

(1) расширенный мобильный широкополосный доступ;

(2) массовое межмашинное взаимодействие и

(3) надежное взаимодействие с низкой задержкой.

Для понимания основных свойств этих трех классов целесообразно различать массовые сценарии Интернета вещей, в которых применяется сравнительно недорогое оборудование (сенсоры, силовые приводы, интеллектуальные измерители, носимые устройства и т.д.), и критические его сценарии, использующие существенно более сложные решения (например, подключенные автомобили, мобильные роботы и дроны).

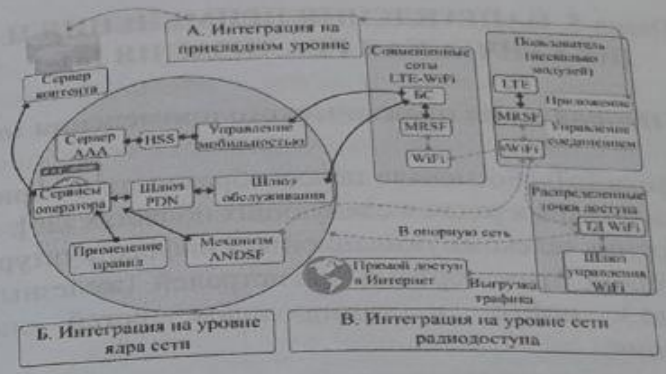


Рис. 4.9. Архитектура гетерогенной сети связи

Контрольные вопросы

1.Объясните эволюцию Интернета вещей и поддерживающих его инфокоммуникационных технологий.

2. Что подразумевается под большими данными (Big Data)? В чем разница между большими данными и «обычными» данными?

3. Что такое «частное облако» (англ. private cloud)?

4. Что такое «общедоступное облако» (англ. public cloud)?

5. Что такое «гибридное облако» (англ. hybrid cloud)?

6. Что такое «облако сообщества» (англ. community cloud)?

7. Перечислите классы сервисов облачных вычислений.

8. Объясните топологию современной интегрированной сети.

9. Дайте и объясните архитектуру интегрированной коммуникационной сети.

10. В чём заключается особенности интегрированных перспективных сетей 5G и IoT.

Глава 5. НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ И ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ IoT

5.1. Направления практического применения IoT

Специфика IoT обосновала целесообразность их применения при решении сложных задач в следующих областях [29]:

- мониторинг телекоммуникационной инфраструктуры сетей;
- мониторинг транспортных магистралей (железных дорог, метро и др.), нефте- и газопроводов, сетей энерго- и теплоснабжения;
- контроль и анализ грузопотока;
- экологический, биологический и медицинский мониторинг;
- жизнеобеспечение и автоматизация систем «умный дом»;
- обнаружение и оповещение о чрезвычайных ситуациях (мониторинг сейсмической активности и вулканической активности для своевременного оповещения о стихийных бедствиях, анализ атмосферы и погоды) и др.

На основе Интернета вещей могут быть реализованы всевозможные «умные» (smart) приложения в различных сферах деятельности и жизни человека (рис. 5.1):

– «Умная планета» - человек сможет буквально «держать руку на пульсе» планеты: своевременно реагировать на упущения в планировании хозяйств, загрязнения и другие экологические проблемы, а значит, эффективно распоряжаться невозобновляемыми ресурсами.

– «Умный город» - городская инфраструктура и сопутствующие муниципальные услуги, такие как образование, здравоохранение, общественная безопасность, ЖКХ, станут более связанными и эффективными.

– «Умный дом» - система будет распознавать конкретные ситуации, происходящие в доме, и реагировать на них соответствующим образом, что обеспечит жильцам безопасность, комфорт и ресурсосбережение.

– «Умная энергетика» - будет обеспечена надежная и качественная передача электрической энергии от источника к приемнику в нужное время и в необходимом количестве.

– «Умный транспорт» - перемещение пассажиров из одной

точки пространства в другую станет удобнее, быстрее и безопаснее.

– «Умная медицина» - врачи и пациенты смогут получить удаленный доступ к дорогостоящему медицинскому оборудованию или к электронной истории болезни в любом месте, будет реализована система удаленного мониторинга здоровья, автоматизирована выдача лекарственных препаратов больным и многое другое.

Рис. 5.1. Умные приложения на основе Интернета вещей

Все больше «умной» электроники входит в нашу жизнь, и мы начинаем жить не просто в окружении «умных» подключенных вещей и устройств, а непосредственно в общей экосистеме - «умных» домах и городах с «умными» транспортными средствами и «умными» заводами и фабриками. Мы и «умные» вещи становимся некой общностью, и от этого уже никуда не уйти, разве что отказавшись от благ цивилизации.

Без IoT невозможны реализация следующих систем:

Носимая электроника (рис. 5.2) - от персональных нательных гаджетов (Smart Wearables, буквально «умная одежда»), мониторов биометрического контроля до ошейников/трекеров,

которые помогают животноводам и владельцам домашних животных находить своих питомцев.

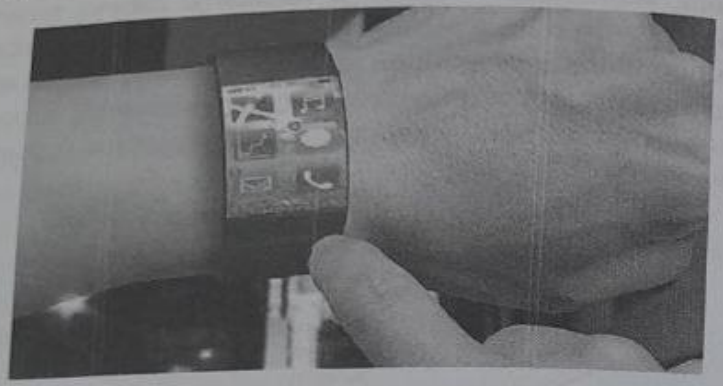


Рис. 5.2. Носимая электроника

«Умный» дом (рис. 5.3), где, наряду с компьютерами, мультимедийными центрами и интеллектуальными телевизорами, используются устройства, которые осуществляют контроль климата в помещении, управление освещением и системой безопасности.

Рис. 5.3. «Умный» дом

«Умный» город (рис. 5.4). IoT предоставляет возможность оперативного и точного учета коммунальных услуг и удобство их оплаты, обеспечивает функционирование систем безопасности

зданий, сбора отходов, уличного освещения, позволяет экономить энергию и увеличивает трафик через адаптивные ограничения скорости и управление светофорами.

«Умное» сельское хозяйство (рис. 5.5). Прежде всего, это «точное земледелие» - «умное» орошение, с анализом влажности почвы и погодных условий, мониторинг состояния посевов, получение метеоданных в реальном времени, а также контроль здоровья, увеличения поголовья и определение местонахождения скота.

Рис. 5.4. «Умный» город

Рис. 5.5. «Умное» сельское хозяйство

Подключенный автомобиль (рис. 5.6). Это новые информационноразвлекательные возможности, обработка и передача данных от систем автомобиля. Технология беспроводной связи между автомобилем (V2V) и автомобильной инфраструктурой (V2I), известная как V2X, позволяет повысить безопасность вождения, уменьшить пробки на дорогах и увеличить пассажиропоток.

Рис. 5.6. Подключенный автомобиль

Медицина (рис. 5.7). IoT позволяет значительно улучшить качество и эффективность медицинских услуг, позволяя работникам системы здравоохранения дистанционно контролировать состояние пациента и получать в реальном времени более точную информацию для диагностики, и в некоторых случаях отказаться от постоянного пребывания пациента в больнице.

Рис. 5.7. Медицина

«Умное» предприятие (рис. 5.8). Наряду с увеличением автоматизации IoT дает возможность создать подключенное роботизированное производство, способное обучаться и обмениваться информацией, организовываясь в высокоэффективные производственные системы, осуществлять предаварийное техобслуживание и производить продукты с гораздо меньшими затратами ресурсов.

Рис. 5.8. «Умное» предприятие

«Умная» энергетика (рис. 5.9). IoT предоставляет инструменты для мониторинга потребления энергии и снижения ее потребления, открывает возможности для более широкого использования преимуществ альтернативных технологий: солнечной, ветровой, волновой, геотермальной и др.

Рис. 5.9. «Умная» энергетика

5.2. Решения на базе IoT технологий

Система определения наличия автомобиля

Рост городов и, как следствие, лавинный рост количества личного транспорта приводят не только к увеличению трафика и пробок на дорогах, но также значительно затрудняет поиск парковочных мест как непосредственно на городских улицах, так и на закрытых парковках (рис. 5.10).

Система контроля за сельскохозяйственными культурами

Отсутствие физической коммуникационной инфраструктуры в сельской местности создает дополнительные ограничения при реализации проектов в сельском хозяйстве. Использование беспроводных технологий с автономными источниками питания позволяет в значительной мере снять эти ограничения.

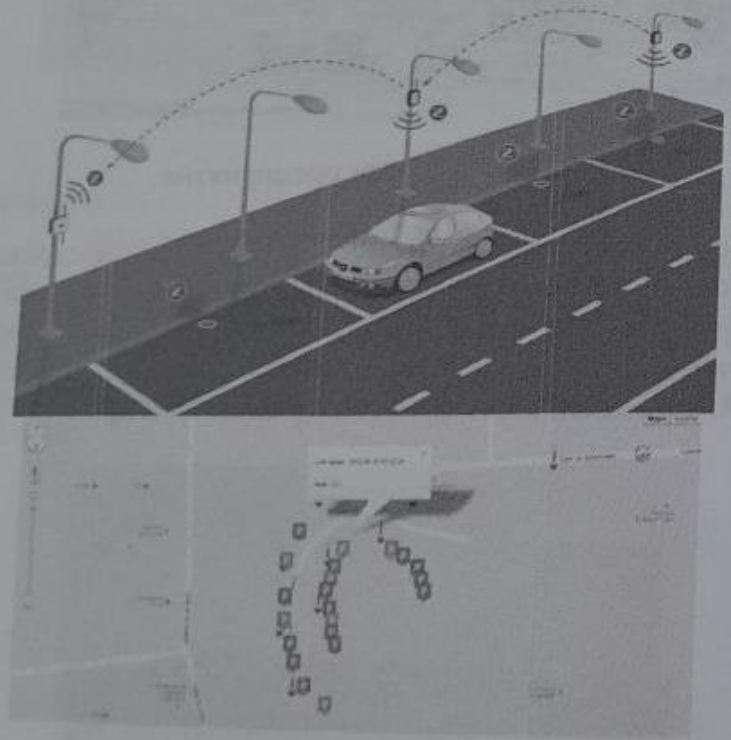


Рис. 5.10. Беспроводное оборудование в системах управления парковками

Набор датчиков: контроль температуры, диаметра стволов и стеблей, уровня солнечной влажности и температуры окружающего воздуха, направления ветра, концентрации удобрений и др. позволяет точно определять моменты необходимости и количества орошения, внесения удобрения, снятия урожая и других организационных мероприятий (рис. 5.11).

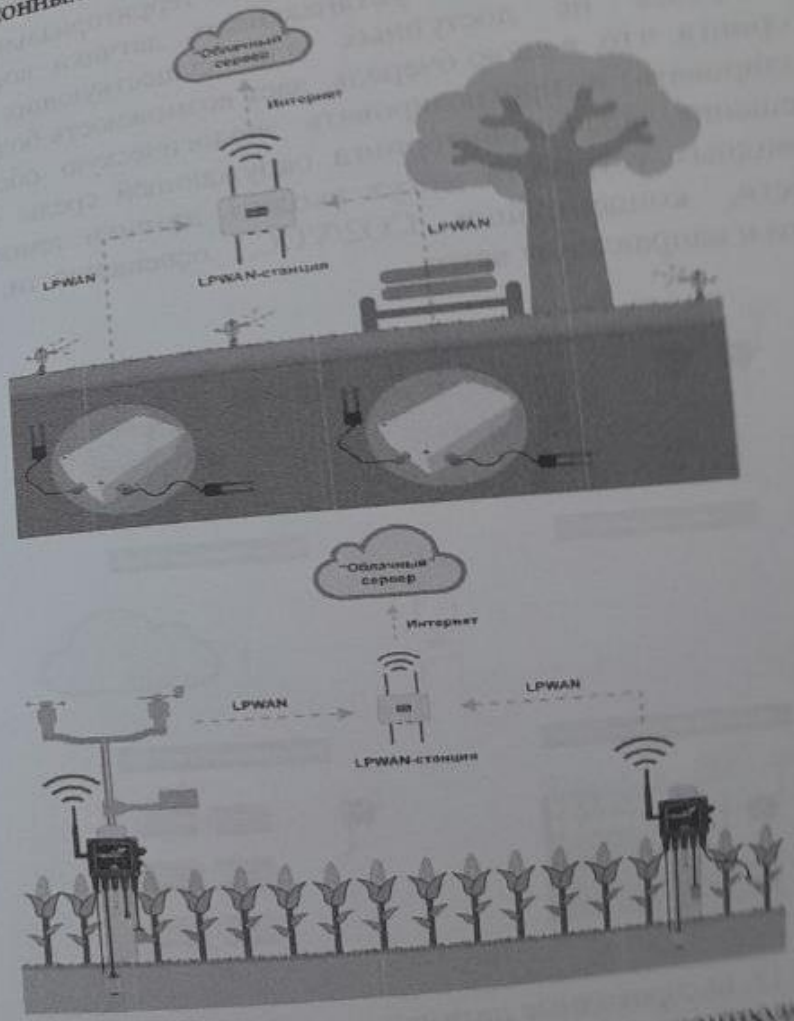


Рис. 5.11. Беспроводные датчики в системах контроля за сельскохозяйственными культурами

Системы мониторинга окружающей среды

Усложняющаяся с каждым годом экологическая ситуация, и, как следствие, ужесточающиеся законодательные и нормативные требования в сфере контроля различного рода загрязнений, приводят к необходимости повсеместного внедрения систем мониторинга окружающей среды (рис.5.12).

Использование для этих целей беспроводных автономных устройств может значительно расширить территориальный охват таких систем и позволит устанавливать датчики контроля в местах, ранее не доступных для существующих систем мониторинга, что, в свою очередь, даст возможность более точно контролировать и прогнозировать экологическую обстановку. Для решения задач мониторинга окружающей среды в состав беспроводных устройств могут входить датчики температуры, влажности, концентрации CO2/VOC, освещенности, шума, скорости и направления ветра.

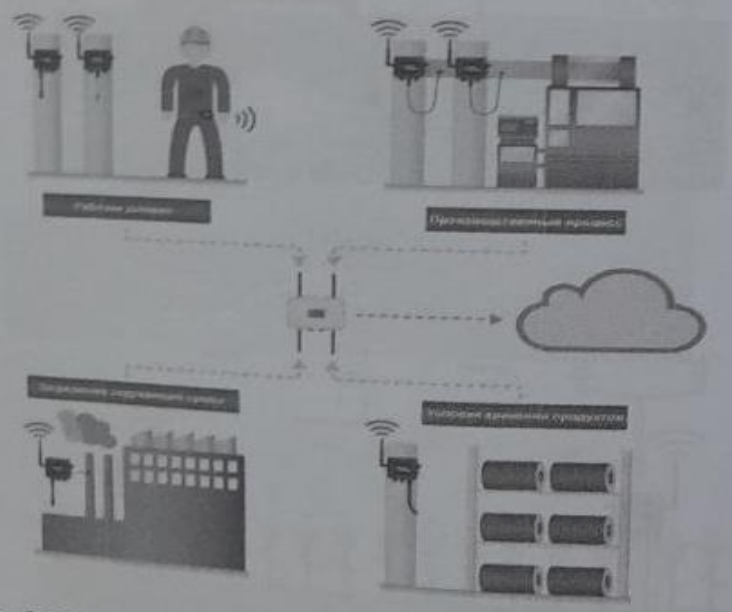


Рис. 5.12. Беспроводные датчики в системах мониторинга окружающей среды

Помимо задач мониторинга окружающей среды аналогичные решения могут быть использованы для контроля состояния рабочих параметров на промышленных предприятиях. Беспроводные решения IoT позволяют значительно расширить возможности контроля данных параметров за счет установки датчиков в местах, в которых размещение проводных датчиков является затруднительным или даже невозможным. Для оперативного контроля рабочих параметров в опасных зонах сотрудники, работающие в таких зонах, могут снабжаться носимыми беспроводными датчиками, которые также могут оснащаться аварийными кнопками обратной связи или системами контроля состояния человека: пульсометрами, датчиками давления и т.п.

Системы обнаружения пожаров

Ежегодные пожары на обширных лесных территориях наносят ощутимый материальный ущерб, приводят к жертвам и становятся причиной экологических катастроф, а предупреждать пожары и, тем более бороться с ними крайне непросто ввиду большой площади лесов и удаленности инфраструктуры (рис.5.13)

Рис. 5.13. Беспроводные системы обнаружения лесных пожаров

Появление беспроводных систем для раннего обнаружения лесных пожаров может приблизить решение данной задачи. Комплексы беспроводных датчиков, которые благодаря технологиям построения mesh-сетей (сетей ячеистой топологии), позволяющим передавать данные как непосредственно на базовую станцию, так и транзитом через ближайшие датчики, дают возможность покрывать такой сетью десятки и сотни километров.

В отдаленных местах, где отсутствует какая-либо возможность передавать данные на базовые станции, подобные комплексы могут применяться в совокупности с системами наблюдения с воздуха, например, с помощью вертолетов, дирижаблей или с помощью автоматических дронов, которые могут осуществлять регулярное патрулирование и собирать данные с изолированных удаленных участков лесного массива.

Мониторинг мостов и сооружений

В настоящее время многие мостовые конструкции и сложные архитектурные сооружения оснащаются системами деформационного мониторинга на стадии проектирования (рис. 5.14). Но большинство мостов, зданий и сооружений не имеют таких систем.

Рис. 5.14. Беспроводные датчики в системах мониторинга мостов

Решение этой задачи может предупредить возможное обрушение этих конструкций, а значит поможет избежать не

только значительного материального ущерба, но и человеческих жертв. Особую сложность в решении проблемы мониторинга представляют сооружения, расположенные вдали от основных коммуникаций связи и энергоснабжения.

Мониторинг трубопроводов

Из-за большой протяженности трубопроводов мониторинг трубопроводных систем, предназначенных для транспортировки воды, газа, нефти и других продуктов, представляет непростую с технической точки зрения задачу, а также требует значительных материальных затрат (рис. 5.14). В тоже время поддержание таких трубопроводных систем в рабочем состоянии, а тем более ремонт и устранение возникающих неисправностей, не менее, если не более затратный. Использование беспроводных датчиков позволяет диагностировать возможные нештатные ситуации на ранней стадии. Помимо этого, автономные беспроводные датчики, не требующие внешнего питания, могут быть расположены по всей длине трассы трубопровода, что позволяет локализовать место повреждения и обеспечить более оперативный выезд ремонтной бригады.

Рис. 5.15. Беспроводные датчики в системах мониторинга трубопроводов

Внедрения сети LoRaWAN в систему ЖКХ небольшого города

На рис. 5.16 представлена пример схемы внедрения сети LoRaWAN в систему ЖКХ небольшого города.

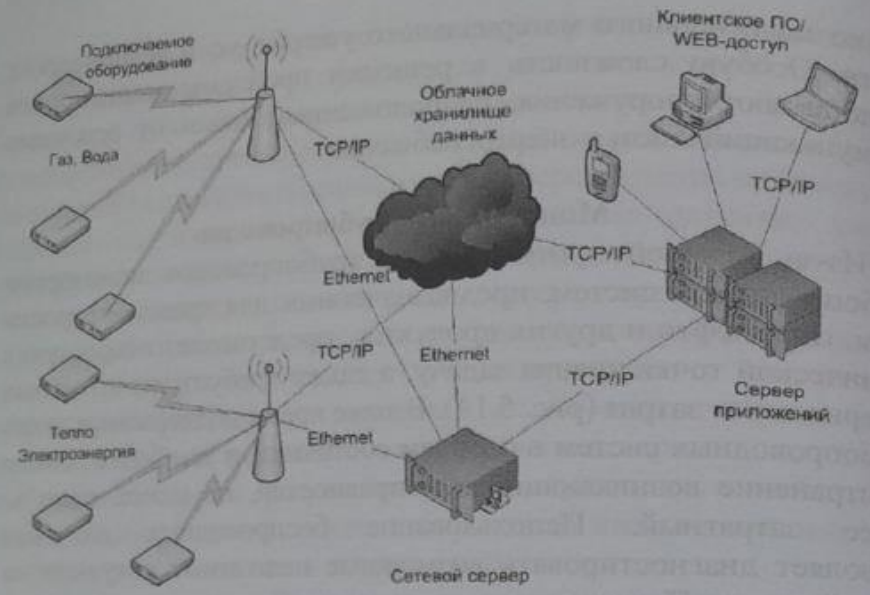


Рис. 5.16. Схема внедрения сети LoRa в систему ЖКХ небольшого города

На схеме показаны счетчики учета газа, воды и электроэнергии, оснащенные радиомодулями LoRa.

Данные счетчики передают информацию по радиоканалу LoRa на базовые станции LoRa. Данные от базовых станций отправляются на сетевой сервер, соединенным по оптическому кабелю. Процесс передачи происходит по протоколу TCP IP. Сетевой сервер управляет всеми базовыми станциями, решает через какой шлюз (базовую станцию) общаться с датчиком (если датчик слышно через несколько шлюзов) и определяет еше ряд важных параметров.

От сетевого сервера пакеты передаются на сервер приложений, где происходит расшифровка показаний от датчиков и они в понятной форме раздаются либо в биллинг, либо в интерфейс потребителю, либо в другое заданное место.

Разработка и внедрение технологии LoRa для узкополосной передачи данных с расширенной зоной покрытия существенно усилила конкуренцию на рынке беспроводных технологий IoT для сотовых технологий, использующих лицензируемые полосы

частот и требующих использования SIM-карт.

В настоящее время LoRa обладает рядом преимуществ по техническим параметрам, использованию нелицензионного спектра, простоте регулирования, отсутствию необходимости получения лицензии на оказание услуг передачи данных. Однако необходимо иметь в виду, что, несмотря на сегодняшний успех, LoRa уже имеет серьезные альтернативы.

Контрольные вопросы

1. Какие «умные» приложения можно внедрить в различные сферы жизни и деятельности человека на основе Интернета вещей?
2. Какие возможности есть в Smart Planet?
3. Какие преимущества дает внедрение «умного города»?
4. Что предусмотрено в «умном доме»?
5. Что предусмотрено в «умной энергетике»?
6. Чего можно добиться в «умном транспорте»?
7. Что предусмотрено в «умной медицине»?
8. Какие устройства относятся к портативной электроникой?
9. Какие преимущества дает «умное сельское хозяйство»?
10. Объясните схему реализации сети IoT LoRaWAN в системе ЖКХ.

Глава 6. ВЕБ ВЕЩЕЙ, ИНТЕРНЕТ НАНО-ВЕЩЕЙ И КОГНИТИВНЫЙ ИНТЕРНЕТ ВЕЩЕЙ

6.1. Веб вещей (WoT)

Составной частью Интернета вещей является Веб вещей (WEB of Things, WoT), который обеспечивает взаимодействие различных интеллектуальных объектов («вещей») с использованием стандартов и механизмов Интернет, таких как унифицированный (единообразный) идентификатор ресурса URI (Uniform Resource Identifier), протокол передачи гипертекста HTTP (HyperText Transfer Protocol), стиль построения архитектуры распределенного приложения REST (Representational State Transfer) и др. [11].

Фактически WoT предусматривает реализацию концепции IoT на прикладном уровне с использованием уже существующих архитектурных решений, ориентированных на разработку web - приложений. Другими словами данные с умных вещей или управление ими должно быть доступно через WWW-страницы. На рис. 6.1 показан пример, как используя специальную страницу в интернет через браузер можно считать данные с датчика света в беспроводной сенсорной сети или изменить цвет четвертого индикатора в сенсоре.

Основные свойства WoT:

1. Использует протокол HTTP в качестве приложения, а не в качестве транспортного механизма передачи данных, как он применяется для традиционных WWW-услуг.

2. Обеспечивает синхронную работу интеллектуальных (смарт) объектов через прикладной программный интерфейс REST (также известный как RESTful API) и в целом соответствует ресурсно-ориентированной архитектуре ROA (Resource-Oriented Architecture).

3. Предоставляет асинхронный режим работы интеллектуальных объектов с использованием в значительной степени стандартных Web-технологий, таких как Atom, содержащей формат для описания ресурсов на веб-сайтах и протокол для их публикации, или Web-механизмов передачи данных, таких как модель работы веб-приложения Comet, при

которой постоянное HTTP-соединение позволяет веб-серверу отправлять данные браузеру без дополнительного запроса со стороны браузера.

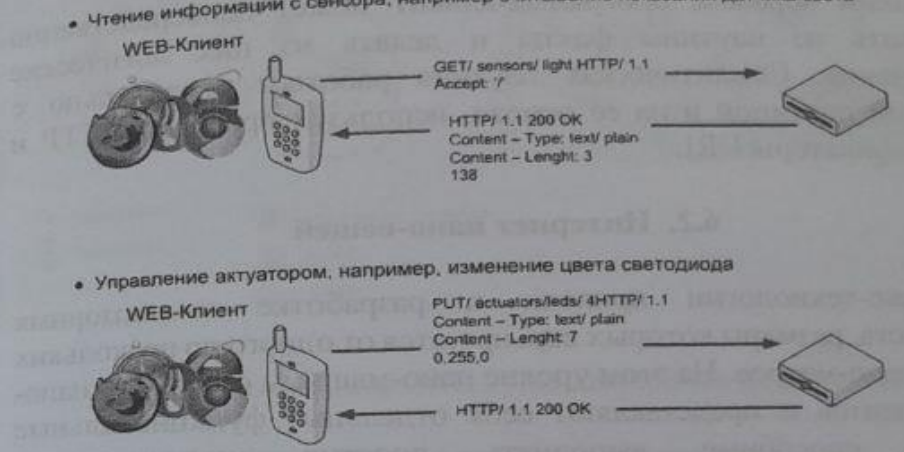


Рис. 6.1. Примеры веб-взамодействия с устройствами сенсорной сети

Эти характеристики WoT обеспечивают простое взаимодействие интеллектуальных объектов через Интернет, кроме того они реализуют единообразный интерфейс для доступа и поддержки функциональности смарт-объектов.

С концепцией WoT перекликается идея *Семантической паутины* (Semantic Web) - это направление развития Всемирной паутины WWW, целью которого является представление информации в виде, пригодном для машинной обработки. Термин «семантическая паутина» был впервые введён Тимом Бернерсом-Ли (изобретателем Всемирной паутины) в 2001 году. Концепция семантической паутины была принята и продвигается Консорциумом Всемирной паутины W3C (World Wide Web Consortium).

В обычной паутине, основанной на HTML-страницах, информация заложена в тексте страниц и извлекается человеком с помощью браузера. Семантическая же паутина предполагает запись информации в виде семантической сети с помощью

онтологий. Под онтологией понимается формальное явное описание понятий в рассматриваемой предметной области (классов). Онтология вместе с набором индивидуальных экземпляров классов образует базу знаний [11].

Таким образом, программа-клиент может непосредственно извлекать из паутины факты и делать из них логические заключения. Семантическая паутина работает параллельно с обычной паутиной и на её основе, используя протокол HTTP и идентификаторы URI.

6.2. Интернет нано-вещей

Нано-технологии привели к разработке миниатюрных устройств, размеры которых варьируются от одного до нескольких сотен нано-метров. На этом уровне нано-машины состоят из нано-компонентов и представляют себя отдельные функциональные блоки, способные выполнять простые измерительные, регулирующие или управляющие операции. Координация и обмен информацией между нано-устройствами позволяют образовывать так называемые нано-сети. В случае соединения нано-устройств с существующими сетями и Интернетом возникает новая сетевая парадигма, называемая Интернетом нано-вещей [31].

Для взаимодействия нано-устройств с существующими сетями и Интернетом требуется разработка новых сетевых архитектур. На рис. 6.2 представлена архитектура Интернета нано-вещей в двух различных реализациях - сеть на теле человека для мониторинга показателей здоровья и отправки их в медицинский центр, и современная офисная сеть, соединяющая множество различных устройств.

Сеть на теле человека состоит из нано-сенсоров и нано-актуаторов, которые могут отправлять информацию через внешний шлюз в медицинское учреждение. В данном случае на нано-уровне используются молекулы, протеины, ДНК, органические вещества и основные компоненты клеток. Таким образом, биологические нано-сенсоры и нано-актуаторы обеспечивают интерфейс между биологической средой человека и электронными наноустройствами, которые могут использоваться в новой сетевой парадигме - Интернете нано-вещей [32].

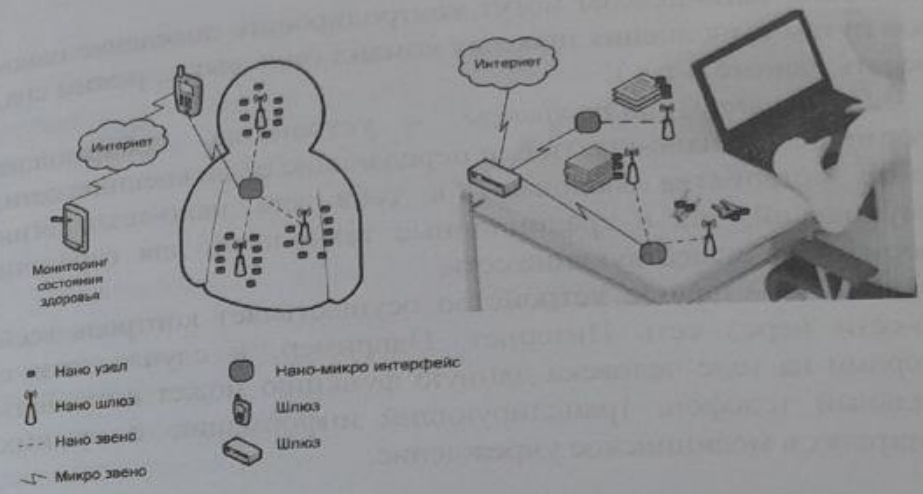


Рис. 6.2. Примеры архитектуры Интернета нано-вещей

Внутриофисная сеть соединяет множество даже самых небольших устройств с наноприемопередатчиками, обеспечивающими соединение с сетью Интернет. В результате этого взаимодействия пользователь может отслеживать состояние и местонахождение любых вещей, без каких либо усилий и временных затрат. При разработке новых миниатюрных устройств могут использоваться самые передовые энергосберегающие технологии, позволяющие получать механическую, электромагнитную и другие виды энергии из окружающей среды.

Независимо от области применения, основными компонентами архитектуры сети Интернета нано-вещей являются:

1. *Нано-узлы* - миниатюрные и простейшие нано-устройства. Позволяют выполнять простейшие расчеты, имеют ограниченную память и ограниченную дальность передачи сигналов. Примерами нано-узлов могут быть биологические нано-сенсоры на человеческом теле или внутри него или нано-устройства, встроенные в повседневные окружающие нас вещи - книги, часы, ключи и т.д.

2. *Нано-шлюзы* - данные нано-устройства имеют относительно высокую производительность по сравнению с нано-узлами и выполняют функцию сбора информации от нано-узлов.

Кроме того, нано-шлюзы могут контролировать поведение нано-узлов путем выполнения простых команд (вкл./выкл., режим сна, передать данные и т.д.).

3. *Нано-микро интерфейсы* - устройства, собирающие информацию от нано-шлюзов, и передающие её во внешние сети. Данные устройства включают в себя как нано-технологии коммуникаций, так и традиционные технологии для передачи информации в существующие сети.

4. *Шлюз* - данное устройство осуществляет контроль всей нано-сети через сеть Интернет. Например, в случае сети с сенсорами на теле человека данную функцию может выполнять мобильный телефон, транслирующий информацию о нужных показателях в медицинское учреждение.

6.3. Когнитивный интернет вещей (CIoT)

Интернет вещей является открытой парадигмой, которая чрезвычайно восприимчива и адаптивна для новых принципов и архитектур, относящихся к различным направлениям развития науки и техники. В этой связи чрезвычайно плодотворным может оказать использование в IoT принципов и методов когнитивности (лат. cognitio, «познание, изучение, осознание») путем создания когнитивного Интернета вещей CIoT (Cognitive Internet of Things) [30, 31].

Когнитивность означает наличие у объекта IoT следующих общих свойств:

- способность к самоанализу и реконфигурации с учётом имеющегося окружения, а также имея в виду достижение целей, обусловленных выполняемыми задачами;
- способность адаптировать своё состояние согласно имеющимся условиям или событиям, на основе определенных критериев и знаний о предыдущих состояниях;
- возможность динамически изменять свою топологию и/или эксплуатационные параметры в соответствии с требованиями конкретного пользователя, когда это необходимо в рамках текущей политики обслуживания, оптимизации пропускной способности сети или иных показателей;
- самоконфигурация с наличием распределенного управления

на основе правил;
- возможность самостоятельного определения своего текущего состояния и, с учетом этого состояния - планирование своей работы, принимая определенные решения в ответ на сложившуюся ситуацию.

Представляется, что на практике когнитивные интернет-вещи смогут:
- использовать технологии получения знаний о своей операционной и географической среде, местонахождении, например с помощью стандартных технологий позиционирования GPS/ГЛОНАСС;
- устанавливать самостоятельно или использовать готовые правила взаимодействия между объектами (интернет-вещами);
- динамически и автономно корректировать свои операционные (рабочие) параметры и протоколы в соответствии с полученными знаниями для достижения заранее определенных целей, в частности выбирать наиболее подходящую технологию передачи радиосигнала; обучаться на основе достигнутых результатов с использованием лучших практик и наиболее эффективных политик для достижения целей создания IoT.

Рассмотрим некоторые предположения относительно создания архитектуры когнитивного Интернета вещей. Концепция CIoT предполагает наличие IoT с механизмами кооперации и «разумности». Объекты CIoT смогут составить определенное представление о состоянии и условиях функционирования окружающих объектов, воспринимать знания об окружающих объектах, продуцировать логические выводы из накопленных знаний и осуществлять действия по адаптации к внешним и внутренним условиям. Соответственно, в архитектуре CIoT (рис 6.3) появляются когнитивные узлы CN (cognitive node) или когнитивные элементы CE (cognitive element), которые способны автономно оптимизировать, например, технические характеристики сети в соответствии с определенными условиями.

В свою очередь CE или CN объединяются в домены автономности AD (Autonomous Domain), где эти устройства относительно тесно связаны между собой, в том числе на определенной территории, и могут кооперировать своё поведение. При этом каждое CE или CN сохраняет свойство автономности. В

свою очередь, многие домены AD могут трансгранично взаимодействовать и кооперироваться через мультидоменную кооперацию MDC (MultiDomain Cooperation). Для организации такого взаимодействия в каждом автономном домене используется когнитивный агент CA (Cognitive Agent), который взаимодействует с CE или CN в своем домене.

Таким образом, взаимодействие доменов возможно как в целом, так и на уровне отдельного когнитивного элемента. При этом в каждом домене AD существуют и простые, не когнитивные узлы, которые, находятся под контролем когнитивных узлов.

Основой для развития схемы когнитивного управления является концепция виртуального объекта VO (Virtual Object), который является представлением физического объекта или объекта реального мира RWO (Real-World Object), что в принципе не противоречит требованиям Рекомендации МСЭ-Т Y.2060.

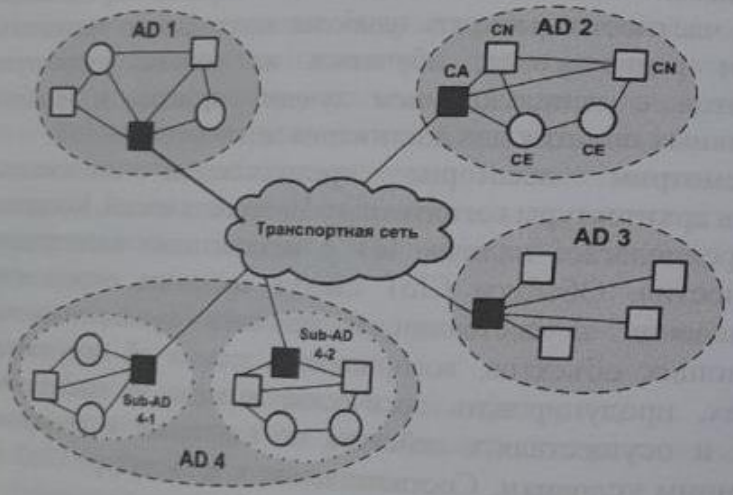


Рис 6.3. Архитектура когнитивного Интернета вещей CIoT

Виртуальный объект динамически создается или удаляется, создавая тем самым представление динамики изменений RWO. Для описания возможностей автоматической агрегации VO, чтобы обеспечить условия для исполнения приложений в предлагаемой схеме когнитивного управления вводится понятие концепции

композитных (сложносоставных) виртуальных объектов CVO (Composite VO) (рис. 6.4).

Рассмотрим применение концепции CIoT на примере оптимизации времени оказания неотложной помощи больному по конкретному адресу. Больной находится под дистанционным контролем системы медицинского мониторинга на базе услуги IoT. Пусть сенсорная система на теле больного («body sensor») зафиксировала резкое и продолжительное изменение параметров состояния человека - резкое учащение дыхания, пульса, сердечную аритмию, признаки обморока.

Рис. 6.4. Схема когнитивного управления

Показания сенсоров - RWO, приводят к изменению состояния объектов VO, связанных с RWO через шлюз. Специальное приложение для обработки и трансляции показаний сенсоров обрабатывает указанную информацию VO и преобразует её к виду, который может быть использован CVO, в данном случае - медицинским центром с помощью процедуры запроса и совпадения ситуации RSM «Request and Situation Matching». Однако если в ходе поиска требуемый CVO не найден, или отсутствует свободный медицинский автомобиль (ситуация «все

на выезде»), то с помощью процедуры принятия решений задействуется другой подходящий для данного случая VO, например сенсор пожарной сигнализации.

В результате в схеме принимает участие новый CVO - служба спасения - на основе анализа близости ситуации к опасной для здоровья человека. В итоге скорая помощь может быть оказана больному не медицинским центром, а службой спасения, специалисты которой также имеют навыки медицинской помощи. С учетом того, что событие происходит в «умном городе», медицинская информация о состоянии больного может транслироваться параллельно на CVO медицинского центра и на CVO «умного автомобиля» службы спасения. Одновременно тревожное сообщение транслируется на CVO службы регулирования дорожного движения, которая организует «зеленую улицу» в направлении дома больного.

Таким образом, описанная ситуация наглядно показывает преимущества когнитивности и когнитивного управления применительно к интернету вещей.

Контрольные вопросы

1. Как происходит процесс считывания данных с датчика в сети беспроводных датчиков через браузер?
2. Перечислите основные свойства WoT.
3. Объясните архитектуру интернет-нанообъектов.
4. Каковы основные компоненты архитектуры интернет-нанотехнологий?
5. Какие устройства являются наноузлами?
6. Какова функция наношлюзов?
7. Какие устройства являются нано-микро интерфейсами?
8. Каковы когнитивные свойств объекта IoT?

Глава 7. ПЛАНЫ, ПРОГНОЗЫ И ПРОБЛЕМЫ ВНЕДРЕНИЯ IoT

7.1. Планы и прогнозы внедрения IoT

«Интернет вещей» представляет собой совокупность разнообразных приборов, автономных датчиков и исполнительных устройств, объединенных в сеть посредством любых доступных каналов связи (проводных или беспроводных), использующих различные протоколы взаимодействия между собой, подключенных к глобальной Сети Интернет и выполняющих собственные или облачные приложения. Рынок IoT постоянно развивается, это направление в настоящее время является одним из самых перспективных (рис. 7.1) [23].

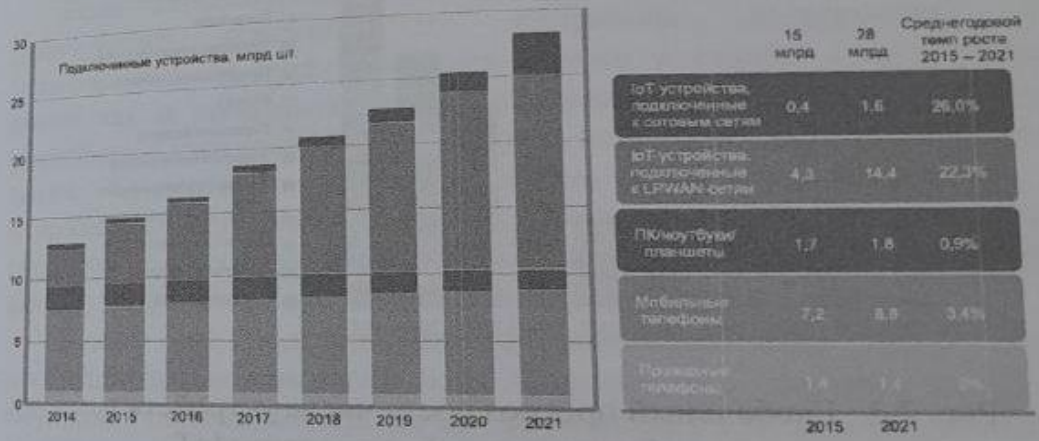


Рис. 7.1. Изменение числа подключенных к Интернету устройств

Максимальный рост демонстрируют устройства, использующие сети CIoT (Cellular Internet of Things - «Интернет вещей» в сетях сотовой связи). В абсолютных же цифрах вне конкуренции сети с низким энергопотреблением LPWAN (Low Power Wide Area Networks). По оценкам специалистов, данная тенденция сохранится в течение ближайших лет. Дальнейшее развитие этих двух основных направлений ставит перед пользователями, желающими использовать IoT в бытовых или промышленных целях, непростую задачу выбора подходящей

технологии.

Государство само является крупнейшим потенциальным потребителем услуг IoT, т.к. оно управляет колоссальной инфраструктурой: дорогами, объектами ЖКХ, зданиями и сооружениями, электрическими и тепловыми сетями и пр. Рынок государственных учреждений и госкомпаний обладает огромным экономическим потенциалом для внедрения технологий IoT с точки зрения повышения энергоэффективности и сокращения затрат на обслуживание производственных активов.

На рис. 7.2 показан глобальный прогноз роста числа устройств в узкополосных беспроводных сетях связи IoT по отдельным видам экономической деятельности.

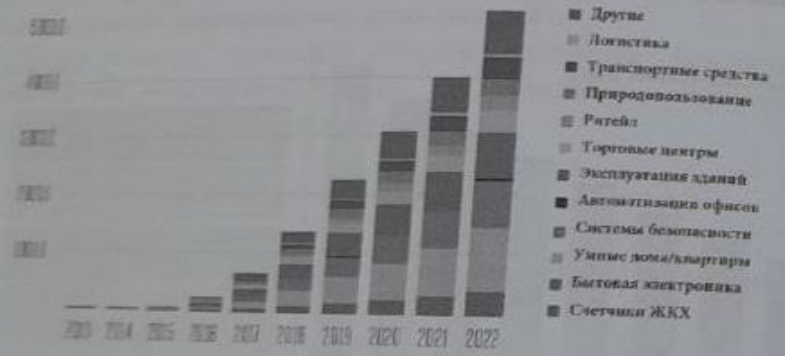


Рис. 7.2. Глобальный прогноз роста числа устройств в узкополосных беспроводных сетях связи IoT

Нестандартное разбиение на отрасли, приведенное на рис.7.2, является следствием того, что одни и те же узкополосные беспроводные сети связи IoT могут обслуживать различные отрасли и их точный учет по конкретным отраслям затруднен. Тем не менее, рис. 7.2 иллюстрирует потенциал возможностей использования узкополосных беспроводных сетей связи IoT.

7.2. Проблемы внедрения IoT

Широкому внедрению Интернета вещей препятствуют

сложные технические и организационные проблемы, в частности, связанные со стандартизацией. Единых стандартов для интернета вещей пока нет, что затрудняет возможность интеграции предлагаемых на рынке решений и во многом сдерживает появление новых. Сильнее всего глобальному внедрению препятствует расплывчатость формулировок концепции интернета вещей и большое число регуляторов и их нормативных актов.

К факторам, замедляющим развитие Интернета вещей, следует отнести сложности перехода существующего Интернета к новой, 6-й версии сетевого протокола IP (IPv6), прежде всего необходимость больших финансовых затрат со стороны телекоммуникационных операторов и провайдеров услуг на модернизацию своего сетевого оборудования.

Если технологические платформы для Интернета вещей уже практически созданы, то, например, юридические и психологические ещё находятся только в стадии становления, равно как и проблемы взаимодействия пользователей, данных, устройств. Одна из проблем - защита данных в таких глобальных сетях. Существует также серьезная проблема, связанная с вторжением Интернета вещей в частную жизнь. Возможность отслеживать местонахождение людей и их собственности ставит вопрос о том, в чьем распоряжении окажутся эти сведения.

Также для полноценного функционирования такой сети необходима автономность всех «вещей», т.е. датчики должны научиться получать энергию из окружающей среды, а не работать от батареек, как это происходит сейчас.

Кроме того, с появлением Интернета вещей возникнет необходимость изменения общепринятых и проверенных бизнес-процессов и стратегий, что может привести к значительным финансовым затратам и рискам.

Основные драйверы и проблемы внедрения Интернета вещей приведены в таблице 7.1. Однако все перечисленные недостатки не существенны по сравнению с тем, какие возможности может дать Интернет вещей для человечества. Поэтому рано или поздно человечество неизбежно будет широко использовать технологии IoT.

Таблица 7.1

Драйверы и барьеры рынка Интернета вещей

Драйверы	Барьеры
Стремительное развитие инфокоммуникационных технологий	Необходимость принятия общих стандартов
Мода на смартфоны, планшеты и другие мобильные устройства	Медленный переход к протоколу IPv6
Логистика и управление поставками	Риск закрытости частных сетей
Повышение безопасности и удобства автотранспорта	Несовместимость ряда компонентов
Необходимость сохранения окружающей среды и снижения энергозатрат	Проблема защиты персональных данных и безопасности
Развитие сферы контроля за контрафактной продукцией и защиты от краж	Сравнительно высокая стоимость внедрения
Поддержка государств и действия инноваторов	

Контрольные вопросы

1. С чем связан рост количества устройств, подключенных к Интернет?
2. Перечислите и опишите драйверы и барьеры рынка Интернета вещей.
3. Как состояние интернета оказывает влияние на развитие рынка интернета вещей?
4. Какие проблемы возникает при внедрении IoT?

Глава 8. ИНТЕРНЕТ ВЕЩЕЙ И БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ

8.1. Беспроводные сети для IoT

В современном мире датчики находятся повсюду. Сейчас это явление воспринимается как должное, поскольку датчики находятся в автомобилях, смартфонах, на предприятиях, осуществляя контроль выбросов угарного газа в атмосферу, и даже в почве, контролируя грунтовые условия в виноградниках.

Концепция интернета вещей (IoT) была разработана параллельно с беспроводных сенсорных сетей (БСС). Понятие «интернет вещей» было впервые использовано Кэвином Аштоном в 1999 году [33] и относится к уникально идентифицируемым объектам и их виртуальном представлении в «подобной интернету» структуре. Этими объектами могут быть любые объекты от крупных зданий, промышленных предприятий, самолетов, автомобилей, машин, любых видов товаров, конкретных частей больших систем до людей, животных и растений, и даже конкретных частей их тел.

Сам по себе IoT не является технологией связи, тем не менее, технологии беспроводной связи будут играть главную роль, в частности, беспроводных сенсорных сетей (БСС) будут иметь множество вариантов практического использования и охватывать многие отрасли экономики, небольшие, прочные, недорогие и маломощные БСС-датчики позволят IoT проникнуть в самые маленькие по размеру предметы, установленные в любой среде. Интеграция этих объектов в IoT станет важной вехой эволюции БСС.

IoT - это экосистема автономных устройств (сенсоров и актуаторов), которые могут взаимодействовать друг с другом без участия человека. Наука и технологии развиваются по спирали и с точки зрения телекоммуникационных технологий IoT - это очередной виток развития сенсорных сетей, методами построения которых ученые и инженеры занимаются уже не одно десятилетие. Параллельно с развитием телекоммуникационных технологий для передачи больших объемов данных, таких как файлы, веб-страницы, аудио- и видеопотоки, развивались

специальные технологии для передачи коротких сообщений небольшими и очень простыми устройствами, питающимися, как правило, от батарейки. К таким устройствам относятся, например, пожарные датчики.

Развивались технологии передачи и обработки данных, все больше различных устройств вовлекалось в сетевое взаимодействие, наконец, росло число устройств, которые могли общаться посредством интернета, — все это стало признаками зарождения IoT [34-36].

Одно из отличий систем IoT от старых сенсорных сетей заключается в том, что если сенсорные сети подразумевают просто телекоммуникационную сеть передачи данных между сенсорами, то IoT предполагает комплексное решение. Оно включает в себя как датчики, телекоммуникационную инфраструктуру, так и серверы, на которые эти данные поступают, а также методы анализа полученных данных и алгоритмы принятия решений (что нужно сделать, после того как у вас произошло какое-либо событие). Поэтому становится актуальной задача осмысления собираемой информации: из этого огромного количества собранной информации нужно научиться вычленять полезное знание. Например, пусть есть множество сенсоров, которые измеряют температуру, давление, состав воздуха. Когда на предприятии происходит авария, нужно по изменениям этих параметров понять, что это не просто из-за туч выглянуло солнце и нагрело воздух, а что произошел форс-мажор. Такие комплексные задачи как раз и осуществляются IoT.

Кроме того, в случае аварии, пожара или другой чрезвычайной ситуации множество датчиков могут одновременно начать передавать данные. Если используется беспроводная сеть - а соединить тысячи автономных устройств проводами тяжело и дорого, а в ряде сценариев и невозможно, - то такая одновременная передача данных большим числом устройств приводит к коллизии и данные теряются. Вот почему поддержка надежной доставки данных большим числом устройств с низким запасом энергии является одной из ключевых задач, стоящих перед разработчиками беспроводных сетей для IoT.

Толчком для развития БСС послужили военные технологии, в частности, системы наблюдения в горячих точках. Сегодня эти

сети состоят из распределенных независимых устройств, оснащенные датчиками для мониторинга физических условий, и применяются в промышленной инфраструктуре, автоматике, здравоохранении, транспорте и многих пользовательских сферах.

В настоящее время БСС считаются одной из наиболее важных технологий XXI века [36]. Технология БСС, позволяющая осуществлять «повсеместно доступное считывание» в рамках всего промышленного процесса, может обеспечить достижение и поддержание важных параметров, недоступных при онлайн-мониторинге по причине указанных выше издержек. Эти параметры являются важными для внедрения оптимального управления для достижения цели повышения качества продукции и снижения потребления энергии.

В энергетике, которая в настоящее время переживает модернизацию системы энергоснабжения, технология БСС также играет важную роль при осуществлении контроля безопасности оборудования передачи и трансформации энергии, а также реконструкции миллиардов умных счетчиков.

По мере развития сопутствующих технологий, стоимость оборудования БСС резко снизилась, а возможности их использования постепенно выходят за пределы оборонной отрасли, распространяясь на промышленный и коммерческий сектора. Следует отметить, что стандарты технологии БСС были хорошо проработаны, а именно Zigbee®1, WirelessHart, ISA 100.11a (рис. 8.1).

Кроме того, новые возможности применения режимов БСС, которые появляются в промышленной автоматизации и домашних приложениях, общий размер рынка приложений БСС продолжит стремительный рост.

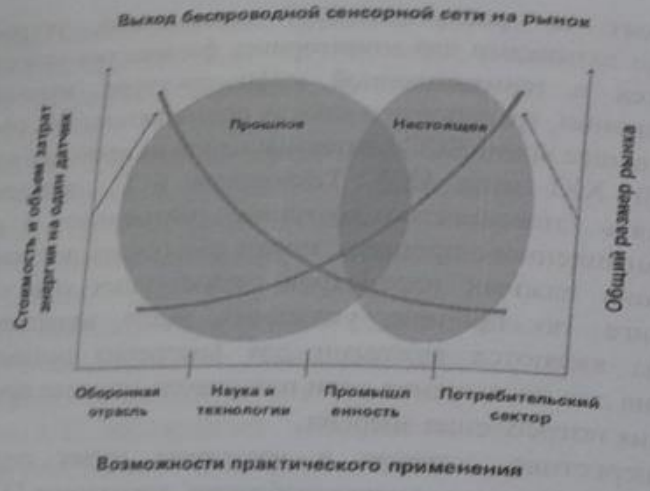


Рис. 8.1. Размеры рынка прикладных решений БСС

8.2. Организация беспроводных сенсорных сетей

В целом, БСС можно описать как сеть узлов, которые совместно осуществляют мониторинг окружающей среды и сбор данных, обеспечивают взаимодействие между людьми или компьютерами и окружающей средой [35]. В настоящее время БСС, как правило, включают сенсорные узлы, узлы приводных устройств, шлюзы и клиентов (рис.8.2).

Большое количество сенсорных узлов, расположенных в случайном порядке внутри или возле контролируемой области (поле обнаружения), формируют сети путем самоорганизации. Сенсорные узлы осуществляют контроль собранных данных для их передачи на другие сенсорные узлы скачкообразным методом.

Во время передачи, отслеживаемые данные могут обрабатываться несколькими узлами для перехода к узлу шлюза после маршрутизации с несколькими переходами, и, в конечном итоге, достичь узла управления по интернету или при помощи спутника. Пользователь осуществляет конфигурацию и управление БСС при помощи узла управления, публикует задачи по мониторингу и осуществляет сбор контролируемых данных.

Беспроводные сенсорные сети (БСС) состоят из двух основных типов узлов:

1. Сенсоры (сенсорные узлы), которые развертывают в местах мониторинга (сенсорное поле) для сбора данных изучаемого явления или процесса и их передачи на базовые станции.

2. Базовая станция (БС), также известная как шлюз (*Gateway*) или приемник (*Sink*), является интерфейсом, соединяющим сенсорную сеть с внешним миром. БС может являться центральной точкой в сенсорном поле или находиться в отдалении от него. БС несет ответственность за получение данных от сенсоров, их обработку и доставку конечному пользователю разнообразными способами, включая телекоммуникационную сеть онлайн или через спутник и другие сети. Структура беспроводной сенсорной сети приведена на рис. 8.2.

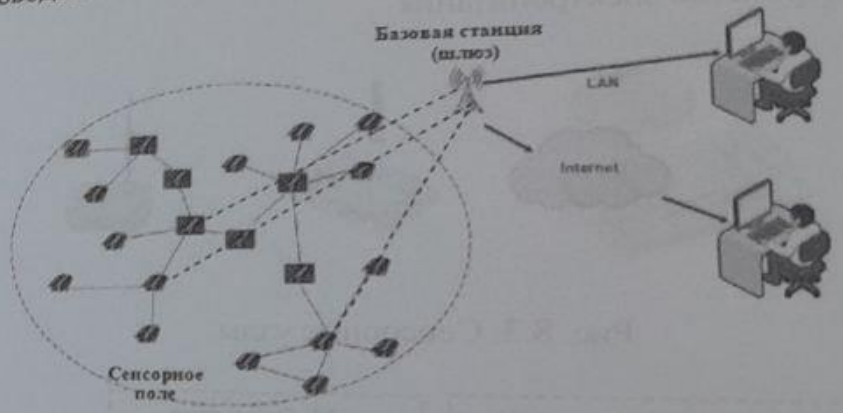


Рис. 8.2. Структура БСС

Данные, отслеживаемые во время передачи, могут обрабатываться на нескольких узлах для направления к узлу шлюза после маршрутизации с несколькими переходами и в конечном итоге достигать узла управления через Интернет или через спутник. Пользователь использует управляющий узел для настройки и управления сетью БСС, объявления задач мониторинга и сбора контролируемых данных.

Выбор конкретных решений для организации беспроводной сенсорной сети в первую очередь зависит от функциональных

возможностей, размер а, затрат, энергетических характеристик и, в настоящее время, при начале достаточно широкого внедрения сенсорных сетей - от обеспечения требуемого качества обслуживания.

Примеры конструкций современных сенсорных узлов приведены на рис. 8.3, а на рис. 8.4 рассматривается типовая архитектура сенсорного беспроводного узла, которая состоит из четырех основных компонентов:

1) Сенсорной подсистемы, включающей один или несколько сенсоров (с соответствующими аналого-цифровыми преобразователями) для получения и накопления данных;

2) Подсистема обработки, включающая микроконтроллеры и память для местной обработки данных;

3) Радиопередатчик для беспроводной передачи данных;

4) Устройство электропитания

Рис. 8.3. Сенсорные узлы

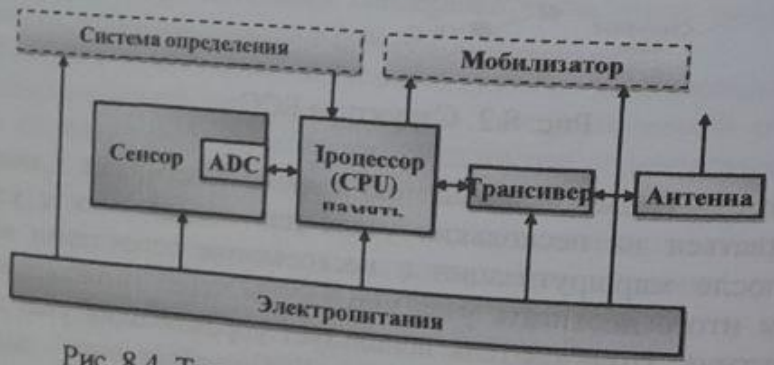


Рис. 8.4. Типовая архитектура сенсорного узла

В зависимости от определенного конкретного применения сенсорные узлы могут также включать в себя дополнительные

компоненты, такие как система позиционирования, чтобы определить их положение, мобилизатор, чтобы изменить их местоположение или конфигурацию (например, ориентация антенны), и так далее. Однако, поскольку последние компоненты дополнительные, мы не будем принимать их во внимание в последующем анализе.

Датчик является центральным элементом узла БСС, который может получить информацию о состоянии окружающей среды и оборудования. Датчик отвечает за сбор и преобразование сигналов, таких как свет, вибрация и химические сигналы в электрические сигналы с последующей их передачей на микроконтроллер. Микроконтроллер принимает данные от датчика и проводит их соответствующую обработку. Затем беспроводный приемопередатчик (RF-модуль) осуществляет передачу данных для физической реализации процесса связи. Важно, чтобы конструкция всех частей узла БСС учитывала характеристики узла БСС – малый размер и ограниченная мощность.

Сенсорные сети представляют собой распределенное в пространстве множество датчиков и исполнительных устройств, объединенных между собой посредством радиоканала. Применяться подобные сети могут в огромном спектре приложений: домашняя и промышленная автоматизация, контроль микроклимата, охранно-пожарные системы, учет и оптимизация потребления водоэнергоресурсов и т.д. Причем область покрытия подобной сети может составлять от единиц метров до нескольких километров. Идеология сенсорных сетей позволяет повсеместно избавляться от проводных интерфейсов и связанных с ними расходов (создание кабель-каналов, декорирование, монтаж проводов, закупка и монтаж специализированных коммутаторов, маршрутизаторов и т.д.). Например, установка системы охранно-пожарной сигнализации сводиться к простому расположению датчиков.

Стоит отдельно рассмотреть, что же представляет собой отдельный узел подобной сети. Обобщенная структура типичного датчика изображена на рис. 8.5.

Как видно из рис. 8.5, датчик сенсорной сети содержит в своем составе:

• **Радиомодем,** включающий низкомощный приемопередатчик и микроконтроллер (МК). МК, в свою очередь, имеет в своем составе вычислительное ядро, ОЗУ, Flash, ПЗУ, EEPROM, АЦП, блок обработки прерываний, определенную номенклатуру интерфейсов и ряд иных периферийных узлов, в зависимости от конкретного устройства.

• **Узел питания.** В цепях питания реализована защита от перенапряжения и от переполюсования клемм. Возможна дополнительная схема для подачи питания от внешнего источника.

• **Блок визуализации** — для отображения текущего состояния устройства (опционально).

• **Блок ввода** — для смены режимов работы, перезагрузки и т.д. (опционально).

• **Интерфейсный блок**, содержащий те или иные порты ввода/вывода, например, программирования или подключения внешнего датчика.

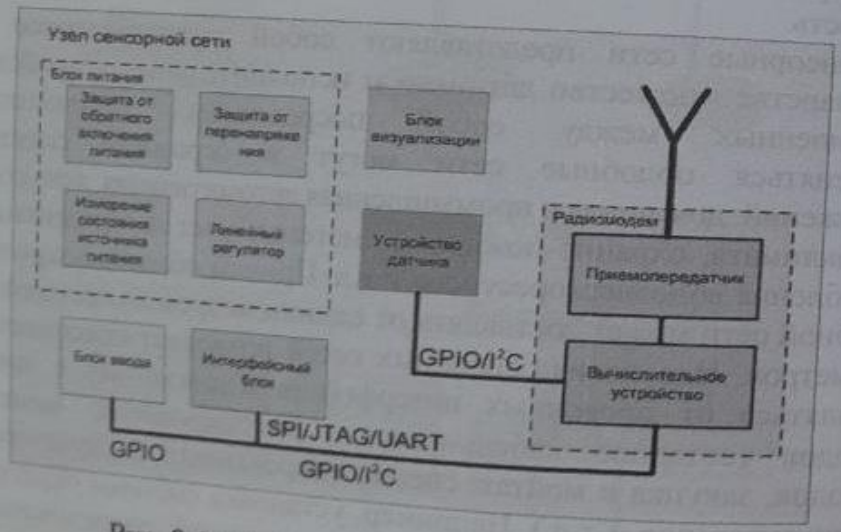


Рис. 8.5. Структура узла сенсорной сети

Сенсорные узлы образуют сенсорное поле, как правило, они находятся в спящем положении. Когда происходит событие, или по расписанию в определенное время, эти узлы просыпаются,

самоорганизовываются в сеть и передают информацию в центр сбора данных (рис. 8.6).

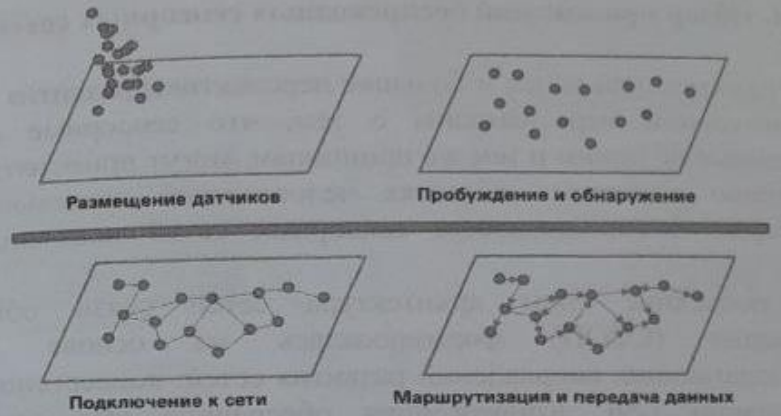


Рис. 8.6. Самоорганизация и передача данных в беспроводных сенсорных сетях

Контрольные вопросы

1. Опишите технологию беспроводной сенсорной сети.
2. Из каких компонентов состоит беспроводная сенсорная сеть?
3. Какова функция сенсорных узлов?
4. Какова функция базовой станции?
5. Объясните простую архитектуру узла беспроводных датчиков.
6. Приведите и объясните структуру узла сенсорной сети.
7. Какую функцию выполняет радиомодем?
8. Какие функции выполняют блоки ввода и интерфейса?

Глава 9. ОБЗОР ПРИЛОЖЕНИЙ И РЕШЕНИЙ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

9.1. Обзор приложений беспроводных сенсорных сетей

Существующий успех и большие перспективы развития БСС в значительной мере связаны с тем, что сенсорные сети, построенные по одним и тем же принципам, могут применяться в совершенно различных областях человеческой деятельности. Приложения всепроникающих сенсорных сетей показаны на рис.9.1.

В последние годы архитектура сетей связи общего пользования (ССОП) формировалась на основе двух основополагающих направлений развития сетей: конвергенции и гармонизации [29]. Конвергенция обеспечила при сетевом развитии совместное использование ресурсов ССОП всевозможными технологиями: сотовыми, Интернет, фиксированной связи, - а гармонизация предоставила возможность пользователю получать услуги в любой из перечисленных сетей единообразным способом. Оба эти направления, в конечном счете, кристаллизовались в концепцию сетей связи следующего поколения *NGN* (*Next Generation Network*) [33,34].

В соответствии с концепцией широкополосной конвергентной сети *BcN* (*Broadband convergence Network*) [35], очередной **качественный скачок** в области инфокоммуникационных услуг будет инициирован **внедрением беспроводных сенсорных сетей**, позволяющих пользователю глобальной телекоммуникационной сети получать телеметрическую информацию о различных объектах и обстановке в любой точке страны, а также отправлять команды на территориально разнесенные объекты. При этом трафик сенсорных сетей может быть передан через сеть связи общего пользования. *Ubiquitous* (всепроникающие) сети, технологической основой которой являются сенсорные сети, открывают новые перспективы развития инфокоммуникаций, создание на их основе U-обществ (рис. 9.2) [36].

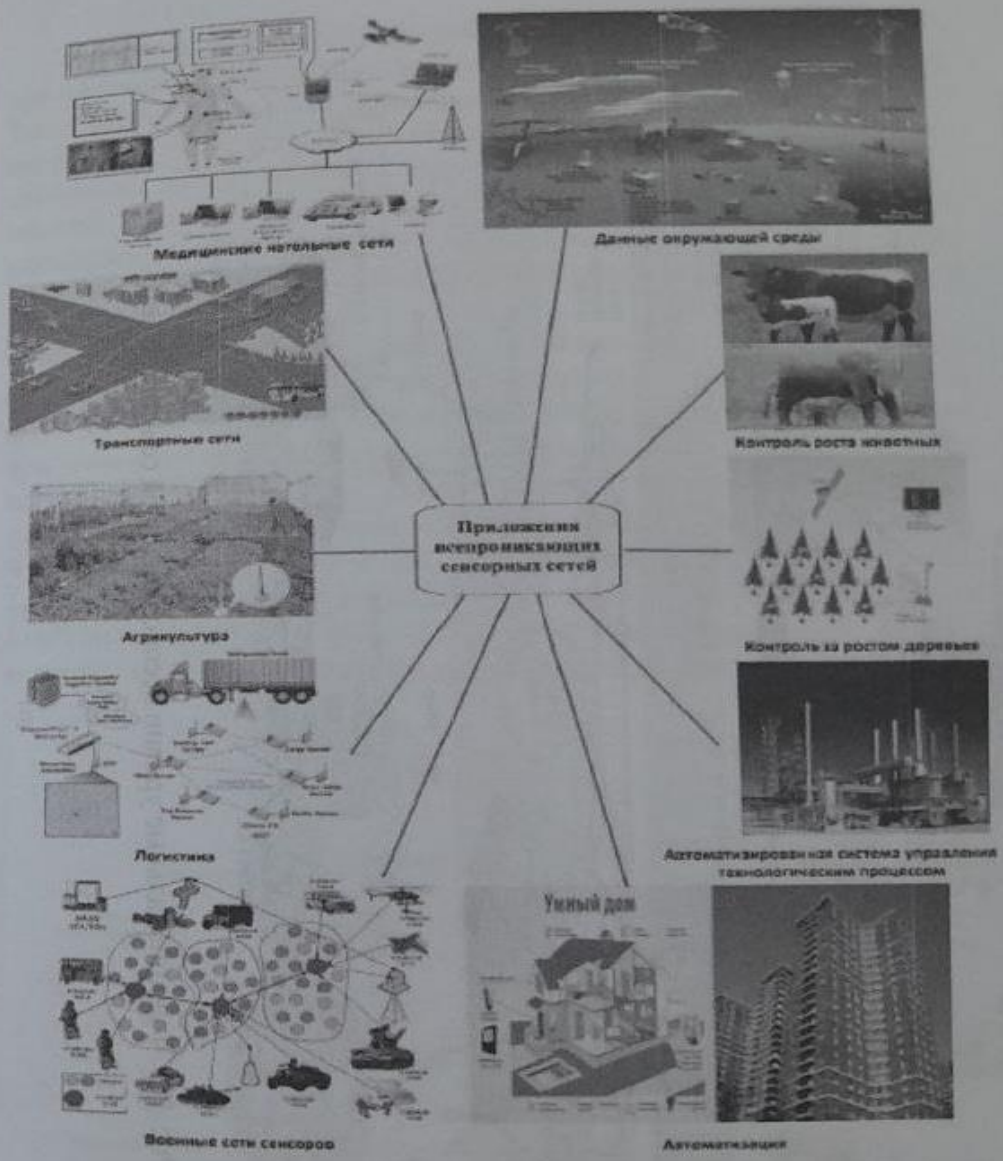


Рис. 9.1. Приложения всепроникающих сенсорных сетей

Рис. 9.2. Функциональные уровни всепроникающей сенсорной сети

В настоящее время для сопряжения БСС с ССОП используется протокол *6LoWPAN*, предложенный *IETF* (Internet Engineering Task Force -Специальная комиссия интернет-разработок), который позволяет интегрировать сенсорные сети в существующее семейство сетей. Данный протокол позволяет передавать IP-пакеты поверх стандарта *IEEE* 802.15.4 способом, удовлетворяющим открытым стандартам (протокол *IPv6)*. При этом обеспечивается взаимодействие с другими IP-каналами и устройствами [36].

Протокол *6LoWPAN* создан для маломощных беспроводных персональных сетей (*LoWPANs*) и описан в документах [RFC4919] и [RFC4944]. В архитектуре сети *6LoWPAN* (рис. 9.3) определены три типа логических устройств (оконечный узел, маршрутизатор и шлюз), а также три вида сетей: «*Простая LoWPAN*», «*Расширенная LoWPAN*» и «*Ad hoc LoWPAN*». Как видно из рис. 9.3, «*Ad hoc LoWPAN*» не подключена к ССОП, «*Простая LoWPAN*» подключена к ССОП через один шлюз, а «*Расширенная LoWPAN*» включает в себя несколько шлюзов, связанных с ССОП и друг с другом посредством магистральной линии связи [36].

Рис. 9.3. Архитектура сети 6LoWPAN

Следует особо выделить следующие особенности сенсорных сетей:

- способность к самовосстановлению и самоорганизации,

- способность передавать информацию на значительные расстояния при малой мощности передатчиков (путем ретрансляции),

- низкая стоимость узлов и их малый размер,

- низкое энергопотребление и возможность электропитания от автономных источников,

- простота установки, отсутствие необходимости в прокладке кабелей (благодаря полностью беспроводной технологии и питанию от батарей) [36];

- возможность установки таких сетей на уже существующий и эксплуатирующийся объект без проведения дополнительных работ,

- возможность управления инфраструктурой БСС с помощью планшетного ПК (рис. 9.4)

- низкая стоимость технического обслуживания.

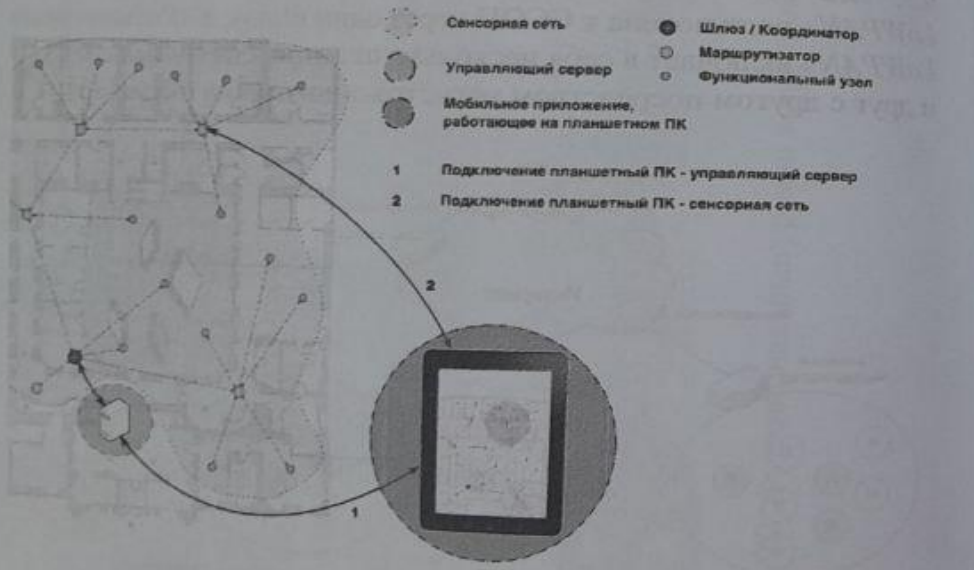


Рис.9.4. Мониторинг и управление БСС с помощью планшетного компьютера

9.2. Решения для автоматизации домов, офисов, промышленных объектов

Умный дом»

«Умный дом» предназначен для максимально комфортной жизни людей посредством использования современных высокотехнологичных средств. Принцип работы системы «умный дом» заключается в автоматизации всего, из чего состоит жилая постройка: освещение, кондиционирование, система безопасности, электроэнергия, отопление, водоснабжение и водоотведение и так далее. К основным подсистемам «умного дома» относятся: климат-контроль, освещение, мультимедиа (аудио и видео), охранные системы, связь и другие (рис. 9.5) [37].

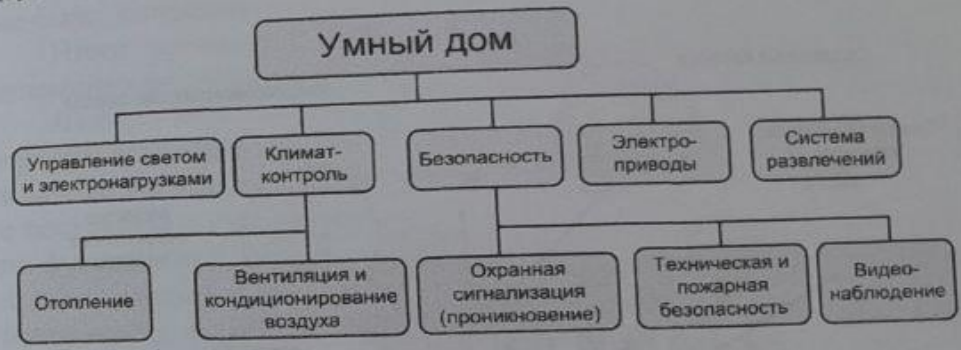


Рис. 9.5. Основные подсистемы «умного дома»

В стандартном проекте «умного дома» можно выделить три основные подсети: сеть мультимедийных устройств, сеть электроосветительного оборудования и сенсорную сеть. В последнем случае это датчики движения, света, температуры, давления, влажности, вибрации и т.п. Таким образом, «умный дом» состоит из программного и аппаратного обеспечения, датчиков и проводной/беспроводной сети (рис. 9.6).

В общем случае, «умный дом» предоставляет его владельцу следующие преимущества:

1) снижение потребления ресурсов (газ, вода, электроэнергия);

2) высокий уровень комфорта;

3) обеспечение необходимого взаимодействия всех автоматизируемых систем объекта недвижимости, задание различных режимов работы;

4) снижение вероятности возникновения аварийных ситуаций;

5) повышение оперативности, простоты и удобства управления.

Для автоматизации дома смарт-узлы могут быть интегрированы непосредственно в бытовые приборы, например, в пылесосы, микроволновые печи, холодильники и телевизоры (их описание приведено ниже). Они могут взаимодействовать друг с другом и с внешней сетью через интернет. Это позволит конечным пользователям легко управлять устройствами дома как локально, так и удаленно.

Рис. 9.6. Основные компоненты «умного дома»

Большинство бытовых устройств из категории «умных» вещей можно поделить на две группы по типу использования интернета.

К первой группе относится техника, которая через WWW обновляет свое программное обеспечение, получает новые функции, принимает управляющие сигналы от находящегося вдали хозяина, и, соответственно, отправляет ему информацию, подтверждающую выполненные действия и свое состояние. Этот тип использования интернета бытовой техникой является наиболее разумным и способен доказать потенциальному потребителю свою полезность. Во вторую группу входит техника, в которой интернет является как бы инородным телом. Суть решения в том, что в совершенно привычный бытовой прибор, типа микроволновки или холодильника, встраивается упрощенный компьютер и дисплей, после чего с их помощью можно получать мультимедийные развлечения там, где их раньше не было, например, на той же кухне.

Ниже приведены наиболее характерные примеры «умных» домашних вещей с подключением к интернет.

Интернет-холодильник (Internet refrigerator или *Smart refrigerator)* – новый класс бытовых холодильников, появившийся в начале XXI века. Как правило, он имеет встроенный компьютер с постоянным подключением к сети интернет и сенсорный экран на фронтальной панели (рис. 9.7). Такой холодильник не только хранит продукты, но и даёт возможность пользоваться интернетом, через который можно получить доступ к различным сайтам (например, с кулинарными рецептами для приготовления блюд) и даже заказывать продукты в интернет-магазинах с доставкой на дом.

Кроме того, с помощью интернет-холодильника можно общаться, используя электронную и видеопочту. Интернет-холодильник может предоставлять целый ряд сервисов: доступ в Интернет, видеотелефон, e-mail, TV, MP3-музыку, базу данных по кулинарным рецептам и правилам питания, электронное перо, чтобы оставить сообщение, голосовые послания.

Рис. 9.7. Интернет-холодильник Digital Dios Refrigerator компании LG Electronics

Ряд моделей интернет-холодильников оборудованы телевизионным и радиоприёмником. Кроме того, при использовании интернет-холодильника появляется возможность вывести на экран картинку от веб-камеры внешнего видеонаблюдения. Это позволяет видеть происходящее во дворе частного дома, даже не покидая кухни, присматривать за своим малышом, находящимся в детской комнате и т.д.

Некоторые устройства данного типа также могут следить за содержимым холодильника, выбирая оптимальные условия хранения и заморозки продуктов. Кроме этого, интернет-холодильник отслеживает продукты с истекающим сроком годности. Информация обо всем этом поступает на смартфон пользователя и последний, находясь в магазине, может оценить свои реальные потребности в продуктах.

Робот-пылесос может действовать автономно, программироваться и управляться через Интернет, для чего имеется ряд сенсоров и инфракрасная встроенная камера (рис. 9.8). Система управления работой пылесоса делает несколько снимков

в секунду создавая, таким образом, карту всего дома или отдельных его комнат.

Устройство также имеет возможность запоминать оптимальный путь уборки и определять своё местонахождение в доме. Аккумулятора хватает на определенное время уборки (обычно до 1,5 часов), по истечении которого робот сам отправляется на подзарядку.

Рис. 9.8. Робот-пылесос VC-RL87W компании Samsung

К пылесосу имеется беспроводный доступ Wi-Fi с помощью компьютера или смартфона. Через эти устройства можно запустить его и в режиме реального времени наблюдать за тем, что происходит в комнате. Более того, можно поговорить с людьми, которые находятся в доме через систему голосовой связи. Встроенный источник света позволяет видеть в полной темноте и проверить помещение даже ночью.

Интернет микроволновая печь (рис. 9.9) имеет встроенный модем для выхода в интернет, память для хранения скачиваемой информации и пульт управления. Она выполняет следующие задачи:

- скачивание рецептов из интернета и самопрограммирование;
- связь с компаниями – производителями продуктов;
- дает доступ к системе заказа продуктов по интернету.

Интернет-кондиционер подключается к интернету по проводной или беспроводной сети Wi-Fi и дает пользователю доступ к управлению кондиционером из любой точки земного шара. Владелец может дистанционно включать и выключать

систему, программировать настройки, выбирать режимы, температуру, скорость вентилятора, задавать параметры, словом совершать любые манипуляции, доступные с обычного пульта.

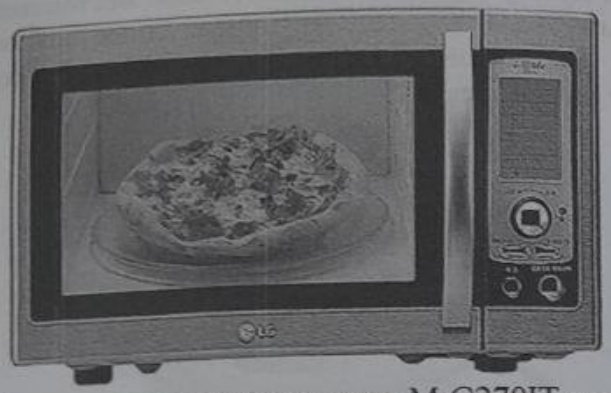


Рис. 9.9. Микроволновая интернет-печь M-G270IT компании LG Electronics

Управлять таким кондиционером можно с любого устройства (компьютер, ноутбук, планшет, смартфон), в котором установлена специальная программа и который имеет выход в интернет. *Система по уходу за домашними животными* призвана обеспечить им все необходимые комфортные условия существования. Такая система используется в случае длительного отсутствия хозяев дома – это позволяет не беспокоиться о благополучии своих домашних любимцев.

Основными задачами системы по уходу за домашними животными являются автоматическая подача еды и питья, а в случае возникновения непредвиденных обстоятельств - информирование хозяев о них (по телефону, с помощью SMS или по электронной почте). По желанию можно составить полный отчет о поведении домашних животных во время отсутствия хозяев - сколько раз и когда ели, пили воду и т.д. Можно сопроводить этот отчет фотографиями (если установлена камера слежения) и передавать их (по электронной почте, с помощью MMS).

Построение сети на основе стандартов 802.15.4/ZigBee

Сенсорные сети сейчас поставляются множеством производителей, что привело к появлению разнообразных индустриальных стандартов, не обеспечивающих взаимодействия между оборудованием различных производителей. Основные работы в области стандартизации протоколов, используемых в сенсорных сетях, проводятся Институтом инженеров электротехники и электроники (IEEE), Международным союзом электросвязи (ITU), Инженерным советом Интернета (IETF) и Международной организацией по стандартизации (ISO) [36].

Результатом этих работ стало семейство стандартов IEEE 802.15.4, регламентирующих физический и канальный уровни для организации беспроводных сенсорных сетей, но оставляющих неопределенными сетевой и прикладной уровни. Последующее развитие IP сетей привело к формированию рабочей группы IETF 6LoWPAN для решения проблемы передачи IPv6 пакетов поверх каналов IEEE 802.15.4 способом, удовлетворяющим открытым стандартам и предоставляющим взаимодействие с другими IP каналами и устройствами в той же мере, как и с устройствами IEEE 802.15.4.

Стандартизация протоколов взаимодействия в сенсорных сетях требует проведения классификации приложений по типу создаваемой нагрузки. Параметры качества обслуживания для пакетных сетей связи рассмотрены в рекомендациях МСЭ-Т Y.1540 и Y.1541. В рекомендации Y.1540 определяются параметры, которые могут быть использованы для оценки эффективности скорости, точности, надежности и доступности пакетной передачи IP. Рекомендация Y.1541 регламентирует классы обслуживания для сетей связи следующего поколения (NGN). В связи с особенностями приложений, в которых применяются сенсорные сети, требуется уточнение и изменение рекомендаций Y.1540 и Y.1541.

Сегодня технология беспроводных сенсорных сетей на основе стандартов 802.15.4/ZigBee является единственной беспроводной технологией, с помощью которой можно решить задачи мониторинга и контроля, которые критичны к времени автономной работы датчиков [38].

Объединенные в беспроводную сеть, датчики образуют распределительную, самоорганизующуюся систему сбора,

обработки передачи информации. Основной областью применения является контроль и мониторинг изменяемых параметров различных физических полей, сред и объектов.

Пример построения сети на основе стандартов 802.15.4/ZigBee наглядно представлен на рис. 9.10.

Рис.9.10. Пример построения сети на основе стандартов 802.15.4/ZigBee

Сенсорная сеть обладает способностью к реализации сообщений по цепочке от одного к другому, что позволяет в случае выхода из строя одного из узлов организовывать передачу информации через соседние узлы без потери качества. Сеть определяет оптимальный маршрут движения информационных потоков.

К достоинствам системы на основе сенсорных сетей можно отнести следующее:

– возможность расположения в труднодоступных местах, куда очень сложно и дорого тянуть обыкновенные проводные решения;

– оперативность и удобство развертывания и обслуживания системы;

– надежность сети в целом – в случае выхода из строя одного из них, информация передается через соседние элементы;

– возможность добавления или исключения любого количества устройств из сети;

– высокий уровень проникновения (стены, потолки) и стойкость к электромагнитным помехам (благодаря высокой частоте работы системы);

– длительное время работы без замены элементов питания.

Использование недорогих беспроводных устройств параметров открывает новые возможности для применения систем телеметрии и контроля, такие как:

– замена кабелей в системах автоматического управления;

– своевременное выявление возможных отказов исполнительных механизмов по контролю таких параметров, как вибрация, температура, давление и т.д.;

– контроль доступа к системам объекта;

– контроль параметра объекта;

– контроль за перемещением персонала по территории предприятия;

– автоматизация контроля проведения инспекций и технического обслуживания;

– контроль экологических параметров окружающей среды.

Использование беспроводных устройств позволяет создавать диспетчерскую систему, обеспечивающую оператору непрерывный доступ к информации о состоянии обслуживаемых объектов.

Применение беспроводных систем для решения задач по автоматизации и мониторингу технологических процессов

Вариант применения беспроводных систем для решения задач по автоматизации и мониторингу технологических процессов представлен на рис. 9.11 [38].

Предлагаемые системы представляют собой законченные коммутационные комплексы, встраиваемые в систему промышленного мониторинга на участке между управляющей системой и технологическим процессом, над которым необходимо осуществить мониторинг.

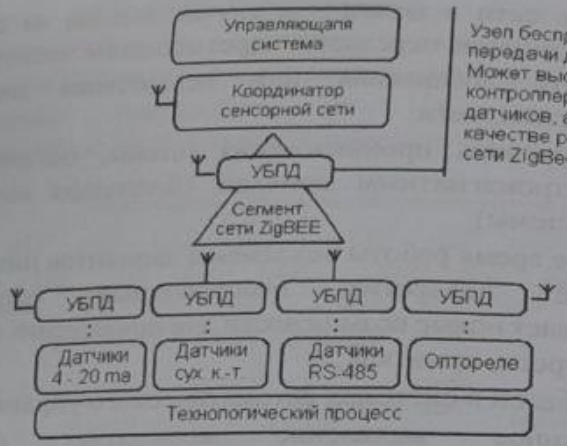


Рис.9.11. Пример интеграции беспроводных сенсорных сетей в систему мониторинга

На базе сенсорных сетей можно проектировать различные варианты построения систем, такие как:

- беспроводная система технологического учета электроэнергии;
- беспроводная система управления центральным пунктом отопления;
- беспроводная система технологического учета водоснабжения и отопления;
- беспроводная система управления очистительными сооружениями;
- беспроводная система охраны труда на вредном производстве;
- беспроводная система диспетчеризация и контроля качества и т.д.

В случае использования беспроводные сенсорные сети при учете электроэнергии в каждой точке учета устанавливается беспроводный контроллер интерфейсов, соединенный по протоколу RS-485 или любому другому протоколу с электросчетчиком (также возможно подключение к источнику импульсов для подсчета количества импульсов). Далее все данные

собираются со всех точек учета по беспроводной сети в центральный диспетчерский пульт.

Пример построения беспроводных сенсорных сетей для организации рабочих мест потребителей услуг коммерческого учета, таких как, администрация, ресурсонаблюдающие организации, управляющие компании наглядно представлен на рис. 9.12 [39].

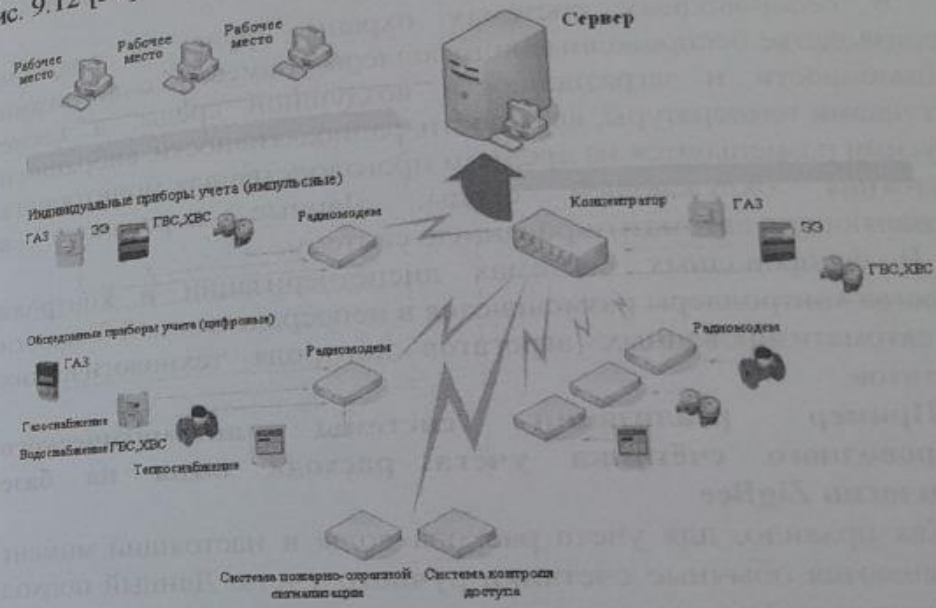


Рис. 9.12. Пример организации системы электронного учета расхода коммунальных ресурсов

В теплоснабжении беспроводные контроллеры размещаются в точках учета (пар, холодная вода, горячая вода) и точках управления (входные и выходные задвижки). Полученные параметры по беспроводной сети передаются на сенсорные устройства, а управляющие воздействия поступают через беспроводные контроллеры на исполнительные механизмы. Также возможно получение информации с конкретных мест отопления для оптимизации расхода тепловой энергии.

В беспроводных системах управления очистительного сооружения беспроводные контроллеры размещаются в точках съема информации и телеуправления (запорная арматура, контроль параметров среды и т.д.). Данные и управляющие воздействия по беспроводной сети передаются в управляющую систему и обратно. При этом возможна автоматическая блокировка стоков при выходе за границы определенных параметров.

В беспроводных системах охраны труда на вредном производстве беспроводные контроллеры совместно с датчиками запыленности и загрязненности воздушной среды, а также датчиками температуры, влажности, радиоактивности, вибрации и другими размещаются на вредном производстве для мониторинга состояния окружающей среды. Данные передаются в управляющую автоматизированную систему.

В беспроводных системах диспетчеризации и контроля качества контроллеры размещаются в непосредственной близости от автоматизированных агрегатов контроля технологических агрегатов.

Пример реализации системы автоматического беспроводного счётчика учета расхода воды на базе технологии ZigBee

Как правило, для учета расхода воды в настоящий момент применяются обычные счетчики ручного учета. Данный подход содержит целый ряд недостатков: сложность контроля, ввиду того, что счетчики располагаются на частной территории; высокие расходы на функции контроля. С учетом прогресса развития современных беспроводных технологий, применяемый подход является неэффективным. Система автоматического беспроводного счётчика расхода воды обладает следующими достоинствами: экономией времени, человеческих и материальных ресурсов; повышением эффективности труда; снижением затрат; снижением ошибок передачи данных.

В настоящее время системы автоматического учета расхода воды бывают трех типов:

Смарт-карта

Данные пользователя не регистрируются в сети. Клиенту необходимо приобрести карту. При отрицательном балансе карты,

система отключает воду. Проблема данного подхода заключаются в следующем: во-первых, водопроводная компания не может рассчитывать скорость продаж, во-вторых в случае неисправности счетчика, клиент может потреблять услуги на внося платежи, либо клиент может не получить уже оплаченную услугу.

Автоматический проводной счётчик

Данный вид счетчиков отличается от обычных тем, что отсчет осуществляется передачей электрических сигналов. Сбором сигналов, обработкой данный и мониторингом ошибок занимается информационная система, при этом несколько счетчиков передают сигналы посредством единой шины. К проблемам данного вида учета можно отнести: высокие стоимость и объемы монтажа, угрозу короткого замыкания, риск перехвата информации, сложности в сопровождении и обслуживании.

Автоматический беспроводной интеллектуальный счётчик

Этот счётчик обладает функциями измерений и обработки данных, получает и отправляет данные по беспроводным каналам связи. Обладает рядом преимуществ:

- не нужно прокладывать кабель;
- простота установки и обслуживания;
- поддерживается большинство международных стандартов передачи данных, различные радиочастоты и протоколы связи.

Однако, себестоимость подобного счетчика высока, требуется постоянная замена элементов питания, имеется ряд проблем в области безопасности передачи данных. Учитывая указанные недостатки, счетчики подобного вида практически не используются в домохозяйствах, хотя системам беспроводной связи, в настоящий момент, уделяется все больше внимания.

Система автоматического беспроводного счётчика расхода воды на базе технологии ZigBee приведена на рис. 9.13.

Клиент устанавливает автоматический беспроводной интеллектуальный водомер, который учитывает количество расходуемой воды. Через беспроводную сеть данные передаются концентратору, который передает данные центру мониторинга через модем иди общественную телефонную сеть. Сервер центра мониторинга рассчитывает стоимость потребленной воды.

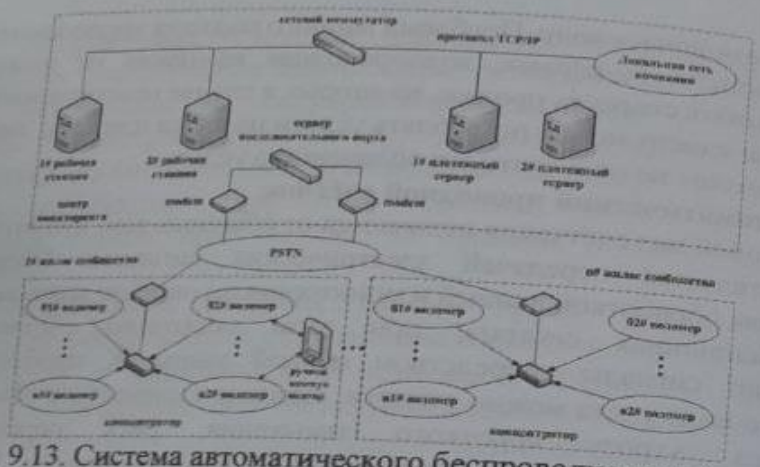


Рис. 9.13. Система автоматического беспроводного счётчика расхода воды

Альтернативный проект системы беспроводного учета воды приведен на рис. 9.14.

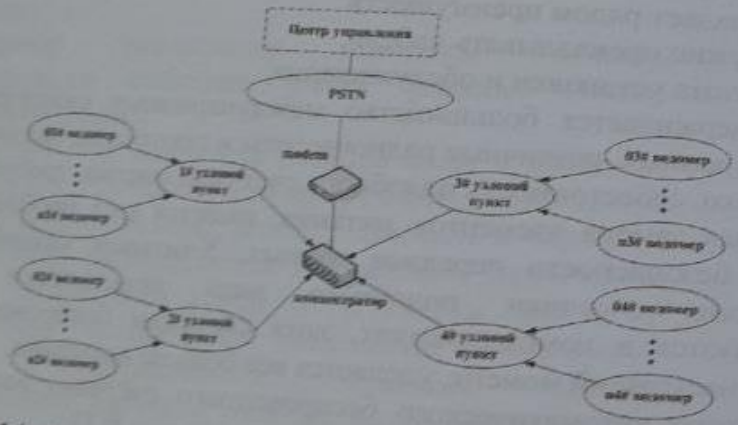


Рис. 9.14. Альтернативный проект системы беспроводного учета воды

Логически ZigBee - узлы подразделяются на 3 типа: терминальное оборудование (end device), маршрутизатор (router), PAN координатор. По физическим свойствам оборудование подразделяется на 2 части: FFD (full function device) и RFD (reduced function device). FFD может выступать в роли

координатора, маршрутизатора и терминального оборудования, RFD - в качестве узла терминала.

Структура системы

При выборе счетчика, мы остановились на модели с импульсным выходом, в том числе потому что на рынке подобный продукт уже имеется. Поэтому основная работа сводится к проектированию коммуникационной части системы между интеллектуальным счетчиком, концентратором и ручным коммуникатором.

Счетчик, высчитывает количество использованной воды. Коммуникационная часть отвечает за связь с узловым пунктом или ручным коммуникатором. Включает себя чтение совокупного количества импульсов, положение работы водомера, положение использования пользователя и т.д. (рис. 9.15).

С целью снижения себестоимости, используется один MCU, отвечающий за суммирование импульсного сигнала и связь ZigBee.

Рис. 9.15. Структура интеллектуального счётчика

Проектирование автоматического беспроводного счётчика должны быть учтены низкое потребление энергии и увеличение срок использования. Для решения вопроса рассмотрим следующие аспекты:

1. Низкое потребление энергии MCU. Выбираем микроконтроллер AVR mega128.

2. Метод – прерывание. Когда водный поток течёт через водомер, произошло импульс, MCU начнет работать. В ином случае он находится в спящем режиме.

3. Метод – Beacon. Beacon может уменьшать ненужные связи. Каждый Beacon делится на несколько Slot. Узел только обеспечивает связь с маршрутизатором или координатором в заданное время.

Концентратор данных и узловой пункт

Функцией концентратора является считывание суммарных данных интеллектуального счетчика. Обычно один концентратора достаточно для одного жилого сообщества.

Функцией узлового пункта является передача команд и данных счетчика из данного концентратора, посредством протоколов ZigBee.

Ручной коммуникатор

Основная функция ручного коммуникатора является реализация связи между платежным сервером и счетчиком (рис.9.16).

Рис. 9.16. Ручной коммуникатор

Для снижения себестоимости решения, по-прежнему используем один MCU. Он выполняет 2 задачи: во - первых, это обеспечения коммуникационной связи, во - вторых, хранение и сбор данных.

Обмен данными при этом может осуществялться двумя способами: через ZigBee сеть, посредством USB - стандарта.

С развитием вычислительной техники и средств связи наступила эра беспроводных сетей и распределенных вычислений. Пройдет еще несколько лет – и беспроводные технологии свяжут между собой огромные количество цифровых устройств, превратив информационные технологии во всепроницающую и вездесущую силу эпохи информационного общества.

Важной особенностью беспроводных сенсорных сетей является самоорганизующаяся природа таких сетей. Локально сгруппированные узлы образуют между собой сеть и через один или несколько шлюзов могут передавать данные для последующей обработки, например, в сети связи общего пользования. Наличие соединений между сенсорными сетями и сетями связи общего пользования требует проведения расчета параметров данных шлюзов, для чего необходимо исследовать природу нагрузки, циркулирующей в беспроводных сенсорных сетях.

Сенсорные сети сейчас поставляются множеством производителей, что привело к появлению разнообразных индустриальных стандартов, не обеспечивающих взаимодействия между оборудованием различных производителей.

Использование БСС в умных электросетях.

Электрическая сеть является неотъемлемой частью электроэнергетики, а также залогом устойчивости и безопасности любого государства. По мере постепенного увеличения зависимости от электроэнергии во всем мире также увеличивается потребность в обеспечении надежности и качества энергосистемы. Коммунальные предприятия, научно-исследовательские институты и ученые проводят исследования возможностей модернизации энергосистемы с целью обеспечения ее эффективности, экологической безопасности, надежности и интерактивности [40].

Умная электрическая сеть является источником для возникновения новых возможностей с далеко идущими последствиями. Следовательно, она обеспечивает безопасное внедрение в систему электроснабжения возобновляемых источников энергии (ВИЭ), электрических транспортных средств и распределенных генераторов; позволяет осуществлять

более эффективное и надежное снабжение электроэнергией на базе имеющегося спроса и предложения; предоставляет системы комплексного контроля и мониторинга; использование автоматической настройки сети для предотвращения отключений или восстановления электроснабжения (возможности самовосстановления); предоставляет потребителям возможность иметь более эффективный контроль потребления электроэнергии и принимать активное участие на рынке электроэнергии.

Датчики являются краеугольным камнем, позволяющим извлечь из умной электрической сети максимум ее потенциала. Сеть идеи «умной» электросети заключается в том, что такая сеть будет реагировать на спрос в режиме реального времени; для этого потребуются датчики, которые будут предоставлять такую информацию «в режиме реального времени». Сети БСС в качестве «умной вводной периферийной информации» могут быть важным средством продвижения технологии умных электросетей. Технология БСС в умной электросети также будет способствовать дальнейшему промышленному развитию БСС [41].

Система онлайн-мониторинга линий электропередач.

На состояние линий электропередач непосредственно влияют ветер, дождь, снег, туман, лед, молния и другие природные силы; в то же время промышленное и сельскохозяйственное загрязнение также является прямой угрозой безопасной эксплуатации линий электропередач. Рабочая среда и рабочее состояние линий электропередач являются весьма сложными системами. Поэтому возникает необходимость автоматического контроля, большего количества средств управления и защиты для автоматической подачи аварийных сигналов при возникновении аварийных ситуаций, а также требуется корректировка стратегии работы диспетчеров в соответствии с режимом работы с тем, чтобы неисправности обрабатывались на раннем этапе или были изолированными в зародыше [40, 41].

Традиционные проводные средства связи не соответствуют коммуникационным потребностям онлайн-мониторинга линий электропередачи. Сети БСС обладают отличительной способностью адаптироваться к суровым условиям, большим

охватом территорий, самоорганизацией, самостоятельной конфигурацией, большой долей независимости при практическом использовании и идеально подходят для систем мониторинга передачи данных линий электропередачи.

Обладая техническими преимуществами БСС в рамках полного диапазона, система онлайн-мониторинга нескольких элементов может своевременно отправлять предупреждения о стихийных бедствиях, быстро находить места неисправностей, получать данные о сбоях в линиях электропередач, сократить время восстановления после поломки, следовательно, повысить надежность электроснабжения. Использование БСС позволит не только эффективно предотвращать и снизить количество поломок оборудования электроснабжения при их сочетании с системами мониторинга температуры проводника, состояния окружающей среды и погоды в режиме реального времени. Сети БСС также могут предоставлять данные для поддержки эффективного электроснабжения, увеличивая и улучшая динамическую емкость линий электропередачи.

На рис. 9.17 приведена общая архитектура системы онлайн-мониторинга линий электропередач на базе БСС.

Интеллектуальный мониторинги система раннего предупреждения для подстанций.

Технология автоматизации внутренних подстанций достигла уровня международных стандартов. Большинство новых подстанций, независимо от разности уровней напряжения, внедряют интегрированные системы автоматизации [40, 41].

Отличительными чертами цифровых подстанций от обычных подстанций является оцифровка сетевой информации, стандартизация информации подстанции и передача данных по сети. Для подстанций в умных сетях больше внимания уделяется умному оборудованию электроснабжения, обмену информацией, функциональной совместимости и функциям интеллектуального использования внутренней станции.

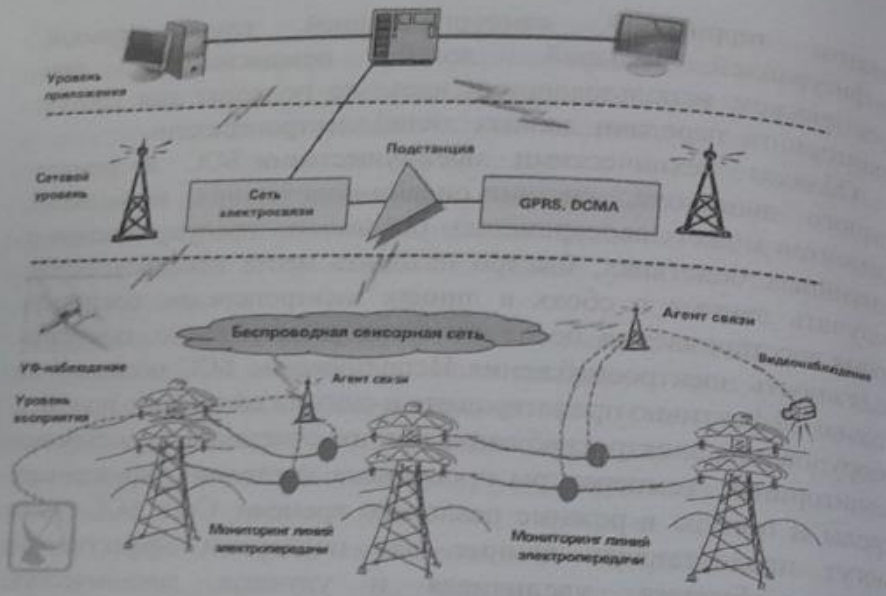


Рис. 9.17. Общая архитектура системы онлайн-мониторинга линий электропередач на базе БСС

В настоящее время внедрено множество умных контролирующих систем, которые могут улучшить управление умной подстанцией. Сюда относятся мониторинг трансформатора-выключателя-температуры, контроль утечки тока в молниеотводе, оборудование для контроля утечки электричества, контроль утечки для комбинированного электрооборудования, экологический контроль мониторинг вторичного оборудования, антикражевое оборудование и т.д. (рис. 9.18).

Прикладные решения БСС могут предоставить надежную, точную, оперативную, безопасную и достаточную информацию для управления подстанцией. Такая информация не связана с обычными данными о телеметрии электроснабжения, удаленной связью, дистанционным управлением, дистанционным регулированием. Такие решения также предоставляют информацию об оборудовании, например, состояние системы охлаждения, время срабатывания выключателя, состояние источников энергии механизма передачи, величину тока

размыкания и информацию об окружающей среде, данные видеонаблюдения и т.д.

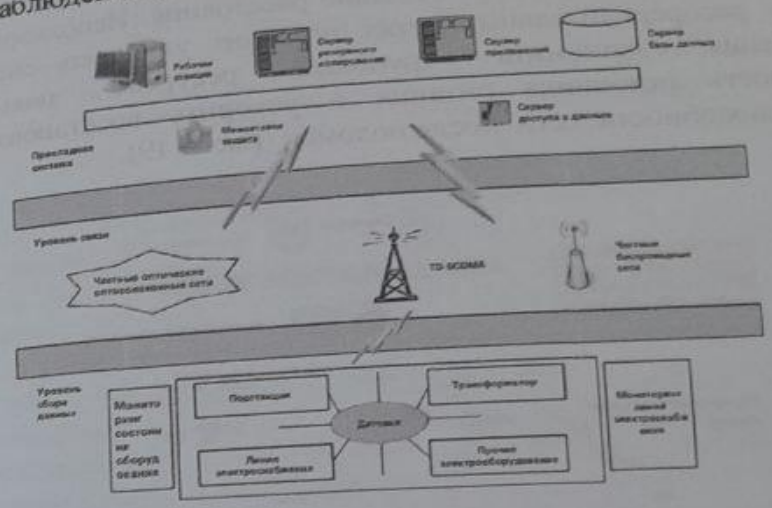


Рис. 9.18. Архитектура системы мониторинга рабочего состояния оборудования

В конечном итоге решения осуществляют оцифровку информационного описания, объединение собранных данных, передачу данных по сети, интеллектуальную обработку данных, визуализацию отображаемых данных и принятие производственных решений.

Онлайн-мониторинг и система раннего предупреждения распределительных сетей

Распределительные сети напрямую объединяют энергосистему и потребителей электроэнергии. Надежность и качество распределительной сети являются критически важными качествами надежного электроснабжения. Распределительная сеть состоит из основного оборудования, такого как фидеры, распределительные трансформаторы, автоматические выключатели, переключатели и вторичного оборудования, такого как релейная защита, автоматические устройства, измерители и счетчики, оборудование связи и управления и т.д. [40, 41].

Распределительные сети отличаются большим количеством точек подключения, большим территориальным покрытием и линиями электропередач на большие расстояния. Использование БСС в распределительных сетях позволит улучшить систему управления, сэкономить трудовые ресурсы, повысить надежность источника питания и ускорить восстановление работоспособности сети после поломок (рис. 9.19).

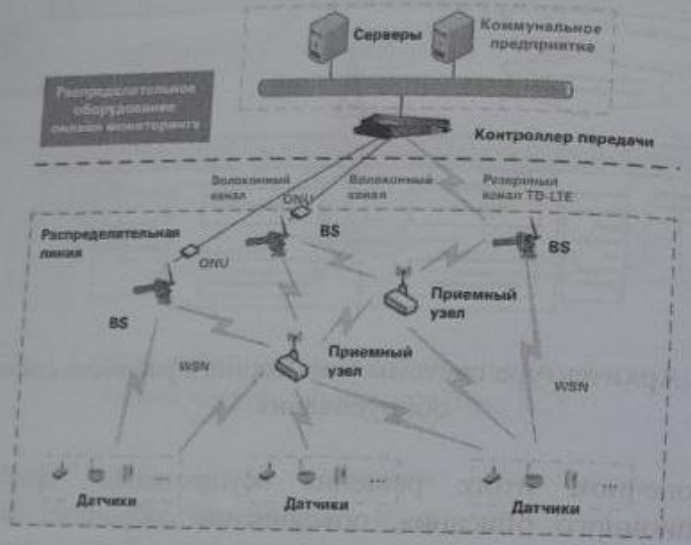


Рис. 9.19. Технология БСС, используемая в приложениях мониторинга распределительной сети

Использование технологии БСС в распределительных сетях может обеспечить защиту и поддержку строительства распределительных сетей в следующих аспектах:

1) При установке комплексного измерительного оборудования можно отслеживать изменения качества электроэнергии и перепады и пиковые нагрузки в потреблении электроэнергии, кроме того, улучшается точность и своевременность напряжения, тока, гармонических волн и других показателей.

2) При комплексном использовании RFID, систем навигации, видеонаблюдения, умных носимых технологий улучшаются

возможности мониторинга в режиме реального времени состояния распределительного оборудования и параметров окружающей среды. Это позволит улучшить возможности по определению местоположения повреждений распределительных линий.

3) Контроль состояния распределительной линии, сети подземных распределительных трубопроводов позволит достичь более высокого уровня автоматического управления эксплуатацией и антикражевыми средствами.

Услуги умного потребления электроэнергии

Основанием услуг умного потребления электроэнергии является надежная энергосистема и концепция современного управления на базе передовых технологий измерения, высокоэффективного контроля, высокоскоростной связи и быстрого накопления энергии для осуществления взаимодействия в режиме реального времени между сетями электроснабжения, снабжением конкретных потребителей, информационного потока и коммерческого потока [40, 41].

Сети БСС могут объединять терминальное оборудование поставщика с датчиками потребителей для создания полноценной интерактивной сети для получения информации о потреблении электроэнергии, а также сбора информации о параметрах электроэнергии в сложной среде. Анализ интегрированной информации на базе БСС может служить пользователю в качестве руководства или напрямую корректировать схему потребления электроэнергии, позволит обеспечить наилучшую структуру энергоресурсов, снизить стоимость электроснабжения, повысить надежность и эффективность.

Сети БСС имеют большие перспективы применения в сферах умного потребления электроэнергии, таких как умные общины, умные промышленные парки и т.д. Система сбора данных об электроэнергии является основой для умных услуг по потреблению электроэнергии. Система может осуществлять сбор нескольких видов данных массовых потребителей. Сюда относятся данные для специальных трансформаторов, средних и малых пользователей специальных трансформаторов, трехфазных коммерческих пользователей, однофазных промышленных и коммерческих пользователей, а также данные

населения и распределительных трансформаторов для проверки точек измерения. Эти данные можно объединять для построения интегрированных информационных платформ.

Архитектура системы сбора данных о потреблении электроэнергии на базе БСС представлена на рис. 9.20.

Использование сенсорных сетей для мониторинга здоровья пациента

Проблема здравоохранения является одной из самых серьезных в XXI веке. В развитых и ряде развивающихся стран возникает проблема старения населения в связи с увеличением продолжительности жизни и снижения рождаемости. Большинству же стран, включая Узбекистан, необходимо радикальное повышение качества медицинского обслуживания. При этом расходы на медицину, как правило, уже составляют значительную часть валового внутреннего продукта и исчисляются астрономическими суммами.

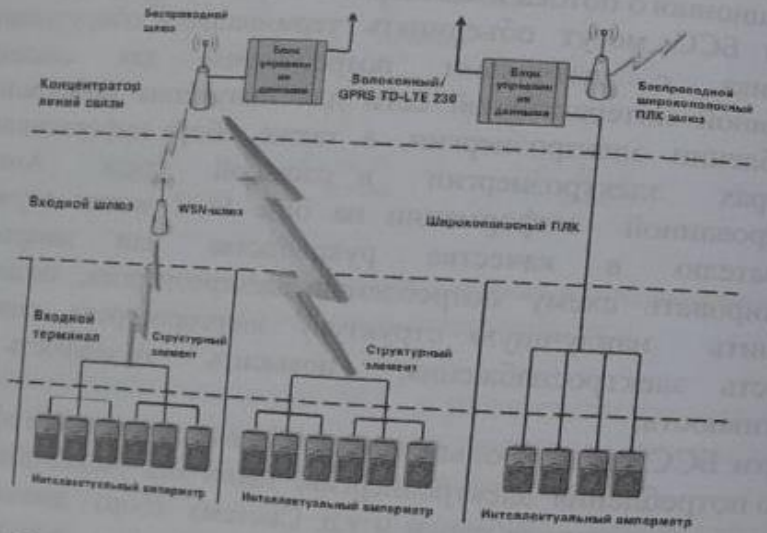


Рис. 9.20. Архитектура системы сбора данных о потреблении электроэнергии на базе БСС

Современная модель здравоохранения базируется на обслуживании населения через сети поликлиник и больниц. Такая модель сегодня уже не отвечает современным требованиям [42].

Одно из важных направлений в изменении подхода к обеспечению здоровья - мониторинг человеком собственной физиологии, физической активности и болезней. Быстрое развитие электроники, средств персональной связи, вычислительной техники, пассивных детекторов физиологического состояния, а также активных средств самолечения способствует развитию этого подхода в здравоохранении от медицинского обслуживания, сконцентрированного в госпиталях и клиниках, к мониторингу состояния здоровья, осуществляемого самим пациентом.

Беспроводные сети сенсоров, расположенных внутри, на или около тела человека и осуществляющих контроль за его состоянием, имеют большой потенциал для революционного преобразования будущих оздоровительных технологий. Беспроводные нательные сети (БНС) поддерживают обширную область приложений медицинской и потребительской электроники. Например, БНС позволяют проводить удаленный мониторинг состояния здоровья пациентов в течение длительного времени без ограничений их нормальной активности.

Применение БНС, включая разрешенные для них частоты, определяют в разных странах соответствующие регулирующие органы. Приведенные ниже данные дают общее представление о решаемых БНС задачах и используемых для этого диапазонах частот.

Коммуникационная служба медицинских имплантов (КСМИ) - Medical Implant Communication Service (MICS) используется для связи с имплантами и работает в большинстве стран в лицензируемой полосе частот 402...405 МГц. Служба беспроводной медицинской телеметрии (СБМТ) - Wireless Medical Telemetry Services (WMTS) также использует лицензируемую полосу частот. Как КСМИ, так и СБМТ не поддерживает приложения с высокой скоростью передачи данных. Для мониторинга также используется нелицензируемая полоса частот для промышленности, науки и медицины (ПНМ) - Industrial, Scientific and Medical (ISM), которая поддерживает высокоскоростные приложения и доступна повсеместно. Однако в этой полосе частот имеются большие возможности для интерференции с другими радиосредствами, включая устройства стандартов IEEE 802.1, IEEE 802.11 и IEEE 802.15.4 немедицинского назначения.

В общем случае беспроводные нательные сенсорные сети представляют собой систему разнородных устройств, расположенных в непосредственной окрестности или внутри тела потребителя и взаимодействующих между собой и с центральным координирующим узлом посредством беспроводной связи, для получения полезного эффекта для потребителя.

Устройства в сети можно разделить на сенсорные узлы, актуаторные узлы и персональные устройства. Примеры датчиков и актуаторов в БНС приведена на рис. 9.21.

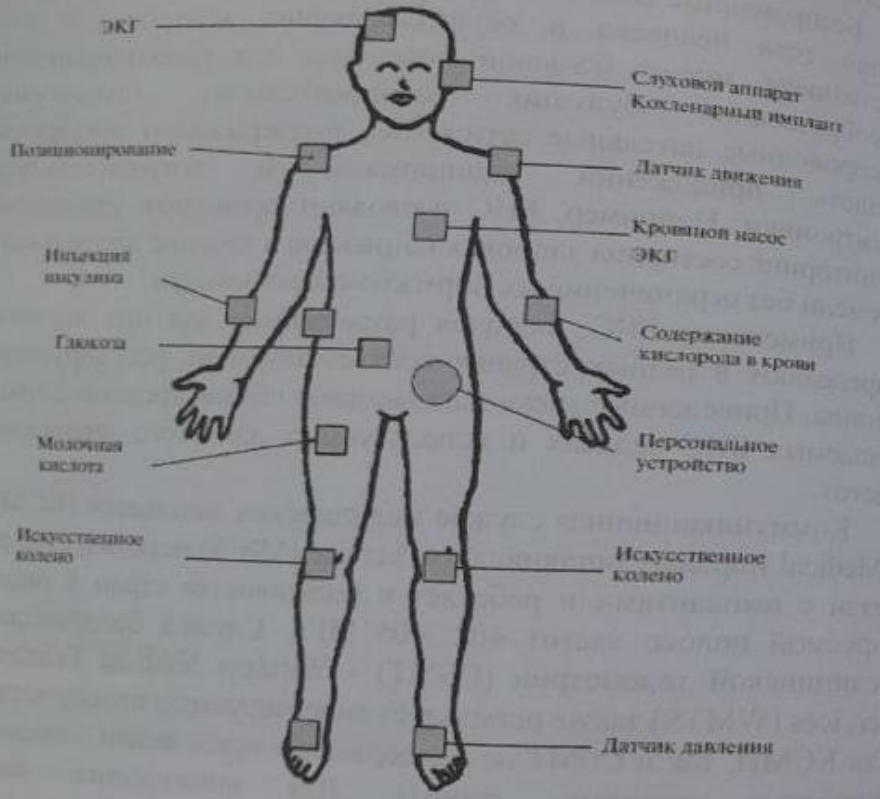


Рис. 9.21. Примеры датчиков и актуаторов в БНС

В БНС стандарта IEEE 802.15.6 различают три типа узлов.

1. Имплантированные узлы – узлы, которые помещены внутрь тела человека. Они могут быть размещены непосредственно под кожей или значительно глубже внутри тела.

2. Поверхностные узлы – узлы, которые расположены на поверхности тела или на расстоянии от него до 2 см.

3. Внешние узлы – узлы, которые не контактируют с кожей человека и расположены вне тела на расстоянии от нескольких сантиметров до 5 м.

Архитектура беспроводной нательной сенсорной сети показано на рис.9.22 и состоит из сенсорных узлов, координатора и каналов связи для передачи собранной информации по беспроводной сети, а далее через интернет в центры мониторинга, и управления и т.п.

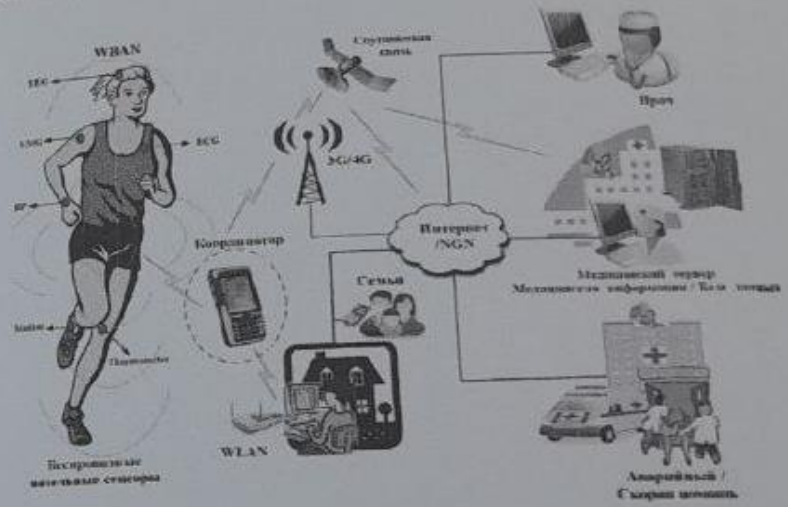


Рис.9.22. Архитектура беспроводной нательной сенсорной сети

Контрольные вопросы

1. Назовите основные области применения беспроводных сенсорных сетей.
2. Объясните функциональные уровни всепроникающих сенсорной сетей.
3. Приведите архитектуру сети 6LoWPAN и поясните её.
4. Какие системы включает в себя “Умный дом”?
5. Перечислите основные компоненты системы “Умный дом”.
6. Приведите примеры применения IoT используемые в

системе "Умный дом".

7. Приведите пример и объясните, как построить сеть на основе стандартов 802.15.4/ZigBee.

8. Приведите пример и объясните организацию системы электронного учета расхода коммунальных ресурсов.

9. Опишите особенности автоматической беспроводной системы учета воды на основе технологии ZigBee.

10. Приведите модель и архитектуру сети беспроводных нательных сенсорных сетей и поясните её.

Глава 10. СТАНДАРТЫ И КЛАССИФИКАЦИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

10.1. Утвержденные стандарты беспроводных сенсорных сетей

Стандартизация является важной предпосылкой для обеспечения функциональной совместимости не только между продуктами разных поставщиков, но и между различными решениями, приложениями и доменами (рабочими областями). Последние представляют особый интерес для IoT и БСС, поскольку общий доступ к устройствам, датчикам и действующим субъектам (узлам) из разных областей приложений, ведущих к новым междоменным (многопрофильным) приложениям, является основной целью IoT. Фактор функциональной совместимости должен приниматься в расчет на разных уровнях от отдельных компонентов до коммуникационного, информационного, функционального и коммерческого уровня [33-36].

На уровне компонентов в основном отражаются устройства, такие как датчики и приводные устройства, а также шлюзы и серверы, которые запускают приложения. Уровень связи отвечает за обмен данными между компонентами, в то время как информационный уровень представляет фактические данные. Функциональный уровень связан с функциональностью, которая может быть представлена программными приложениями, а также аппаратными решениями. На коммерческом уровне представлены описания бизнес взаимодействий. В рамках обеспечения БСС и IoT обмена информацией между «вещами» и приложениями, охватывающими различные области приложений, основной интерес представляют общие стандарты информационного и коммуникационного уровня.

Кроме того, общие функции могут использоваться в рамках различных областей применения. На уровне компонентов находятся различные типы устройств. Тем не менее, стандарты, определяющие, к примеру, форм-факторы и разъемы для модулей (например, беспроводные модули, платы управляющего процессора (CPU)) являются актуальными. Предпосылкой для

успешной стандартизации являются отобранные сценарии использования и требования.

Архитектурные стандарты необходимы для структурирования всей системы и определения соответствующих функций, информационных потоков и интерфейсов. Поскольку БСС будет использоваться в более широком контексте IoT, необходимо также учитывать стандарты IoT и процедуру стандартизации. В частности, это касается высокоскоростного протокола обмена данными, информационного и функционального уровня. Обратите внимание, что приведенный ниже перечень стандартов и процедур по стандартизации не является исчерпывающим.

По размеру физической зоны развертывания БСС относятся к классу беспроводных персональных сетей WPAN (Wireless Personal Area Networks). Важнейшим фактором производительности беспроводных сенсорных сетей является ограниченная емкость аккумуляторов, установленных в сенсорных узлах. Следует иметь в виду, что заменить батарейки часто не представляется возможным. Соответственно, на датчиках необходимо произвести простейшую первичную обработку, направленную на уменьшение количества передаваемых данных и, самое главное, на минимизацию количества циклов приема и передачи данных. Для решения этой проблемы были разработаны специальные протоколы связи [38, 39].

Наиболее известными протоколами БСС являются протоколы ZigBee Alliance.

Широкое распространение получили следующие три семейства стандартов для построения беспроводных сенсорных сетей:

- IEEE 802.11 - Wireless Local Area Network (WLAN - беспроводные локальные сети);
- IEEE 802.15 - Wireless Personal Area Network (WPAN - беспроводные персональные сети);
- IEEE 802.16 - Broadband Wireless Access (BWA - беспроводной широкополосный доступ).

Беспроводная персональная вычислительная сеть WPAN представляет собой локальную сеть с малым радиусом действия, обычно не превышающим 15...20 м, и предназначается для замены кабельных соединений между персональными компьютерами, а

также для связи с разнообразной периферией и мультимедиа устройствами (КПК, принтеры, факсы, сканеры, стереосистемы, и т.д.). Однако некоторые WPAN-сети способны работать на дальности до 100 м (ZigBee, Bluetooth). Первым стандартом, способным реализовать данные задачи, стал IEEE 802.15.1. Стандарт базируется на спецификации Bluetooth v1.x и определяет физический уровень (PHY layer) и уровень доступа к среде (MAC layer).

Следующим шагом в расширении семейства 802.15 было создание стандарта, обеспечивающего взаимодействие устройств классов 802.11 и 802.15. Вскоре для устройств, работающих в зоне WPAN-сетей, оказалось недостаточно скоростей, обеспечиваемых Bluetooth. Возникла потребность в выработке стандарта, позволяющего создавать беспроводной канал данных с пропускной способностью в десятки и сотни Мбит/с (IEEE 802.15.3). Перечисленные выше стандарты отлично подходят для передачи больших объемов информации (голоса, данных, видео) с высокой скоростью (от 1 до 200 Мбит/с).

Устройства на их основе способны работать в автономном режиме (от батарей и аккумуляторов) на дальности передачи от 10 до 100 м. Эти стандарты позволяют заменить проводные соединения в устройствах, с которыми мы имеем дело каждый день (компьютеры, вычислительные сети). Однако существует огромное множество на первый взгляд незаметных систем (разнообразные датчики, системы сбора информации и т.д.), обладающих спецификой, вследствие чего в такого рода приложениях невозможно со стопроцентной эффективностью использовать упомянутые технологии. Для реализации подобных задач был выработан стандарт IEEE 802.15.4 (ZigBee) для низкоскоростных WPAN-сетей.

Очевидно, что беспроводные сети короткого радиуса действия будут взаимодействовать между собой. Планируется разработать оборудование, выполняющее функции шлюза между разными беспроводными сетями. Так, если система безопасности, построенная на ZigBee, обнаружит злоумышленника, она соединится с сетью IEEE 802.11, чтобы известить об этом компьютер, а тот, в свою очередь, передаст SMS на мобильный телефон хозяина или позвонит в службу охраны. Сравнительные

характеристики стандартов семейства 802.15 и стандарта 802.11b приведены в таблице 10.1.

Таблица 10.1

Сравнение стандартов семейств 802.15. и 802.11b

Стандарт	802.15.4 Zigbee			802.15.1 Bluetooth	802.11b Wi-Fi
Приложения	Мониторинг, управление			Голос, данные	Данные, видео
Частота, ГГц	0.868	0.915	2.4		
Преимущества	Цена, энергосбережение, размеры			Цена, передача голоса	Скорость, гибкость
Макс. скорость	20 кбит/с	40 кбит/с	250 кбит/с	1 мбит/с	11 мбит/с и более
Дальность, м	10-100, 1000			100	100
Чувствительность, дБм (сред).	-92			-70	-76
Размер стека, кБайт				>250	>1000
Срок службы батареи, дней	100-1000			1-7	0,5-1

Исходя из приведенных характеристик, ближайшими конкурентами являются технологии Bluetooth и ZigBee. Соответственно, примерно схожи области их применимости - беспроводные устройства домашнего и промышленного назначения, включая системы дистанционного управления, компьютерной периферии и т.д. Однако в отличие от технологии Bluetooth, ZigBee разработана для приложений, одним из ключевых требований которых является низкое энергопотребление. Периоды активности устройств, выполненных по технологии ZigBee, могут быть крайне малы, что обеспечивает продолжительный срок службы батарей.

Кроме того, микросхемы Wi-Fi и Bluetooth слишком дороги для организации на их основе крупных сетей разнообразных устройств в масштабах предприятий и офисных зданий, а стандарт 802.15.4/ZigBee позволяет разрабатывать беспроводные

интерфейсы с минимальными затратами, что обеспечивается простотой схемотехники, минимальным количеством внешних пассивных элементов, программным обеспечением стека, использующим отведенный ему объем памяти с высокой эффективностью (таблица 10.1). Стандарт позволяет создавать сети с многоячейковой топологией, таким образом обслуживая очень большое число узлов и увеличивая дальность связи без дополнительных затрат на усилители мощности.

Технология ZigBee не предназначена для передачи больших объемов информации, как Wi-Fi или Bluetooth. Однако для передачи, например, показаний датчиков, объем которых редко превышает десятков байт, не требуется высоких скоростей - в этом случае обязательны высокие показатели по энергопотреблению, цене и надежности. Большинство устройств ZigBee будет работать по следующему алгоритму: устройство находится в «спящем» состоянии практически все время, обеспечивая оптимальный режим энергосбережения. При поступлении новой информации либо во время очередного сеанса связи устройство активизируется, быстро передает данные и снова переходит в режим пониженного энергопотребления.

Типовые временные задержки при этом составляют 30 мс для подключения нового устройства к сети, 15 мс для перехода из «спящего» в активное состояние, 15 мс для доступа к каналу. Так удается продлить срок службы батарей до 10 лет и более в зависимости от типа приложения и длительности рабочего цикла, причем ток при передаче может составлять порядка 15...30 мА, а в «спящем» режиме - менее 2 мкА. В результате, задержки по отклику настолько малы, что человек, войдя в комнату и щелкнув переключателем беспроводной связи ZigBee, даже не заметит, что свет появился почти мгновенно, в то время как задержки при подключении устройствк сети Bluetooth составляют порядка 3 с (рис. 10.2).

Однако, благодаря ультранизкому потреблению энергии в спящем режиме, беспроводные сенсорные сети, питаемые от внешней среды, могут использовать прерывистый рабочий цикл, изображенный на рис. 10.3. Энергия хранится в буфере (рис.10.3,а) (конденсаторы, батареи) и используется для выполнения измерительного цикла, как только энергии в буфере становится

достаточно (рис.10.3,б и рис.10.3,в). Далее система опять возвращается к спящему режиму (рис.10.3,г), ожидая нового измерительного цикла.

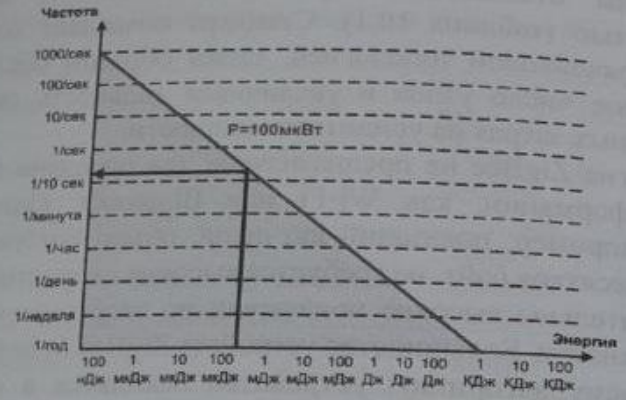


Рис. 10.2. График потребления энергии узлом БСС

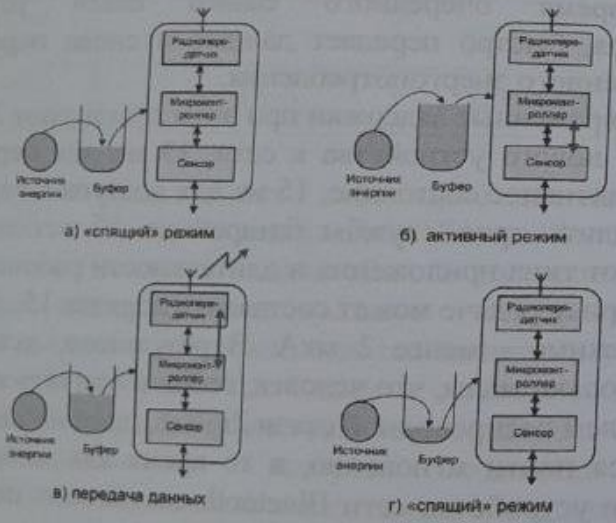


Рис.10.3. Рабочий цикл в БСС

Для питания узлов сенсорной сети от окружающей энергии необходимо снизить потребления энергии датчиками

(сенсорами/актуаторами), микроконтроллером и радиопередатчиком. В последние годы значительный прогресс в этом направлении был достигнут производителями микроконтроллеров и радиочастотных чипов (Atmel, Microchip, Texas Instruments и др.) как для рабочего, так и для холостого режима. Пример типичного потребления энергии узлом беспроводных сенсорных сетей приведен на рис.10.4.

Можно выделить три типичных значения потребляемой мощности:

1) 1-5 мкВт: потребление энергии в «спящем» режиме;
2) 500 мкВт - 1 мВт: потребление энергии в активном режиме;
3) 50 мВт: пик передачи энергии.

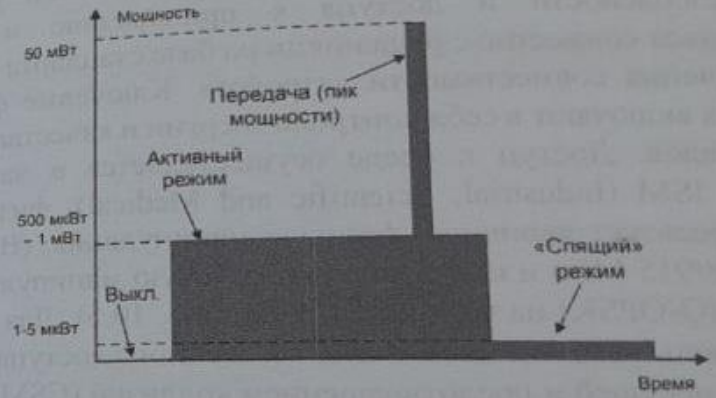


Рис. 10.4. Пример типичного потребления энергии узлом беспроводных сенсорных сетей

Анализ приведенной диаграммы позволяет сделать следующие выводы. Во-первых, минимальная мощность источника энергии из внешней среды для построения жизнеспособных беспроводных узлов должна быть порядка 1-5 мкВт, что соответствует достаточной величине для холостого режима микропроцессора и радиочастотного чипа.

Во-вторых, современные источники энергии из внешней среды не могут обеспечивать беспроводные сенсорные сети энергией, достаточной для активного режима (потребление энергии в 500 мкВт - 1 мВт против 10-100 мкВт для выходной

мощности таких источников).

Стандарт IEEE 802.15.4 для беспроводных низкоскоростных персональных сетей (WPAN) определяет физический уровень PHY и уровень доступа к среде MAC. Уровень PHY обеспечивает доступ к физической среде распространения радиосигнала: задает тип модуляции, скорость и другие параметры сигнала, непосредственно осуществляет прием и передачу. Уровень MAC осуществляет добавление и вывод из сети устройств, контролирует доставку пакетов данных, обеспечивает автоматическое подтверждение приема (квитирования) данных, реализует механизмы доступа к каналу передачи, поддерживает 128-битное AES- шифрование и другие функции.

Спецификация стека ZigBee определяет сетевой уровень, уровни безопасности и доступа к приложению и может использоваться совместно с решениями на базе стандарта 802.15.4 для обеспечения совместимости устройств. Ключевые функции PHY-уровня включают в себя контроль энергии и качества связи и анализ каналов. Доступ к среде осуществляется в частотных диапазонах ISM (Industrial, Scientific and Medical), физический уровень использует двоичную фазовую манипуляцию (BPSK) на частотах 868/915 МГц и квадратичную фазовую манипуляцию со смещением (O-OPSK) на частоте 2,4 ГГц (рис. 10.5). Для доступа к каналу используется механизм множественного доступа к среде с контролем несущей и предотвращением коллизий (CSMA-CA).

Данный механизм, основанный на определении состояния канала связи перед началом передачи, позволяет существенно сократить (но не устранить) столкновения, вызванные передачей данных одновременно несколькими устройствами. Стандарт 802.15.4 основывается на полудуплексной передаче данных (устройство может либо передавать, либо принимать данные), что позволяет использовать метод CSMACA только для предотвращения коллизий, а не для их обнаружения.

Дальность распространения сигнала обычно составляет 30 ...50 м, однако при использовании внешних усилителей мощности, малошумящих усилителей и согласованной антенны дальность может достигать 100 м без существенных потерь в скорости. Пропускная способность напрямую зависит от выбранной частоты. Максимальная скорость передачи, равная 250 Кбит/с,

достигается в диапазоне 2,4 ГГц (16 каналов с шагом 5 МГц). Для частот 868 МГц (1 канал) и 902 - 928 МГц (10 каналов с шагом 2 МГц) скорости передачи равны соответственно 20 Кбит/с и 40 Кбит/с.

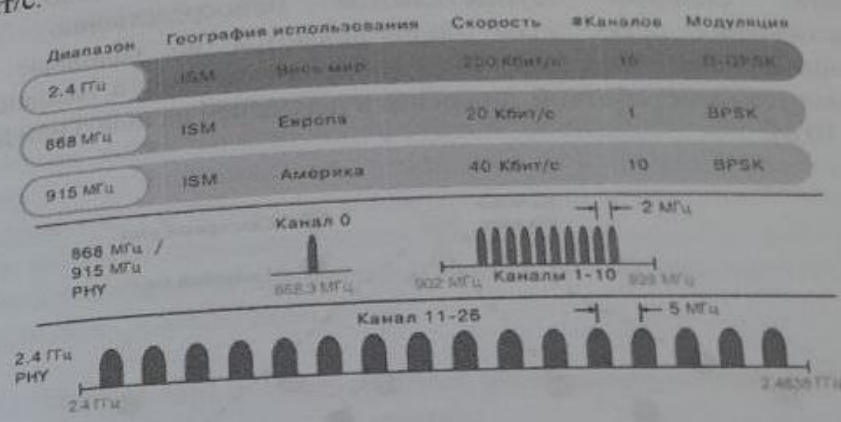


Рис. 10.5. Краткая характеристика стандарта 802.15.4

10.2. Классификация беспроводных сенсорных сетей

Беспроводные сенсорные сети могут быть классифицированы на основе различных концепций в зависимости от типа узлов в сети или в зависимости от окружающей среды, в которой они развернуты, а также в зависимости от метода развертывания или в зависимости от расположения узлов в сети и т.д. Выделим некоторые принципиальные для дальнейшей разработки алгоритмов выбора головного узла характеристики БСС [36].

Гомогенные и гетерогенные БСС. Сенсорные сети могут быть разделены на два основных типа гомогенные (однородные) и гетерогенные БСС (неоднородные) в зависимости от составляющих их узлов. В однородных беспроводных сенсорных сетях все сенсорные узлы одинаковы с точки зрения энергии батареи и аппаратной сложности. Гетерогенные же сенсорные сети могут содержать два, три или больше типов узлов, соответственно с различными энергетическими и функциональными возможностями.

Одноранговые и иерархические сети. БСС могут быть классифицированы в зависимости от структуры сети на одноранговые и иерархические. В одноранговой сети все узлы выполняют одинаковые задачи и передача данных на шлюз или базовую станцию осуществляется непосредственно. В иерархических сетях узлы подразделяются на головные и сенсорные узлы. Сенсорные узлы собирают данные, а головные занимаются их обработкой, анализом и передачей на шлюз или БС (рис. 10.6).

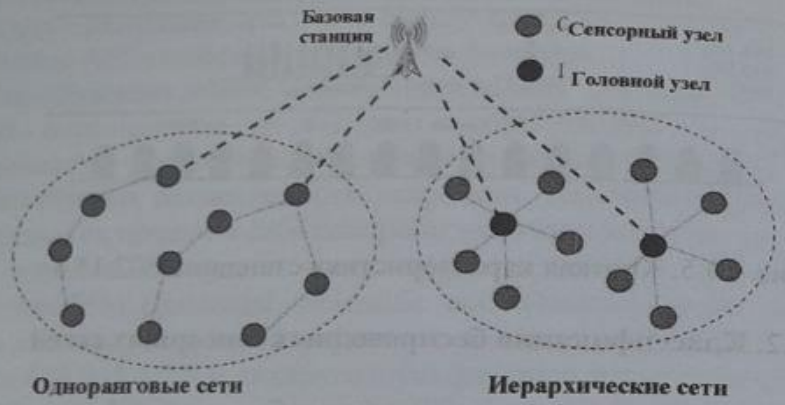


Рис. 10.6. Классификация БСС в зависимости от структуры сети

Случайное и детерминированное размещение сенсорных узлов. БСС могут быть классифицированы в зависимости от метода размещения сенсорных узлов. При случайном размещении сенсорные узлы могут быть случайным образом разбросаны по некоторой области. Детерминированное размещение предполагает размещение узлов в соответствии с предварительно определенным планом построения сети. Естественно, что алгоритмы распределения данных между сенсорными узлами в первом и втором случае могут быть существенно различны.

Статичность и мобильность. Потребность в мониторинге людей, животных и вещей в целом вызывает необходимость применения мобильных узлов в БСС. Сенсорные узлы, используемые в беспроводных сенсорных сетях, могут быть

стационарным или мобильным. При этом мобильные сенсорные узлы могут перемещаться с места на место, из-за чего связь между двумя узлами в сенсорной сети с мобильными узлами может быть очень сложной.

Двумерные и трехмерные беспроводные сенсорные сети. БСС могут быть также классифицированы на двумерные и трехмерные беспроводные сенсорные сети. Несмотря на то, что большинство существующих работ в области беспроводных сенсорных сетей в настоящее время посвящены двумерному пространству, на самом деле такие сети работают в трехмерном пространстве, особенно с учетом появления новых приложений, таких как летающие сенсорные сети. Таким образом, требуется оценить возможность применения известных протоколов для *2D* в области БСС, работающих в *3D*.

10.3. Модель OSI в приложениях беспроводных сенсорных сетей

Сетевая модель OSI

OSI (базовая эталонная модель взаимодействия открытых систем) представляет собой концептуальную модель, которая описывает и стандартизирует внутренние функции системы связи, разделяя ее на абстрактные уровни [36].

Модель OSI состоит из семи уровней. Любой протокол может взаимодействовать со своим собственным протоколом уровня или отдельными протоколами верхнего или нижнего уровня (таблица 10.2).

Прикладной уровень - это верхний уровень модели, который позволяет пользовательским приложениям взаимодействовать с сетью.

Уровень представление преобразует данные, полученные из сети, в формат приложения, в то время как приложение преобразует запросы в формат для передачи по сети. Кодирование/декодирование данных также может выполняться на этом уровне.

Сеансовый уровень отвечает за поддержание сеанса связи и взаимодействия в течение длительного времени.

Транспортный уровень предоставляет множество функций для надежной передачи данных от отправителя к получателю.

Сетевой уровень определяет путь передачи данных. Маршрутизатор работает в этом слое.

Канальный уровень. Спецификация IEEE 802 делит этот уровень на два подуровня: уровень логической связи (LLC - Logical Link Layer) и уровень доступа к среде (MAC).

LLC проверяет и обеспечивает передачу данных по соединению и выполняет функцию интерфейса между MAC и сетевым уровнем.

MAC является нижним подуровнем канального уровня и выполняет функцию интерфейса между физическим уровнем и LCC. Обеспечивает механизмы управления MAC-адресацией и подключением к каналу.

Таблица 10.2

Сетевая модель OSI

Модели OSI		
Тип данных	Уровни	Функции
Информация	7. Прикладной (application)	Подключение к сетевым службам
Поток	6. Представление (presentation)	Представление и шифрование данных
Сеансы	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь и надежность между конечными точками
Пакеты/ датаграммы	3. Сетевой (network)	Сетевая маршрутизация и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа с физической средой передачи, сигналами и двоичными данными

Физический уровень - это нижний уровень модели OSI, который позволяет передавать данные, передаваемые в двоичном коде, с одного устройства на другое. Он передает электрические или оптические сигналы по кабелю или радиоэфиру, принимает их и соответствующим образом преобразует в биты.

Упрощенная модель OSI

Стандарт IEEE 802.15.4 определяет только два подуровня модели OSI - физический уровень и уровень MAC. Для описания остальных уровней используется спецификация, разработанная ZigBee Alliance, которая определяет упрощенную пятиуровневую модель.

Документ IEEE 802.15.4 описывает частоты, аппаратные особенности и прочие параметры сети, в то время как документ ZigBee содержит в себе описание процесса сетевого управления, параметры безопасности, а также немаловажные понятия совместимости и профилей устройств [36].

Особенностью сетей IEEE 802.15.4-2006 является возможность реализации практически любой топологии, включая сотовую.

Стек протоколов ZigBee построен по принципу иерархической семиуровневой модели протоколов передачи данных в открытых системах OSI (Open System Interconnection). Стек включает в себя уровни стандарта IEEE 802.15.4, отвечающие за реализацию канала связи, и программные сетевые уровни и уровни поддержки приложений, определенные спецификацией Альянса ZigBee (рис. 10.7).

Архитектура IEEE 802.15.4 определяет в свою очередь ряд уровней, призванных упростить стандарт. Каждый уровень ответственен за одну часть стандарта и предоставляет услуги вышерасположенному уровню.

Интерфейсы между уровнями определяют логические связи, описанные в данном стандарте.

Документ IEEE Std 802.15.4 определяет спецификации физического уровня (PHY) и подуровень доступа к сетевой среде MAC (Medium Access Control) для низкоскоростной беспроводной среды с портативными переносными устройствами и максимальным расстоянием доступности POS (Personal Operating Space) равным 10 метрам. При этом предполагается, что при более

низких скоростях передачи возможна работа и на больших расстояниях (< 100 м).

Таблица 10.3

Модель IEEE 802

	Упрощенная модель Zigbee	Модель IEEE 802
1	Прикладной	Верхние уровни
2	Профили приложений	
3		
4		
5	Сетевой	
6	Канальный	Подуровень управления логической связью (LLC)
		Подуровень управления соединением к среду передачи (MAC)
7	Физический	Физический

Физический уровень PHY предоставляет два вида услуг: информационный сервис PHY и сервис управления, обеспечивающий взаимодействие с сервисом PLME (Physical Layer Management Entity) точки доступа SAP (известный под названием PLME-SAP). Информационный сервис PHY делает возможным передачу и прием через радиоканал протокольных блоков данных PPDU (Protocol Data Unit).

Стандарт определяет следующие скорости передачи данных: 250 кбит/с, 100кбит/с, 40 кбит/с и 20 кбит/с. Прием и передача данных по радиоканалу осуществляется на физическом уровне PHY, определяющем рабочий частотный диапазон, тип модуляции, максимальную скорость, число каналов: O-QPSK - квадратичная фазовая манипуляция со смещением для диапазона 2,4 ГГц (16 каналов, 250 Кбит/с), BPSK - двоичная фазовая манипуляция для частот 915 МГц (10 каналов, 40 Кбит/с) и 868 МГц (1 канал, 20 Кбит/с).

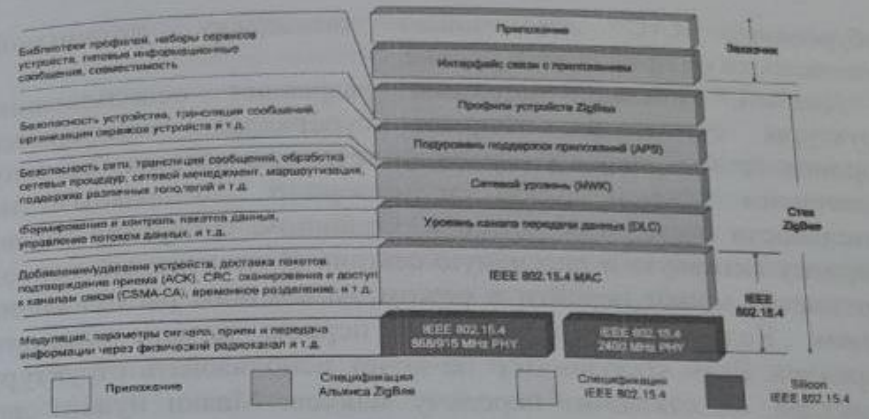


Рис. 10.7. Архитектура стека ZigBee/802.15.4

Уровень PHY осуществляет активацию/дезактивацию приемопередатчика, детектирование энергии принимаемого сигнала на рабочем канале, выбор физического частотного канала, индикацию качества связи при получении пакета данных и оценку свободного канала для реализации протокола CSMA-CA (протокол множественного доступа к среде с контролем несущей и предотвращением коллизий). Важно понимать, что стандарт 802.15.4 - это физическое радио (микросхема радиоприемопередатчика), а ZigBee - это логическая сеть и программный стек, обеспечивающие функции безопасности и маршрутизации [38,39].

MAC уровень стека

Субуровень MAC предоставляет два сервиса: информационный MAC-сервис и сервис управления MAC-уровня - обеспечение интерфейса для субуровня управления MLME (MAC Level Management Entity) для точек доступа (известных как MLME-SAP). Информационный сервис MAC обеспечивает прием и передачу протокольных блоков данных MAC-уровня (MPDU) с помощью информационного сервиса физического уровня.

Характерными особенностями субуровня MAC являются использование управления маяками (beacon), реализация доступа, управление GTS (Guaranteed Time Slot), проверка корректности кадров, подтверждение доставки кадров и т.д. Кроме того,

субуровень MAC обеспечивает поддержку механизмов безопасности на прикладном уровне.

Данный стандарт опционно разрешает использование структуры суперкадра. Формат суперкадра определяется координатором. Суперкадр ограничен сетевыми маяками (beacon), посланными координатором и содержит 16 равных по длительности временных доменов. Опционно суперкадр может содержать активную и пассивную секции. В неактивный период координатор может перейти в режим экономного расходования питания. Кадр-маяк передается в первом домене каждого суперкадра. Если координатор не хочет использовать структуру суперкадра, он отключит передачу маяков. Маяки нужны для синхронизации подключенных устройств, чтобы идентифицировать PAN, и описать структуру суперкадров. Любое устройство, желающее осуществлять обмен в период CAP (Contention Access Period) между двумя маяками, конкурирует за это право с другими устройствами, использующими доменный механизм CSMA-CA. Все обмены завершаются до момента следующего сетевого маяка [40].

Характеристики MAC уровня:

– 64-битная IEEE адресация, 16-битная адресация внутри локальных сетей (теоретически максимальное количество устройств в сети 264, организация простых сетей при использовании 16-битной локальной адресации с более чем 65 тыс. (216) устройств).

Способы адресации:

– идентификаторы: сетевой ID + ID устройства (топология «Звезда»);

– идентификатор Отправителя/Получателя (передача между равноправными узлами);

– вхождение в сеть/выход из сети автоматическая/полуавтоматическая организация сети;

– формат пакетов сообщений сети ZigBee, максимальная полезная загрузка одного пакета данных составляет 104 байта данных, максимальная длина кадра равна 127 байт;

– уровни безопасности:

– свободный доступ к сети;

– список контроля доступа;

– таймеры определения задержек при передаче и актуальность пакетов данных;

– шифрование с использованием 128-битного симметричного ключа AES;

– механизм доступа в сеть, функции временного разделения и гарантированных временных интервалов, доступ к каналу посредством протокола CSMA-CA;

– поддержка сетевых топологий, включая соединения типа «точка – точка», «звезда», многоячейковой и кластерной топологий;

– оповещение о поступлении пакета данных, подтверждение приема (ACK), 16-битный контроль ошибок (CRC);

– пакетный/потоковый режимы передачи [41].

Главным достоинством технологии Bluetooth Low Energy (BLE) является специальный алгоритм управления энергопотреблением. Устройства, использующие BLE, будут потреблять намного меньше энергии, чем другие Bluetooth - устройства предыдущих поколений. Во многих случаях одной миниатюрной батарейки типа «таблетка» будет достаточно для работы устройства более года. Таким образом, непрерывно работающие датчики (например, датчик температуры), смогут передавать информацию на другие устройства, такие как сотовый телефон или планшетный компьютер [43].

Основными областями применения BLE являются устройства обеспечения безопасности, управления электроприборами и отображения показаний, датчики с батарейным питанием, домашние медицинские приборы, спортивные тренажеры.

К спецификации BLE проявляется большой интерес. В частности, рабочая группа 6LoWPAN рассматривает BLE как одну из значительных составляющих концепции «Интернет вещей» и приступила к разработке спецификации, позволяющей транслировать пакеты IPv6 посредством BLE, аналогично взаимодействию IPv6 со стандартом IEEE 802.15.4.

Как и классический стек протоколов Bluetooth, стек BLE состоит из двух основных частей: контроллера (Controller) и узла сети (Host). Контроллер включает в себя физический и канальный уровень и может быть реализован в виде системы-на-кристалле (СнК) с интегрированным беспроводным трансивером. Часть

стека, именуемая узлом сети, реализуется программно на микроконтроллере приложений и включает в себя функциональность верхних уровней:

- уровень логической связи (Logical Link Control – LLC);
- протокол адаптации (Adaptation Protocol – L2CAP);
- протокол атрибутов (Attribute Protocol – ATT);
- протокол атрибутов профилей устройств (Generic Attribute Profile – GATT);
- протокол обеспечения безопасности (Security Manager Protocol – SMP);
- протокол обеспечения доступа к функциям профиля устройств (Generic Access Profile – GAP).

Взаимодействие между верхней и нижней частями стека осуществляется через интерфейс Host Controller Interface (HCI). Дополнительная функциональность прикладного уровня может быть реализована поверх уровня узла сети. Структура стека протоколов BLE представлена на рис. 10.8.

Следует также отметить, что спецификация Bluetooth 4.0 предусматривает одно- и двухрежимную работу устройств. При этом однорежимные контроллеры классического Bluetooth и BLE не совместимы. Для обеспечения совместимости контроллер должен быть двухрежимным. Что касается узлов сети, то они являются, как правило, однорежимными.

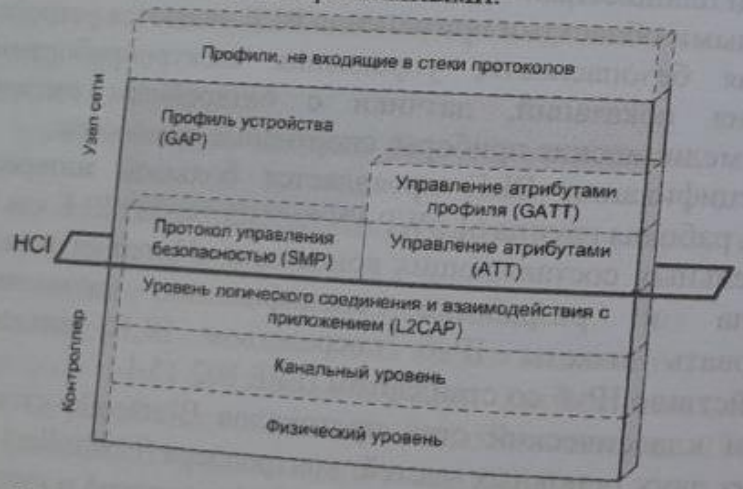


Рис. 10.8. Стек протоколов Bluetooth Low Energy (BLE)

Устройства BLE работают в диапазоне 2,4 ГГц. В стандарте определено 40 частотных каналов с расстоянием в 2 МГц между каналами. На физическом уровне применена GFSK-модуляция (частотная модуляция с гауссовой фильтрацией) с индексом модуляции в пределах от 0,45 до 0,55, что позволяет уменьшить пиковое потребление энергии.

Скорость передачи на физическом уровне 1 Мбит/с. В стандарте BLE чувствительность приемника определена как уровень сигнала на приемнике, при котором частота битовых ошибок (Bit Error Rate – BER) достигает уровня 10^{-3}. Она должна составлять – 70 дБм или лучше.

На канальном уровне различают два типа каналов – каналы объявления и каналы данных. Каналы объявления используются для поиска устройств, установления соединения, широковещательных передач, тогда как каналы данных используются для двунаправленного обмена между устройствами.

Для каналов объявления выделено три частотных канала в центре полосы, что минимизирует перекрытие с каналами 1, 6 и 11 стандарта IEEE 802.11. Остальные 37 каналов используются для обмена данными. Для снижения влияния помех, многолучевого распространения, а также для снижения влияния соседних устройств при обмене данными предусмотрено скачкообразное переключение частоты.

На рис 10.9 приведен формат пакета данных BLE.

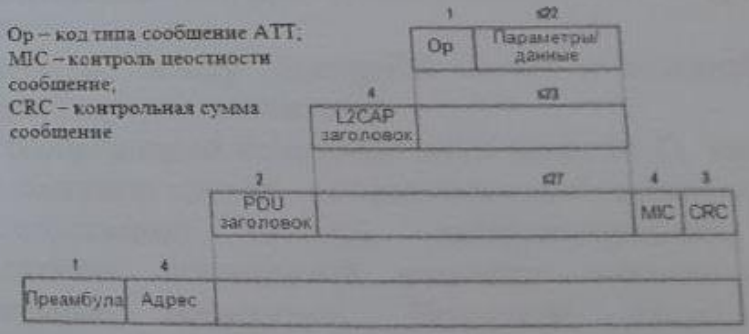


Рис. 10.9. Формат пакета данных BLE

В BLE для передачи широковещательных пакетов применяются каналы объявления. Любое устройство, передающее

пакеты по этим каналам, называется объявителем. Передача пакетов по каналам объявлений происходит только в специально выделенных интервалах времени, которые называются событиями объявлений. Во время этих событий устройство-объявитель передает пакеты объявлений последовательно по каждому из трех частотных каналов. Устройства, единственной функцией которых является прием пакетов объявлений, называются сканерами.

Контрольные вопросы

1. Какие стандарты беспроводной связи используется для построения сенсорных сетей?
2. Для чего предназначены беспроводные персональные вычислительные сети WPAN?
3. Объясните рабочий цикл БСС.
4. Объясните особенности потребления энергии узлом БСС.
5. Перечислите основные характеристики стандарта 802.15.4
6. Как классифицируется БСС?
7. Поясните основные принципиальные характеристики БСС для выбора головного узла сенсорной сети.
8. Какие функции выполняют канальные и физические уровни в спецификации IEEE 802.15.4?
9. Приведите и объясните архитектуру стека ZigBee/802.15.4.
10. Приведите и объясните стек протоколов Bluetooth Low Energy (BLE)

Глава 11. АРХИТЕКТУРА БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

11.1. Архитектура беспроводных сенсорных сетей, типы узлов, соединений и способы передачи данных

Стандартизацией сенсорных сетей занимаются многие международные организации, среди которых ISO, IEC, ITU-T, IEEE и др. Так исследовательская группа по сенсорным сетям SGSN (Study Group on Sensor Networks) объединённого технического комитета №1 ISO/IEC JTC 1 (Joint Technical Committee 1) определила базовую архитектуру сенсорной сети и ее основные интерфейсы (рис. 11.1) [44].

Как видно из рис. 11.1, сенсорный узел состоит из:

- аппаратного обеспечения;
- базового программного обеспечения;
- прикладного программного обеспечения.

В составе архитектуры определены четыре базовых интерфейса:

1. Интерфейс между базовым и прикладным программным обеспечением сенсорного узла.
2. Интерфейс между базовым программным обеспечением и аппаратным обеспечением сенсорного узла (сенсоры, актуаторы и/или коммуникационный узел и т.д.).
3. Беспроводные или проводные интерфейсы между узлами в сенсорной сети.
4. Интерфейс между сенсорной сетью и внешней средой (провайдеры услуг, пользователи).

Узел беспроводной сенсорной сети (рис. 11.1), называемый сенсором, содержит датчик, воспринимающий данные от внешней среды (собственно сенсор), микроконтроллер, память, радиопередатчик, автономный источник питания и иногда исполнительные механизмы. Возможна также передача управляющих воздействий от узлов сети к внешней среде [44]. Модель узла сенсорной сети и его аппаратные составляющие пиведенқ на рис. 11.2.

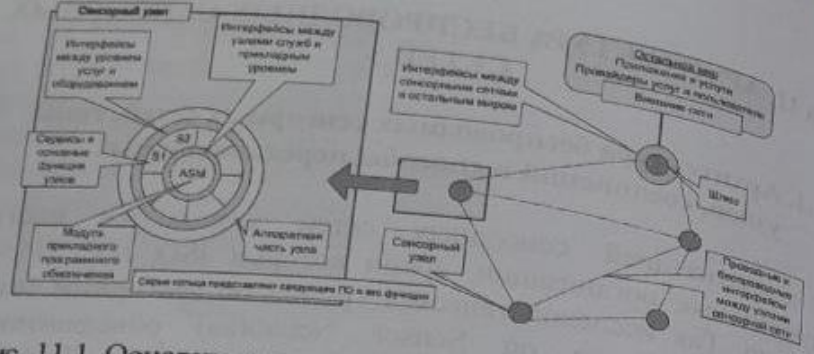


Рис. 11.1. Основные элементы и интерфейсы сенсорной сети

Рис. 11.2. Модель узла сенсорной сети и его аппаратные составляющие

Сенсорный узел представляет собой плату размером обычно не более одного кубического дюйма. На плате размещаются процессор, память - флэш и оперативная, цифро-аналоговые и аналого-цифровые преобразователи, радиочастотный приемопередатчик, источник питания и различные датчики, актуаторы. Таким образом, аппаратная часть узла беспроводной сети может быть разделена на следующие четыре подсистемы (рис. 11.3):

1) *коммуникационная подсистема* - обеспечивает беспроводные соединения с другими узлами в сенсорной сети и содержит радио приемопередатчик;

2) *вычислительная подсистема* - обеспечивает обработку данных и функциональность узла и состоящая из микроконтроллера MCU, в состав которого входят процессор,

оперативная SRAM, энергонезависимая EEPROM и флэш-память, аналого-цифровой преобразователь ADC, таймер, порты ввода/вывода;

3) *сенсорная подсистема* - обеспечивает соединение сенсорного беспроводного узла с внешним миром, в состав которой могут входить аналоговые и цифровые сенсоры, актуаторы;

4) *подсистема электропитания* - обеспечивает энергетическое снабжение всех элементов беспроводного сенсорного узла и включает устройства генерации и аккумулирования энергии, а также регулировки напряжения.

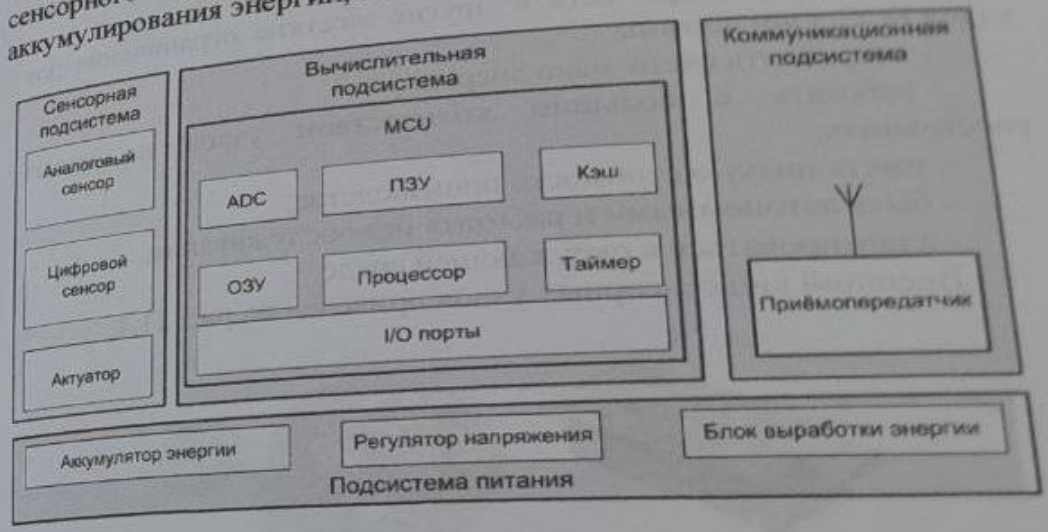


Рис. 11.3. Узел беспроводной сенсорной сети

Датчики могут быть самыми разнообразными. Чаще других используются датчики температуры, давления, влажности, освещенности, вибрации, местоположения, реже - магнитоэлектрические, химические (например, измеряющие содержание CO, CO_2, уровень радиационного фона), звуковые и некоторые другие. Набор применяемых датчиков зависит от функций, выполняемых беспроводными сенсорными сетями.

Полученные от датчика электрические сигналы часто не готовы для обработки, поэтому они проходят в моте через стадию преобразования. Например, сигнал часто требует усиления для

увеличения амплитуды, возможно применение фильтров для устранения нежелательного шума в определенных диапазонах частот и т.п.

Преобразованный сигнал трансформируется при помощи аналого-цифрового преобразователя (АЦП) в цифровой сигнал. В итоге сигнал получается в цифровой форме и он готов к дальнейшей обработке в процессоре и хранению в памяти микроконтроллера. При наличии исполнительных механизмов возможна также передача управляющих воздействий от узлов сети к внешней среде через актуатор. Питание сенсорного узла осуществляется обычно от небольшой батареи.

Помимо размера, есть и другие жесткие ограничения для узлов БСС. Они должны:

- потреблять очень мало энергии;
- работать с большим количеством узлов на малых расстояниях;
- иметь низкую стоимость производства;
- быть автономными и работать без обслуживания;
- адаптироваться к окружающей среде.

Внешний вид сенсорных узлов приведен на рис. 11.4.

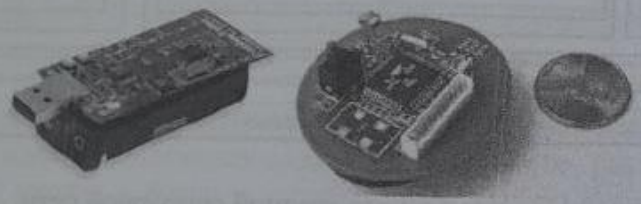


Рис. 11.4. Внешний вид сенсорных узлов

Для выполнения функций на каждый сенсорный узел устанавливается специализированная операционная система (ОС). Примером широко известной операционной системы для сенсорных узлов является разработанная система с открытым кодом TinyOS - это управляемая событиями операционная система реального времени, рассчитанная на работу в условиях ограниченных вычислительных ресурсов. Эта ОС позволяет

сенсорам автоматически устанавливать связи с соседями и формировать сенсорную сеть заданной топологии.

В качестве примера в таблице 11.1 приведены параметры сенсорных узлов ML-Node-Z (компании MeshLogic) и ZigBit (компании Atmel). Следует отметить, что интегрированных сенсорных датчиков на этих платах нет.

Таблица 11.1

Характеристики сенсорных узлов

Параметры	Тип сенсорного узла:	
	ML-Node-Z	ZigBit
Микроконтроллер		
Процессор	Texas Instruments MSP430	ATmega1281
Тактовая частота	От 32,768 кГц до 8 МГц	4 МГц
Оперативная память, Кбайт	10	8
Flash-память, Кбайт	48	128
Приемопередатчик		
Тип	IEEE 802.15.4	IEEE 802.15.4
Диапазон частот, МГц	2400 - 2483,5	2400 - 2483,5
Скорость передачи данных, Кбит/с	250	250
Выходная мощность, дБм	От -24 до 0	От -28 до 3
Чувствительность, дБм	-95	-101
Антенна	Чип	1 или 2 чипа
Внешние интерфейсы		
АЦП	12разрядный, 7 каналов	10-разрядный, 3 канала
Цифровые интерфейсы	I2C/SPI/UART/USB	I2C/SPI/UART/IRQ/JTAG
Другие параметры		
Напряжение питания, В	От 0,9 до 6,5	От 1,8 до 3,6
Размеры, мм	44x33x10	19x14x3
Температурный диапазон, °С	От -40 до 85	От 0 до 85

Поскольку одной из важнейших функций сенсоров является автоматический выбор схемы организации сети и маршрутов передачи данных, беспроводные сенсорные сети по существу являются самонастраиваемыми. Чаще всего сенсорный узел должен иметь возможность самостоятельно определить свое местоположение, по крайней мере, по отношению к тому другому сенсору, которому он будет передавать данные. То есть сначала происходит идентификация всех сенсоров, а затем уже формируется схема маршрутизации.

Сенсорные узлы могут закрепляться стационарно, а также иметь относительную мобильность, то есть произвольно перемещаться друг относительно друга в некотором пространстве, не нарушая при этом логической связанности сети. В последнем случае сенсорная сеть не имеет фиксированной постоянной топологии, и ее структура динамически меняется с течением времени.

В сенсорной сети узлы обычно общаются посредством беспроводной связи. Связь может осуществляться посредством радио, инфракрасного излучения (ИК-порта) или оптических сигналов. Одним из наиболее распространенных вариантов радиосвязи является использование полос частот для промышленных, научных и медицинских целей ISM (Industrial, Scientific and Medical), которые определены Сектором радиосвязи Международного союза электросвязи ITU-R и доступны без лицензий в большинстве стран.

Некоторые из этих частот уже используются в беспроводных локальных сетях (WLAN). Для сенсорных сетей малого размера и низкой стоимости усилитель сигнала не требуется. Аппаратные ограничения и нахождения компромисса между эффективностью антенны и потреблением энергии накладывают определенные ограничения на выбор частоты передачи в диапазоне сверхвысоких частот. Чаще всего используются следующие частоты ISM - 433 МГц (Европа) и 915 МГц (Северная Америка). Основными преимуществами использования радиочастот ISM является широкий спектр частот и доступность по всему миру. Они не привязаны к конкретному стандарту, тем самым дают большую свободу для реализации энергосберегающих стратегий в сенсорных сетях.

Имеются также узлы БСС, которые используют для передачи оптическую среду. Применяются две схемы передачи - пассивная с использованием светоотражателя CCR (Corner-Cube Retroreflector) и активная с использованием лазерного диода и управляемых зеркал. В первом случае не требуется интегрированный источник света, для передачи сигнала используется конфигурации из трех зеркал CCR. Активный метод использует лазерный диод и систему активной лазерной связи для отправки световых лучей приемнику.

Особые требования к применению сенсорных сетей делают выбор среды передачи сложной задачей. Например, морские приложения требуют использования водной среды передачи. Здесь нужно использовать длинноволновые излучения, которые могут проникать сквозь поверхность воды. В труднодоступной местности или на поле боя могут возникнуть ошибки и большие помехи. Кроме того может оказаться, что антенны узлов не обладают нужной высотой и мощностью излучения для связи с другими устройствами. Следовательно, выбор передающей среды должен сопровождаться надежными схемами модуляции и кодирования, что зависит от характеристик передающего канала.

Типовая архитектура БСС включает три типа узлов (рис. 11.5) [34-36]:

1. *Координатор* - осуществляет глобальную координацию, организацию и установку параметров сети, является наиболее сложным устройством БСС, требует наибольший объём памяти и наибольшую мощность источника питания. В одной сети должен присутствовать только один координатор. Из координатора осуществляется выход во внешнюю сеть (он реализует функцию шлюза - gateway). Часто координатор называют базовой станцией (БС).

Координатор выполняет следующие функции:

- определяет незадействованные каналы из перечня каналов, доступных для организации сети и определяемых разработчиком и организует сеть;
- передает сетевые сигнальные пакеты с информацией о существующей сети;
- управляет сетевыми подчиненными устройствами, устанавливает параметры сети - определяет максимальную

глубину вложенных подсетей, число сетевых маршрутизаторов и число подчиненных устройств;

- обеспечивает маршрутизацию информации между подчиненными устройствами;
- большую часть времени находится в режиме приема;
- обеспечивает организацию таблиц маршрутизации;

позволяет маршрутизаторам и конечным устройствам входить в сеть.

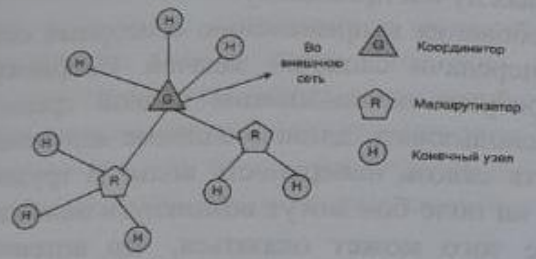


Рис. 11.5. Типы узлов БСС

2. *Маршрутизатор* - принимает, буферизирует и передает данные от других узлов БСС, а также определяет направление передачи.

Маршрутизатор выполняет следующие функции:

- определяет активные каналы, подключается к сети и позволяет оконечным устройствам входить в сеть - использует дополнительные, определенные приложением, списки активных каналов;
- ретранслирует сигнальные сетевые пакеты с параметрами сети от координатора;
- администрирует сетевые адреса подключенных к маршрутизатору подчиненных устройств;
- поддерживает следующие классы устройств маршрутизации: устройство с таблицей маршрутизации и с функцией древовидной маршрутизации, устройство только с функцией древовидной маршрутизации, поддержка функции аварийной древовидной маршрутизации;
- поддерживает два режима работы устройств: без перехода в «спящий режим» и с переходом в «спящий» режим в периоды,

определяемые координатором сети и параметрами сетевой синхронизации;

- поддерживает функции маршрутизации многоячейковых сетей: создает таблицы соседних сетевых узлов с параметром качества связи с каждым из них, создает таблицы сетевой маршрутизации, ретранслирует пакеты запроса и подтверждения определения маршрутов между устройствами;
- поддерживает функции маршрутизации по древовидному принципу - транслирует сообщения вверх и вниз по иерархической древовидной структуре ветви в зависимости от адреса получателя сообщения.

3. *Конечное (оконечное) устройство (сенсорный узел)* - выполняет только прикладные действия (сбор информации и управление удаленным объектом) и не осуществляет ретрансляцию данных.

Сенсорный узел имеет следующие особенности:

- всегда ищет и пытается войти в существующую сеть - использует дополнительные, определенные приложением, списки активных каналов и - сигнальные пакеты синхронизации существующей сети для определения параметров сети и маршрутизатора для входа в сеть;
- питается от автономного источника (батареи);
- из пакетов синхронизации определяет наличие данных от координатора;
- запрашивает данные от координатора;
- способен находиться длительное время в «спящем» режиме (до 99,99% от всего времени работы).

По выполняемым наборам функций все узлы БСС можно отнести к двум видам:

1. *Устройство с полным набором функций FFD (Fully Function Device) :*

- поддержка стандарта IEEE 802.15.4;
- дополнительная память и энергопотребление позволяют выполнять роль координатора сети;
- поддержка всех типов топологий («точка-точка», «звезда», «дерево», «ячеистая сеть»);
- способность выполнять роль координатора сети;
- способность обращаться к другим устройствам в сети.

2. *Устройство с ограниченным набором функций RFD (Reduced Function Device):*

- поддерживает ограниченный набор функций стандарта IEEE 802.15.4;
- поддержка топологий «точка-точка», «звезда»;
- не выполняет функции координатора;
- обращается к координатору сети и маршрутизатору.

Координаторы и маршрутизаторы всегда относятся к устройствами FFD, оконечные устройства могут быть FFD или RFD.

Выделяют два типа архитектуры беспроводных сенсорных сетей: однородные (одноранговые) и иерархические (кластерные). Однородность сети подразумевает, что все узлы выполняют одинаковые функции при сборе, обработке и передаче информации. Этот подход позволяет добиться оптимальной маршрутизации. Пересылка данных происходит по самым эффективным по некоторым критериям маршрутам, что позволяет добиться экономии таких важных ресурсов, как энергия (передача идёт по маршруту с самым высоким запасом энергии) и время (передача происходит по самому короткому маршруту). Для критически важных данных может быть организована передача по наиболее надёжному пути. Агрегирование данных, если необходимо, происходит по мере следования сообщений к координатору. Однако при такой организации сети формирование связей между узлами происходит спонтанно, что ведёт к столкновениям пакетов и возникновению задержек, связанным с выходом из спящего режима узлов, находящихся на выбранном пути передачи.

Альтернативным подходом является иерархическая (древовидная) маршрутизация. Она основана на делении сети на области, называемые кластерами. Кластер образуют маршрутизатор и конечные узлы, у которых он запрашивает сенсорные данные (рис. 11.6). Внутри каждого кластера маршрутизатор отвечает за сбор информации со всего кластера, её обработку и дальнейшую передачу. Остальные узлы кластера осуществляют только сбор данных и передачу их маршрутизатору. Таким образом, узлы в иерархической сети не равноправны. Во-первых, агрегирование данных происходит на маршрутизаторах,

и, во- вторых, пересылка агрегированных данных далее может производиться только маршрутизаторами. Таким образом, минимизируются задержки передачи, поскольку маршрутизаторы доступны всегда.

Столкновения пакетов исключены благодаря централизованному методу создания ссылок. Однако такая маршрутизация не предоставляет оптимальных путей передачи данных. К тому же сенсорный узел, выполняющий функции маршрутизатора, тратит значительно больше энергии, что приводит к быстрому истощению его батарей. Существуют архитектуры, предполагающие использование в качестве маршрутизаторов физически выделенных сенсоров, обладающих большими запасами энергии и вычислительными мощностями, однако этот подход применим только для узкого ряда приложений.

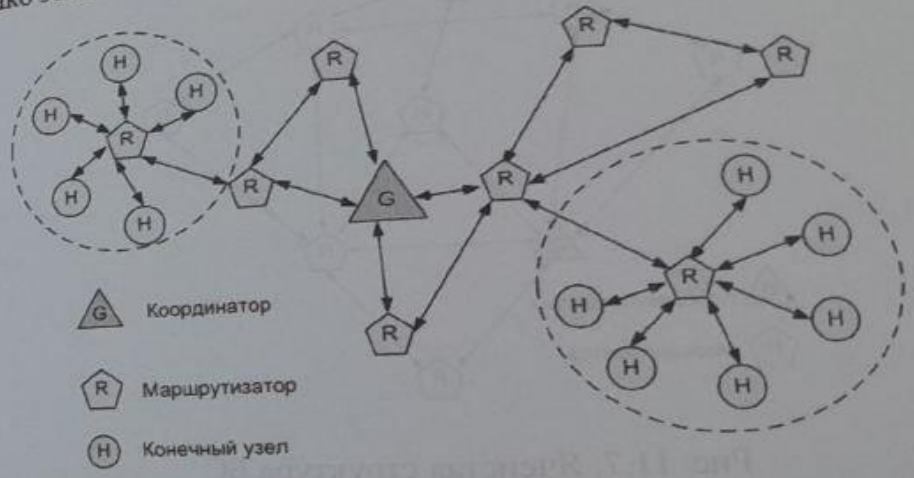


Рис. 11.6. Кластерная структура БСС

Маршрутизаторы кластеров ретранслируют данные друг другу и, в конечном счете, данные передаются координатору. Координатор обычно имеет связь с IP- сетью, куда и направляются данные для окончательной обработки. В каждой сети должно быть, по меньшей мере, одно полнофункциональное устройство FFD для работы в качестве координатора.

Возможно также построение одноранговых ячеистых сетей (рис. 11.7). В таких сетях функциональные возможности каждого

сенсорного узла одинаковы. Возможность самоорганизации и самовосстановления сетей ячеистой топологии позволяет в случае выхода части сенсоров из строя спонтанно формировать новую структуру сети. Правда, в любом случае необходим центральный функциональный узел-координатор, принимающий и обрабатывающий все данные, или шлюз для передачи данных на обработку внешнему узлу. Спонтанно создаваемые сети часто называют латинским термином Ad Hoc, что означает «для конкретного случая».

Возможные топологии сенсорной сети приведены на рис. 11.8. Одноранговые сети могут формировать произвольные топологические структуры (точка-точка, звезда), ограниченные только дистанцией между каждой парой узлов.

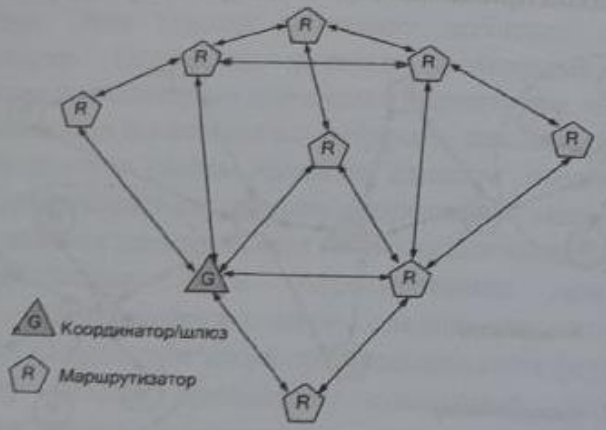


Рис. 11.7. Ячеистая структура БС

Ячеистая топология (Mesh Topology) - базовая полносвязная топология, в которой каждый маршрутизатор сети соединяется с несколькими другими маршрутизаторами этой же сети. Характеризуется высокой отказоустойчивостью, но и более сложной настройкой.

Примером одноранговой или пиринговой сети (от англ. peer-to-peer, P2P - равный к равному) является кластерное дерево. Сеть типа кластерное дерево является частным случаем сети P2P, в

которой большинство устройств являются FFD. Устройства RFD подключаются к кластеру в качестве конечных узлов.

Для присоединения к сети удалённых от координатора новых сетевых устройств могут использоваться уже присоединённые к сети FFD в режиме координатора. В этом режиме они, как и изначально координатор PAN, «зазывают» маяками в сеть новые сетевые устройства. В результате формируется кластер из сетевых устройств, которые «слышат» своего координатора. Тем не менее, вся информация о кластере доступна координатору PAN. Подобным образом могут формироваться мультикластеры из сетевых устройств.

Рис. 11.8. Возможные топологии сенсорной сети

11.2. Алгоритмы и свойства протоколов канального уровня

Беспроводные сенсорные сети, как правило, функционируют на базе протокола *IEEE 802.15.4* (*Gutierrezet al.2001*), который был разработан специально для коммуникаций на небольшом расстоянии с малой мощностью сенсорных сетей, и поддерживается большинством академических и коммерческих сенсорных узлов. Когда диапазон передачи данных всех сенсорных узлов достаточно большой, и сенсорные узлы могут передавать свои данные непосредственно к базовой станции, они

могут сформировать звездную топологию, как показано слева на рис. 11.9 [44].

В этой топологии каждый сенсорный узел непосредственно связывается с базовой станцией, используя единственный шаг. Поэтому, такое взаимодействие называется одношаговым. Тем не менее, сенсорные сети часто покрывают большие географические районы, и мощность радиопередачи должна быть сведена к минимуму в целях экономии энергии; следовательно, многошаговое взаимодействие является более общим случаем для сенсорных сетей (показано справа на рис. 11.9).

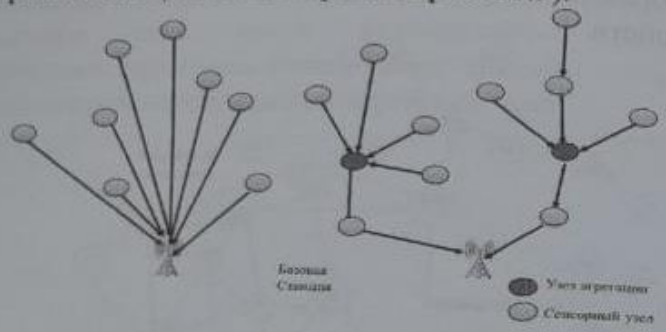


Рис. 11.9. Одношаговое и многошаговое взаимодействие в БСС

В этой топологии сети сенсорные узлы должны не только передать свои собственные данные, но также служат в качестве передатчиков для других сенсорных узлов, то есть, они должны обеспечить передачу данных и от других сенсорных узлов к базовой станции. Эта проблема маршрутизации, то есть, задача нахождения пути с несколькими шагами ретрансляции от сенсорного узла на базовую станцию, является одной из самых важных проблем и получила огромное внимание научного сообщества.

Маршрутизация в беспроводных сенсорных сетях является весьма сложной задачей из-за присущих БСС особенностей, которые отличают эти сети от других беспроводных сетей таких, как мобильные *Ad Hoc* сети или сотовые сети:

- традиционная адресация на основе *IP*-протоколов не может быть применена к БСС из-за относительно большого количества сенсорных узлов. В БСС иногда получить данные

важнее, чем знать идентификаторы узлов, с которых они отправлены.

- ресурсы сенсорных узлов в беспроводных сенсорных сетях ограничены с точки зрения возможностей обработки информации, пропускной способности, объема памяти, вычислительных возможностей, таким образом, требуется рациональное управление ресурсами.
- сенсорные узлы как очень простые элементы зачастую ненадежны.
- топология сенсорных сетей изменяется очень часто. В некоторых приложениях сенсорные узлы могут мобильными и изменять свое местоположение.
- некоторые узлы в сети осуществляют одни и те же цели, то есть трафик данных может быть сгенерирован так, что различные сенсорные узлы будут передавать одну и ту же информацию.

Одна из главных целей маршрутизации в БСС состоит в том, чтобы выполнить передачу данных, продлить при этом срок службы сети и предотвратить деградацию соединений. Создание протоколов маршрутизации в БСС зависит от многих ограничивающих факторов. Эти факторы должны быть учтены, прежде чем эффективная связь может быть установлена в БСС.

Одним из наиболее важных вопросов является адаптация к изменениям в связности, масштабируемости и отказоустойчивости.

Поэтому при разработке алгоритмов маршрутизации и планировании беспроводных сенсорных сетей должны учитываться следующие факторы:

- Потребление энергии (Энергетическая эффективность). Идеальный алгоритм должен обеспечить своевременную передачу информации с заданной точностью и с минимальными энергозатратами. В многошаговой БСС каждый узел играет двойную роль: сенсор и маршрутизатор данных. Сбой некоторых сенсорных узлов из-за перерыва в питании может вызвать значительные топологические изменения и может потребовать повторной маршрутизации пакетов и реорганизации сети. Энергетическая эффективность - одна из важнейших задач в создании беспроводных сенсорных сетей.

- **Модель передачи данных.** Сбор и передача данных в БСС зависят от приложения и актуальности представления данных (сообщений). Модели передачи данных могут быть классифицированы как непрерывная, управляемая событиями и гибридная. Непрерывная модель передачи данных подходит для приложений, которые требуют постоянного мониторинга. Таким образом, сенсоры и передатчики будут работать непрерывно. В событийно-управляемой и гибридной моделях сенсорные узлы реагируют на появление какого-либо события или запроса и генерируют сообщения на головной узел кластера или на БС. Алгоритм выбора головного узла и протокол маршрутизации во многом зависят от модели передачи данных, непосредственно связанной с потреблением энергии и стабильностью маршрута.

- **Гетерогенные узлы.** В зависимости от применения сенсорный узел может играть различную роль в сети или иметь различные параметры. Существование разнородных сенсоров поднимает много технических проблем, связанных с маршрутизацией данных.

- **Толерантность к отказам или надежность.** Некоторые сенсорные узлы могут выходить из строя или быть заблокированы вследствие недостаточного уровня электропитания, возникновения критических условий во внешней среде, физического повреждения или помех. Отказ отдельных сенсорных узлов не должен влиять на общее функционирование сенсорной сети. БСС должна поддерживать требуемый уровень качества обслуживания и обеспечивать необходимую надежность. Далее в диссертации будет предложен новый отказоустойчивый алгоритм кластеризации для беспроводных сенсорных сетей.

- **Масштабируемость.** В зависимости от решаемой задачи число сенсорных узлов в беспроводных сенсорных сетях, размещенных в сенсорном поле, может изменяться от нескольких сотен до тысяч или более.

- **Гибкость.** Алгоритмы в сенсорных сетях должны быть способны адаптироваться к различным приложениям БСС. Условия работы и возможности самого сенсорного узла могут сильно изменяться. Всё это должно быть учтено при разработке алгоритмов для беспроводных сенсорных сетей.

- **Средства передачи.** Характеристики окружающей среды также определяют метод радиосвязи для БСС. Например, для подводных беспроводных сенсорных сетей *UBCC* (*Underwater Wireless Sensor Networks*) средой передачи является вода. Традиционные проблемы, связанные с беспроводным каналом (например, замирание, высокий коэффициент ошибок и помехи), также могут влиять на работу сенсорной сети.

- **Связность.** Высокая плотность узлов в сенсорных сетях способствует поддержанию необходимого значения связности. Тем не менее, связность может уменьшаться вследствие вмешательства, помех, шумов или препятствий.

- **Покрытие.** В беспроводных сенсорных сетях каждый сенсорный узел покрывает ограниченную физическую область окружающей среды. Доля покрытия пространства также является важным параметром БСС, особенно для систем мониторинга.

- **Мобильность.** Большинство приложений предполагает, что сенсорные узлы стационарны. Тем не менее, мобильность сенсорных узлов может быть необходима в различных приложениях, например, летающих сенсорных сетях. Маршрутизация данных от или до движущихся узлов является более сложной, так как стабильность маршрута становится важной проблемой в дополнение к энергии, пропускной способности и т.д.

- **Двумерное и трехмерное пространство.** Сенсорные сети могут часто развертываться в трехмерном пространстве, например, в многоэтажных зданиях, при мониторинге лесов, подводном мониторинге, летающих сенсорных сетях и т.д. Переход от двумерного пространства к трехмерному порождает множество новых задач в связи с иной топологией сети.

- **Агрегация данных.** Сенсорные узлы могут генерировать значительные избыточные данные, включая аналогичные сообщения о событиях от нескольких узлов. Естественно, такие данные можно агрегировать для того, чтобы число сообщений уменьшилось. Объединение данных является типичной операцией во многих приложениях БСС, особенно, в иерархических протоколах маршрутизации для самоорганизующейся БСС. Такой метод широко используется для увеличения жизненного цикла сети.

- **Самоорганизация.** Сенсорные сети должны иметь возможность самоорганизации. Поэтому, вычислительные возможности, возможности обеспечения связи, возможности управления должны обеспечивать и возможность автономного существования БСС в течение какого-либо времени.

- **Точность и латентность.** Обеспечение точной информацией в реальном времени - одна из главных задач приложений БСС. Данные должны передаваться через беспроводную сенсорную сеть своевременно и точно. Идеальный алгоритм должен обеспечивать качественную передачу данных с минимальными энергозатратами.

Для определения маршрута передачи информации в БСС от конечного узла до узла–координатора, а также между оконечными узлами, используются специальные протоколы маршрутизации. Протоколы маршрутизации в БСС решают следующие задачи:

- самоорганизация узлов сети (самоконфигурирование, самовосстановление и самооптимизация);
- маршрутизация пакетов данных и адресация узлов;
- минимизация энергопотребления узлов сети и увеличение общего времени жизни всей сети;
- сбор и агрегация данных;
- регулирование скорости передачи и обработки данных в сети;
- максимизация зоны покрытия сети;
- обеспечение заданного качества обслуживания (QoS); защита от несанкционированного доступа.

При выборе пути передачи информации в сети в качестве метрик в них могут быть использованы следующие параметры:

а) длина пути (количество участков переприема информации);
б) надежность;
в) задержка;
г) пропускная способность;
д) загрузка;
е) стоимость передачи трафика и др.

Протоколы маршрутизации БСС отвечают за поддержку маршрутов в сети и должны гарантировать надежную связь даже в жестких неблагоприятных условиях. Многие протоколы маршрутизации, управления электропитанием, распространения

данных, были специально разработаны для БСС, где энергосбережение является существенной проблемой, на решение которой направлен протокол. Другие же были разработаны для общего применения в беспроводных сетях, но нашли свое применение и в БСС (рис. 11.10).

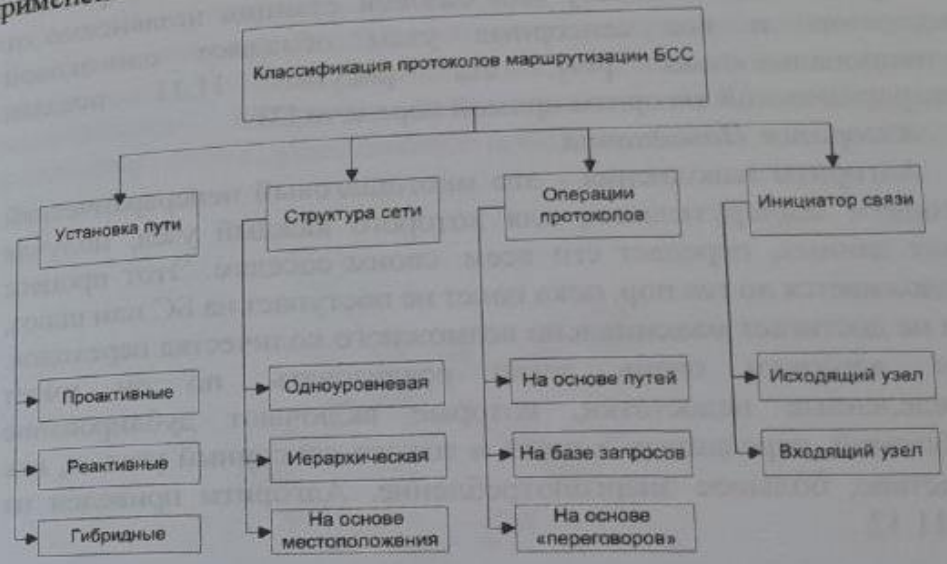


Рис. 11.10. Классификация протоколов маршрутизации БСС

Существует большое количество протоколов маршрутизации для БСС, классифицировать их можно по разным признакам (рис. 11.10). В зависимости от используемого режима работы сети, обуславливающего необходимость передачи информации от узлов, все протоколы маршрутизации можно разделить на проактивные (все пути определяются заранее, до того, как они будут нужны), реактивные (пути определяются по требованию) и гибридные (комбинация первых двух).

Протоколы, учитывающие структуры сети, делятся на:

а) протоколы одноуровневой (плоской) (flat-based) маршрутизации - все узлы БСС имеют одинаковую функциональность, примеры: SPIN (Sensor Protocols for Information via Negotiation), DT (Direct Transmission), Rumor Routing.

Алгоритм прямой передачи (DirectTransmission)

Алгоритм прямой передачи представляет собой неиерархический алгоритм маршрутизации для одношаговых сетей, где каждый сенсорный узел передает информацию непосредственно к шлюзу или базовой станции независимо от расстояния и все сенсорные узлы обладают одинаковой функциональностью [44]. На рисунке 11.11 показан неиерархический алгоритм прямой передачи DT.

Алгоритм Наводнения

Алгоритм наводнения - это многошаговый неиерархический алгоритм маршрутизации, для которого каждый узел, получая пакет данных, передает его всем своим соседям. Этот процесс продолжается до тех пор, пока пакет не поступает на БС или шлюз, или не достигает максимально возможного количества переходов. Этот алгоритм очень легко реализовать, но он имеет определенные недостатки, которые включают дублирование сообщений, переданных в один и тот же сенсорный узел, и, как следствие, большое энергопотребление. Алгоритм приведен на рис.11.12.

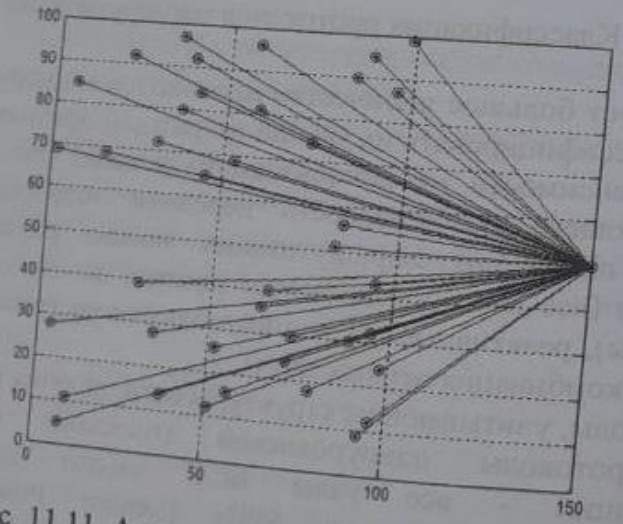


Рис. 11.11. Алгоритм прямой передачи в БСС

Алгоритм распространения слухов

Алгоритм распространения слухов представляет собой улучшенный вариант алгоритма наводнения. В этом алгоритме вместо того, чтобы передавать каждый пакет всем соседям, пакет направляют единственному соседу, выбранному случайным образом из таблицы соседей. Алгоритм распространения слухов преодолевает проблему дублирования сообщений, но при этом увеличивается задержка при передаче сообщений, что представляет собой существенную проблему для неиерархических алгоритмов.

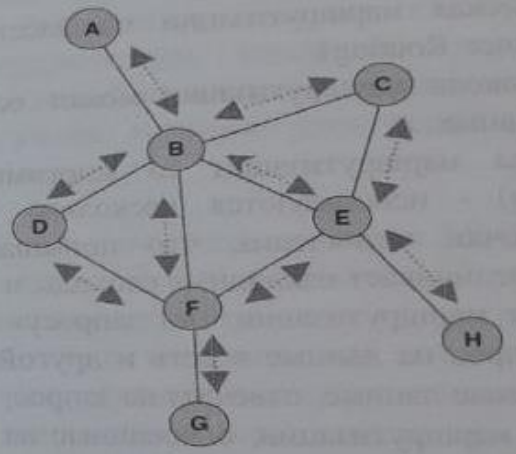


Рис. 11.12. Алгоритм наводнения в БСС

б) протоколы иерархической (hierarchical-based)

аршрутизации - узлы сети выполняют разные функции, они могут быть и физически разными, примеры: LEACH (Low Energy Adaptive Cluster Hierarchy), SEP (Stable Election Protocol), DEEC (Distributed Energy Efficient Clustering), TEEN (Threshold-sensitive Energy Efficient Protocol).

в) протоколы маршрутизации на основе информация о местонахождении узла (location-based). Информация о местонахождении узла может быть использована для маршрутизации. Сенсорные узлы, как правило, распределены

случайным образом на сенсорном поле, и местоположение этих сенсоров определяется при помощи системы глобального позиционирования (GPS, ГЛОНАСС) или использования других методов, например, систем локального позиционирования на базе WiFi. Заметим, что знание информации о географическом положении может представлять собой дополнительные расходы, особенно когда расположение узлов изменяется с течением времени, что характерно для мобильных сенсорных сетей. Наиболее известными алгоритмами, которые принадлежат к данной категории, являются:

- географическая и энергетическая маршрутизация GEAR (Geographic and Energy Aware Routing).
- географическая маршрутизации по расстоянию GEDIR (Geographic Distance Routing).

Работа протокола маршрутизации может основываться на различных принципах:

а) протоколы маршрутизации со многими маршрутами (multipath routing) - используются несколько маршрутов от источника до точки назначения, что повышает надежность соединения, но увеличивает накладные расходы и энергозатраты;

б) протоколы маршрутизации «по запросу» (query-based) - узел посылает запрос на данные в сеть и другой узел, который имеет запрашиваемые данные, отвечает на запрос;

в) протоколы маршрутизации, основанные на «переговорах» (negotiation routing) между узлами;

г) протоколы, учитывающие качество обслуживания (QoS – based), что позволяет обеспечить определенный уровень услуг в сети.

В протоколах, направленных на агрегацию данных, промежуточные узлы, располагающиеся между источниками информации и базовой станцией (БС), могут осуществлять агрегацию данных и посылать БС уже сведенные данные. Этот процесс позволяет сенсорным узлам экономить энергию.

Все протоколы маршрутизации также можно разделить на два вида - в одних инициатором соединения является источник информации, а в других - получатель.

Иерархические алгоритмы маршрутизации

В иерархических алгоритмах маршрутизации узлы

самоорганизуются в кластеры и головной узел выбирается для каждого кластера. Головные узлы осуществляют сбор данных с узлов - членов кластера, производят их обработку и передачу информации на шлюз или базовую станцию. Такое агрегирование данных в головных узлах значительно уменьшает энергопотребление в сети и увеличивает длительность жизненного цикла. Главным вопросом в разработке алгоритмов для иерархических беспроводных сенсорных сетей является выбор головного узла кластера. Существует два способа выбора головного узла кластера: выбор случайного головного узла или выбор предопределённого головного узла. Рассмотрим далее алгоритмы случайного выбора головного узла. Случайный выбор головных узлов приводит к созданию кластеров различных размеров. В иерархических алгоритмах маршрутизации и самоорганизации каждый из членов кластера имеет возможность стать головным узлом, головной узел задаёт расписание для членов кластера и т.д.

Алгоритм адаптивной кластеризации LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy). Протокол с контролем топологии и кластеризацией с низким потреблением. Подходит для сетей с иерархической структурой. Протокол является самоорганизующимся и адаптирующимся под различные состояния сети для распределения энергии по сети [44]. Узлы полагаются однородными и имеют ограниченный запас энергии. В сети имеется базовая станция, и все узлы знают о ее физическом местоположении. Узлы динамически объединяются в кластеры, внутри которых происходит выбор главного узла (clusterhead), для предотвращения чрезмерного потребления энергии. Протокол включает в себя агрегирование данных и сокращение рассеивания энергии в 8 раз [44].

Работа LEACH разделена на раунды. Каждый из таких раундов стоит из фазы настройки и стационарной фазы. В фазе настройки производится выбор главных узлов и объединение их с соседними устройствами. Решение о выборе принимается независимо всеми узлами в одно и то же время. Решение о выборе головного узла принимается на случайное основе с помощью следующего алгоритма.

Каждому из n узлов присваивается случайное значение r от 0 до 1. По представленной ниже формуле (3) рассчитывается значение порога $T(n)$:

$$T(n)=\frac{P}{1-P\cdot\left(r \bmod P^{-1}\right)},\ \forall n \in G \quad T(n)=0, \forall n \notin G, \qquad (11.1)$$

где r – номер текущего раунда;

P – вероятность выбора головным узлом;

n – указатель на текущий узел.

G – число узлов, которые не были главными узлами в последних $1/P$ раундах.

Если $N<T(n)$, то узел становится главным кластером. Такой алгоритм гарантирует, что каждый узел будет выбран главным узлом только один раз в течении $1/P$ раундов.

Узлы, которые были головными узлами в нулевом раунде, не могут быть ими снова в течении раундов $1/P$. После этого все узлы могут становиться головным узлом. В стационарной фазе данные передаются базовой станции. По сравнению с фазой настройки, стационарная фаза более продолжительна для того, чтобы минимизировать расход энергии.

В протоколе используется CSMA (Carrier Sense Multiple Access) – протокол MAC-уровня, в котором каждый узел проверяет отсутствие передачи другими узлами, до начала передачи на транспортном уровне.

Критическим параметром сети является процент узлов, которые являются головным узлом (в иностранной литературе употребляется термин cluster head [44]). В случае среднего и большого процента, и если расстояние до головного узла длиннее, чем между узлами и стоком, то тратится больше энергии. Оптимальным считается 5% головных узлов от количества всех узлов сети. В таком случае протокол помогает достигнуть уменьшение общей энергии сети в семь – восемь раз в случае однонаправленной передачей, в четыре – восемь раз, при передаче пакетов по нескольким узлам сразу.

Если требуется, то все узлы становятся

неработоспособными, в

последовательному разделению ролей головных у

Минимизируется общий расход энергии сети с помощь

разделения нагрузки между всеми узлами в разные моменты

времени. Превосходит статические кластеризующие алгоритмы.

Необходим выбор наиболее энергичного узла, так называемого

cluster-head. Узлы не обязаны знать о топологии всей глобальной

сети. Подходит для мало удаленных друг от друга узлов.

Топология протокола LEACH указана на рис. 11.13.

Кроме того, при выборе головного узла другие сенсорные узлы

определяют, к какому кластеру они хотят присоединиться на

основе мощности получаемого сигнала RSS (Received Signal

Strength) от головного узла.

Когда все узлы организовались в кластеры, головной узел

создает расписание передачи информации на основе метода

TDMA, что гарантирует отсутствие коллизий при передаче

сообщений.

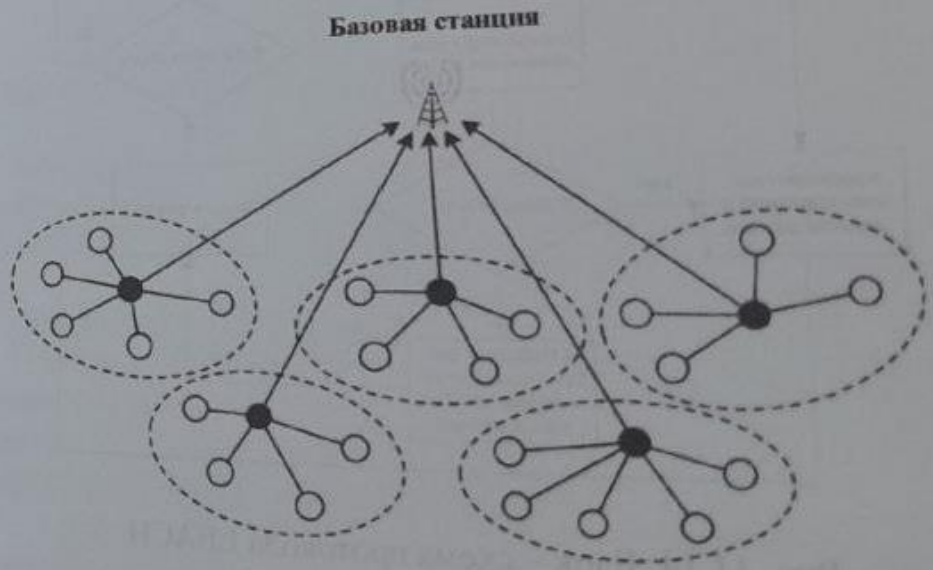


Рис. 11.13. Топология LEACH

Передача данных (Steady-state phase)

Головной узел широкополосным способом рассылает

расписание передачи и запрашивает своих членов кластера о передаче данных. Узлы передают данные в отведенные для этого интервалы TDMA. После получения сообщений от всех узлов головной узел формирует свои сообщения и передает эти сообщения на шлюз или базовую станцию. Блок схема протокола LEACH отображена на рис. 11.14.

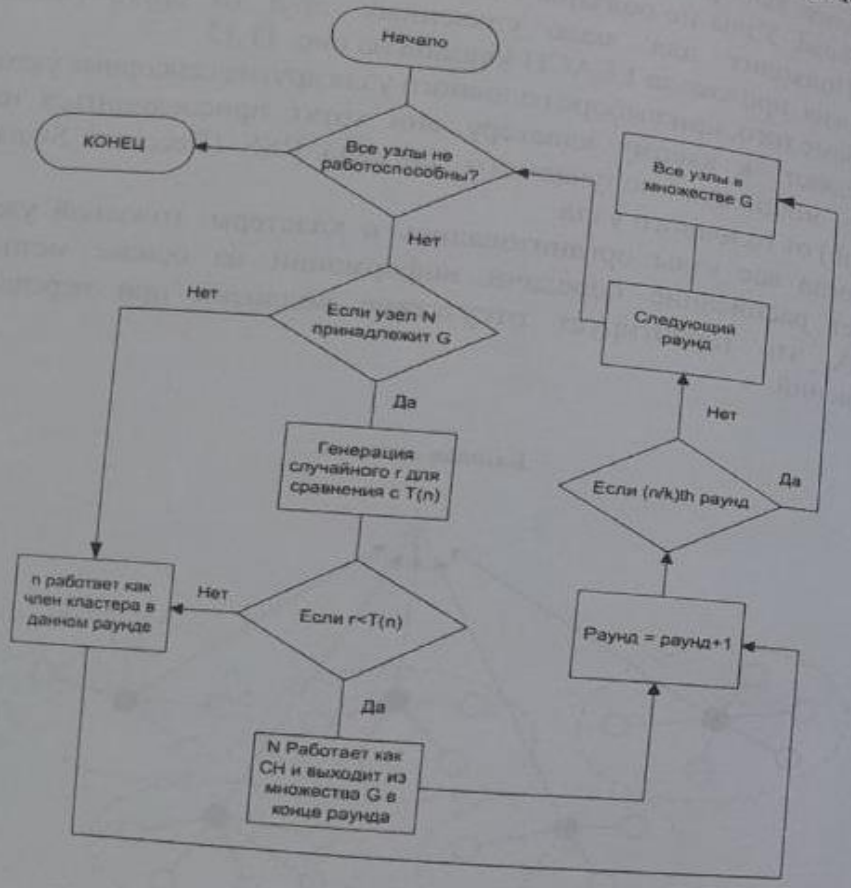


Рис. 11.14. Блок – схема протокола LEACH

В качестве радио-модели используем типовую модель для беспроводных сенсорных сетей [44] приведенную на рис. 11.15.

Рассматриваемая нами радио-модель описывается следующими уравнениями (11.2-11.3):

$$E_{TX}(k,d) = E_{TX-elec} \cdot k + E_{amp} \cdot k \cdot d^2, \quad (11.2)$$

$$E_{RX}(k) = E_{RX-elec} \cdot k + E_{RX}(k), \quad (11.3)$$

где E_{TX} – энергия, затрачиваемая на передачу;

E_{RX} – энергия, потребляемая при приеме;

$E_{TX-elec}$ и $E_{RX-elec}$ – энергии, необходимые для работы электронной схемы передатчика и приемника, соответственно;

E_{amp} - энергия, необходимая для схемы усилителя;

k – размер пакета;

d – расстояние между передатчиком и приемником.

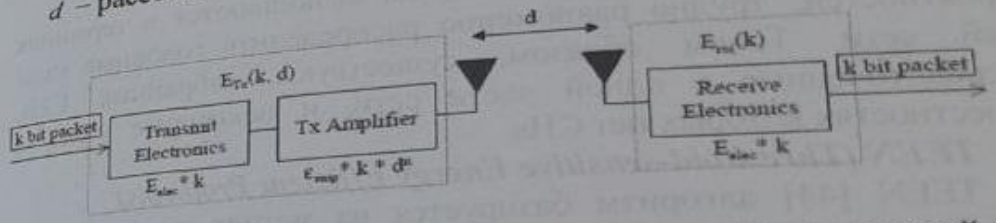


Рис. 11.15. Радио-модель для беспроводных сенсорных сетей

Впоследствии алгоритм LEACH был неоднократно модифицирован и появились такие алгоритмы, как E-LEACH, M-LEACH, LEACH-C, V- LEACH, W-LEACH, T-LEACH и т.д. [44].

Преимущества алгоритма LEACH состоят в следующем:

- любой сенсорный узел, который являлся головным узлом в текущем раунде, не может быть выбран в качестве головного узла снова, так что для каждого узла нагрузка в виде роли головного распределяется более или менее равномерно;
- используемый метод TDMA и расписание передачи позволяют избежать ненужных коллизий;
- члены кластера могут находиться в спящем режиме, чтобы избежать излишнего потребления энергии.
- первая выход из строя узла происходит в восемь раз позже, чем при использовании прямой передачи и статических кластерных протоколов.

Тем не менее, существуют и несколько недостатков в алгоритме LEACH:

- он выполняет только прямую передачу данных внутри кластера и непосредственно из головного узла в БС. Это не всегда возможно в связи с большим размером сети. Кроме того, при большом расстоянии между головными узлами и БС потребляется много энергии;

- несмотря на ротацию головных узлов CH в каждом раунде, чтобы добиться балансировки нагрузки, LEACH не может обеспечить реальную балансировку в случае сенсорных узлов с различным количеством начальной энергии, поскольку головные узлы избираются в терминах вероятностей без энергетических соображений;

- так как выборы головного узла выполняются в терминах вероятностей, трудно равномерно распределить головные узлы всей сети. Таким образом, существуют избранные CHs, сосредоточенные в одной части сети, и некоторые узлы, в окрестностях которых нет CHs.

TEEN (Threshold-sensitive Energy Efficient Protocols)

TEEN [44] алгоритм базируется на методе кластеризации LEACH. Каждый узел в кластере периодически становится головным узлом. Сеть с использованием алгоритма TEEN также имеет иерархическую структуру на основе кластерной организации (рис. 11.16). Головной узел может назначать своим узлам «жесткий» (hard) и «мягкий» (soft) пороги:

- жесткий порог (Hard Threshold): Узел посылает информацию головному узлу только, если количество накопленных данных находится в заданных пределах;

- мягкий порог (Soft Threshold): узел посылает информацию головному узлу только, когда количество накопленных данных изменилось как минимум на величину, равную или большую, чем мягкий порог.

Согласно сказанному выше, TEEN имеет следующие преимущества:

- жесткий порог (HT) сокращает количество сообщений, передавая информацию только тогда, когда собираемые данные находятся в диапазоне интереса. Кроме того, мягкий порог уменьшает количество сообщений исключением тех, у которых

есть минимальное изменение в собираемых данных. Таким образом, алгоритм TEEN уменьшает потребление энергии и улучшает эффективность и полезность БСС в целом;

- TEEN оперативно реагирует на большие изменения в собираемых данных, что подходит для реактивных сценариев и критически важных приложений.

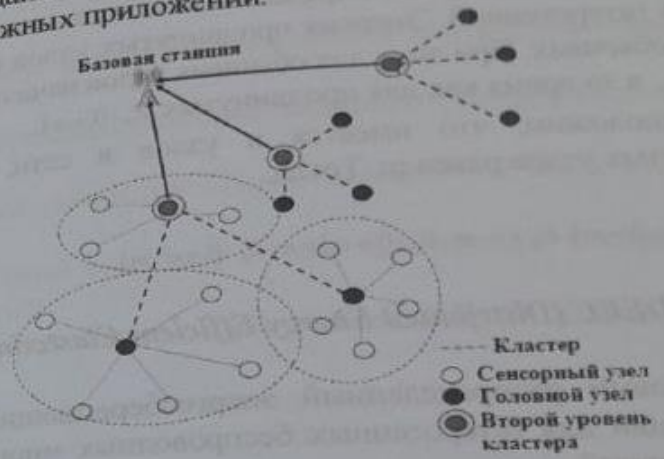


Рис. 11.16. Основная топология алгоритма TEEN

SEP (Stable Election Protocol)

Тем не менее, существуют несколько недостатков и в алгоритме TEEN:

- алгоритм TEEN не подходит для приложений БСС с периодическим сбором данных, так как пользователь не может получить никаких данных, если значения атрибутов не могут достичь порога;

- существуют потраченные впустую тайм-слоты и вероятность того, что БС может быть не в состоянии отличить неработоспособные узлы от работоспособных, потому что передача может осуществляться только тогда, когда данные превосходят жесткий порог или текущее значение для мягкого порога, отличается на величину, равную или большую, чем сам мягкий порог;

- если головные узлы CH находятся вне радиуса связи друг с другом, данные могут быть потеряны, потому что

распространение информации осуществляется только посредством головных узлов CH.

Алгоритм SEP [44] разработан для выбора головного узла в БСС исходя из предположения, что в сети возможно наличие двух типов узлов с точки зрения их энергии: обычные и продвинутые узлы. Последнее сразу же определяет, что в данном случае сеть является гетерогенной. Энергия продвинутых узлов больше, чем энергия обычных. При этом для обычных узлов начальная энергия равна E_0, в то время как для продвинутых $E_0 \cdot (1+\alpha)$.

Предположим, что имеется n узлов в сети, а процент продвинутых узлов равен m. Тогда:

$$n = (1-m)\cdot E_0 + n\cdot m\cdot E_0\cdot(1+\alpha) = n\cdot E_0\cdot(1+\alpha\cdot m) \qquad (11.4)$$

DEEC (Distributed Energy Efficient Clustering)

Это новый распределенный энергосберегающий алгоритм кластеризации для гетерогенных беспроводных многоуровневых сенсорных сетей.

DEEC оценивает вероятность выбора головного узла P_i в многоуровневых гетерогенных БСС в соответствии со следующей формулой:

$$P_i = P_{opt}\left[1-\frac{E(r)-E_i(r)}{E(r)}\right] = P_{opt}\frac{E_i(r)}{E(r)}, \qquad (11.5)$$

где $E_i(r)$ – энергия узла в раунде.

При этом в алгоритме DECC средняя энергия сети $E(r)$ для произвольного раунда r рассчитывается как:

$$E(r) = \frac{1}{N}E_{total}\left(1-\frac{r}{R}\right) \qquad (11.6)$$

R обозначает общее количество раундов жизни сети и оценивается следующим образом:

$$R = \frac{E_{total}}{E_{round}}, \qquad (11.7)$$

где E_{total} – является суммарной энергией в сети,

E_{round} - это расход энергии в течение раунда.

Контрольные вопросы

1. Объясните основные элементы и интерфейсы сенсорной сети.
2. Опишите модель сенсорного сетевого узла и его аппаратные компоненты.
3. Из каких подсистем состоит аппаратная часть сенсорной сети?
4. Какие типы включает в себя архитектура беспроводных сенсорных сети?
5. Что представляет собой координатор и какие функции выполняет?
6. Какие функции выполняет роутер?
7. Приведите и объясните структуру и топологию беспроводных сенсорных сетей.
8. Приведите и объясните кластерную структуру сети беспроводных датчиков.
9. Приведите и объясните сотовую структуру беспроводной сенсорной сети.
10. Приведите и поясните возможные топологии сенсорных сетей.

Глава 12. ПОЛОСЫ РАДИОЧАСТОТ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БСС

12.1. Режимы работы беспроводных сенсорных сетей

Самой энергозатратной операцией для сенсорных узлов является передача данных в беспроводное окружение. Потому энергосберегающие формы передачи являются ключевым фактором для продления срока службы сенсоров, так как он практически целиком зависит от срока службы батарей.

Сбор данных беспроводной сенсорной сетью может производиться различными способами в зависимости от целевого назначения конкретной сети. Принимая во внимание различные способы использования сетевых ресурсов, беспроводные сенсорные сети можно разделить на классы в зависимости от вида их функционирования и типа целевого приложения [34-36]:

1. *Проактивные сети.* Узлы такой сети периодически включают свои сенсоры и передатчики, снимают показания и передают их на базовую станцию. Таким образом, они делают "моментальную фотографию" своего окружения с некоторой периодичностью и используются обычно для приложений, требующих регулярного мониторинга некоторых значений.

2. *Реактивные сети.* Узлы реактивных сетей с некоторой периодичностью снимают показания, однако не передают их, если полученные данные попадают в определенную область нормальных показаний. В то же время сведения о неожиданных и резких изменениях в показаниях датчиков или их выходе за диапазон нормальных значений незамедлительно передаются на базовую станцию. Этот вид сети предназначен для работы с приложениями реального времени.

3. *Гибридные сети.* Это комбинация двух вышеперечисленных типов, где сенсорные узлы не только периодически отправляют снятые данные, но и реагируют на резкие изменения в значениях.

12.2. Выделенные для БСС полосы радиочастот и связанные с этим вопросом проблемы

В сенсорной сети узлы обычно общаются посредством беспроводной связи. Связь может осуществляться посредством радио, инфракрасного излучения (ИК-порта) или оптических сигналов. Одним из наиболее распространенных вариантов радиосвязи является использование полос частот для промышленных, научных и медицинских целей ISM (Industrial, Scientific and Medical), которые определены Сектором радиосвязи Международного союза электросвязи ITU-R и доступны без лицензий в большинстве стран (табл. 12.1).

Таблица 12.1

Полосы частот определенные ITU-R

Диапазон частот		Полоса	Центральная частота	Область применения
6,765 МГц	6,795 МГц	30 КГц	6,780 МГц	Локальное применение
13,553 МГц	13,567 МГц	14 КГц	13,560 МГц	
26,957 МГц	27,283 МГц	326 КГц	27,120 МГц	
40,660 МГц	40,700 МГц	40 КГц	40,680 МГц	
433,050 МГц	434,790 МГц	1,84 МГц	433,920 МГц	Европа, Африка, Ближний Восток, Россия
902 МГц	928 МГц	26 МГц	915 МГц	Северная и Южная
2,4 ГГц	2,5 ГГц	100 МГц	2,45 ГГц	
5,725 ГГц	5,875 ГГц	150 МГц	5,8 ГГц	
24 ГГц	24,25 ГГц	250 МГц	24,125 ГГц	
61 ГГц	61,5 ГГц	500 МГц	61,25 ГГц	Локальное применение
122 ГГц	123 ГГц	1 ГГц	122,5 ГГц	Локальное применение
244 ГГц	246 ГГц	2 ГГц	245 ГГц	Локальное применение

Некоторые из этих частот уже используются в беспроводных локальных сетях (WLAN). Для сенсорных сетей малого размера и низкой стоимости усилитель сигнала не требуется. Аппаратные ограничения и нахождения компромисса между эффективностью антенны и потреблением энергии накладывают определенные ограничения на выбор частоты передачи в диапазоне

сверхвысоких частот. Основными преимуществами использования радиочастот ISM является широкий спектр частот и доступность по всему миру. Они не привязаны к конкретному стандарту, тем самым дают большую свободу для реализации энергосберегающих стратегий в сенсорных сетях.

Радиооборудование в стандарте 803.15.4 работает на одном из нелицензируемых частотных диапазонах (рис.12.1):

- 868–868,6 МГц;
- 902–928 МГц;
- 2400–2483,5 МГц.

Рис. 12.1. Выбор радиоканалов в стандарте IEEE 803.15.4

В Республике Узбекистан на основании Решения Государственной комиссии по радиочастотам Республики Узбекистан (ГКРЧ РУз) № 256 от 11.07.2011 г., дополнения в соответствии с Решением ГКРЧ РУз, № 360 от 26.07.2013 г., дополнений в соответствии с Решениями Республиканского совета по радиочастотам (РСРЧ) № 75 от 26.12.2014 г., № 252 от 24.04.2017 г., № 327 от 09.04.2018 г., № 331 от 30.04.2018 г. № 367 от 28.09.2018 г. определён перечень радиоэлектронных устройств малого радиуса действия, ввоз, реализация и использование которых на территории республики осуществляется без оформления частных решений ГКРЧ и разрешительных документов радиочастотных органов (таблица 12.1) [45].

В соответствии с Решением Республиканского совета по радиочастотам №521 от 30.12.2021 полосы радиочастот 863 - 870 МГц и 922 - 928 МГц на вторичной основе выделены для применения юридическими и физическими лицами оборудования

узкополосных беспроводных сетей связи стандартов технологии LPWAN на территории Республики Узбекистан, ввоз, реализация и использование которых осуществляется без оформления отдельных решений РСРЧ для каждого конкретного типа радиоэлектронных средств (РЭС) [46].

Перечень радиоэлектронных устройств малого радиуса действия, ввоз, реализация и использование которых на территории республики осуществляется без оформления частных решений ГКРЧ и разрешительных документов радиочастотных органов

Таблица 12.1

№ п/п	Полосы и номиналы радиочастот	Наименование радиоэлектронных устройств
1.	4 - 18 кГц	Глубинные селективные радары, предназначенные для обнаружения пустот и металла с эффективной изотропной излучаемой мощностью до 10 мВт.
	20 - 2000 МГц	Радары подземного зондирования (GPR) с эффективной изотропной излучаемой мощностью до 10 мВт.
	125 кГц; 134,2 кГц	Индукционные устройства - системы связи, основанные на использовании свойств магнитного поля, предназначенные для работы с эффективной изотропной излучаемой мощностью до 10 мВт.
2.	433,075-434,79 МГц (433,92±0,2%) МГц	Радиоэлектронные средства для обработки штрихкодовых этикеток и передачи информации, полученной с этих этикеток, в полосе радиочастот с допустимой мощностью излучения передатчика до 10 мВт.
3.	33,2-57,5 МГц	Слуховые радиотренажеры для людей с дефектами слуха с допустимой мощностью излучения передатчика до 10 мВт.

4.		Оборудование радиоуправления и радиосигнализации:
4.1.	26,945 МГц 26,960 МГц 433,075-434,79 МГц (433,92±0,2%) МГц	Устройства охранной радиосигнализации: - для охраны автомашин с допустимой мощностью излучения передатчика до 2 Вт; - для охраны помещений с допустимой мощностью излучения передатчика до 2 Вт; - для охраны автомашин с допустимой мощностью излучения передатчика до 5 мВт.
4.2.	433,075-434,79 МГц (433,92±0,2%)	Устройства дистанционного управления, охранной сигнализации и оповещения
4.3.	433,075-434,79 МГц (433,92±0,2%) МГц 868-868,2 МГц 149,95-150,0625 МГц	- с допустимой мощностью излучения передатчика до 10 мВт; - с допустимой мощностью излучения передатчика до 10 мВт. Аппаратура охранной радиосигнализации удаленных объектов с допустимой мощностью излучения передатчика до 25 мВт.
5.	30-41 МГц 46-49 МГц 1880-1900 МГц	Абонентские бесшнуровые телефонные аппараты с допустимой мощностью излучения передатчика до 10 мВт (использующие не более 1 абонентского номера). Портативные абонентские радиоблоки и бесшнуровые телефонные аппараты технологии DECT в полосе радиочастот с допустимой средней мощностью излучения передатчика до 10 мВт (с пиковой мощностью 250 мВт).
6.	26957-27283 кГц 28,0-28,2 МГц 40,66-40,70 МГц	Детские радиопереговорные устройства и радиоуправляемые игрушки с допустимой мощностью излучения передатчика до 10 мВт. Аппаратура радиоуправления моделями самолетов, катеров и т.п. с допустимой мощностью излучения передатчика до 1 Вт.
7.		Радиомикрофоны и базовые станции к радиомикрофонам:
7.1.	165,70 МГц 166,10 МГц 166,50 МГц	- с допустимой мощностью излучения передатчика до 20 мВт;

7.2.	167,15 МГц 470-698 МГц 710-782 МГц 790-814 МГц 823-865 МГц 852-876 МГц 925,0-937,5 МГц	- с допустимой мощностью излучения передатчика до 10 мВт.
7.3.	66-74 МГц 87,5-92 МГц 100-108 МГц	- различных применений с допустимой мощностью излучения передатчика до 10 мВт.
8.		Радиомикрофоны и базовые станции к радиомикрофонам:
8.1.	433,050-434,790 МГц	- с допустимой мощностью излучения передатчика до 20 мВт;
8.2.	446.0-446.2 МГц	- класса PMR446 с выходной мощностью не более 0,5 Вт.
9.	315 МГц 902 МГц	Устройства дистанционного управления, применяемые в качестве электронных ключей, обеспечения безопасности и прочие, с эффективной изотропной излучаемой мощностью до 10 мВт
10.	24,05-24,25 ГГц	Автомобильные радары транспортных средств малой мощности для целей радиоопределения, включающего определение положения, скорости, дистанции или других характеристик объекта:
10.1.	24,7 ГГц	- с выходной мощностью не более 0,05 мВт;
10.2.	76-77 ГГц	- с эффективной изотропной излучаемой мощностью до 10 мВт;
10.3.		- с эффективной изотропной излучаемой мощностью до 1 Вт.
11.	2,400-2,4835 ГГц	Беспроводные видеокамеры
12.	125 кГц 1 32 кГц 13,56 МГц 433 МГц 865-868 МГц 869,4-869,65 МГц 902-915 МГц 2450 МГц 2,400-2,4835 ГГц	Системы радиочастотной идентификации RFID, считыватели и антенны
13.		Мобильные репитеры (усилители) с допустимой мощностью излучения до 500 мВт.

13.1	450 МГц	- в стандартах CDMA и EVDO;
13.2	700 МГц	- в стандарте LTE;
13.3	800 МГц	- в стандартах CDMA 2000-1x и LTE;
13.4	900 МГц	- в стандарте GSM;
13.5	1800 МГц	- в стандартах GSM и LTE;
13.6	2100 МГц	- в стандартах UMTS и WCDMA;
13.7	2500 МГц	- в стандарте LTE.

Применение оборудования узкополосных беспроводных сетей связи стандартов технологии LPWAN в выделенных полосах радиочастот осуществляется при выполнении следующих требований:

– максимальная мощность оконечных устройств и базовых станций сетей технологии LPWAN не должна превышать 25 мВт с применением для оконечных устройств методов снижения помех, как ограничение рабочего цикла, режима прослушивания перед излучением;

– использование радиооборудования в пределах аэропортов (аэродромов) определяется условиями электромагнитной обстановки;

– применяемое радиооборудование не должно создавать вредных радиопомех другим радиоэлектронным средствам (РЭС) и не может требовать защиты от помех со стороны РЭС других радиослужб;

– оформление разрешительных документов на использование базовых станций, а также разрешительных документов на ввоз на территорию Республики Узбекистан оконечных устройств узкополосных беспроводных сетей связи стандартов технологии LP WAN осуществляется ГУП Центр электромагнитной совместимости (ЦЭМС) в установленном порядке;

– радиооборудование подлежит сертификации в порядке, установленном в республике;

– технические характеристики используемого радиооборудования должны соответствовать стандартам и нормам на параметры радиоизлучений, установленным в республике.

При этом РЭС узкополосных беспроводных сетей связи стандартов технологии LPWAN, использующие радиочастоты в

диапазоне 800 МГц, не должны причинять вредных помех РЭС, которым радиочастоты распределены на первичной основе, и не могут требовать защиты от вредных помех со стороны РЭС, которым радиочастоты распределены на первичной основе.

12.3. Представление вопроса обеспечения информационной безопасности в беспроводных сенсорных сетях

Безопасность БСС в качестве характеристики среды узлов и среды приложений требует не только традиционной защиты безопасности, но также и наличие особых требований в отношении защиты, безопасности и конфиденциальности (TSP) БСС-сетей [3, 47].

Защита, безопасность и конфиденциальность

В зависимости от сценария приложения TSP БСС могут требовать защиты целостности, доступности, конфиденциальности, невозможности аннулирования и конфиденциальности пользователей. Она поддерживает целостность и надежность системы, защищая ее от вредоносных атак. TSP БСС может потребоваться осуществлять защиту узлов от несанкционированного доступа, защиту каналов связи и маршрутизации на сетевом уровне [48]. Для обнаружения атак TSP могут потребоваться функции регистрации/проверки. Технология TSP БСС состоит из аутентификации сообщений, шифрования, контроля доступа, идентификации подлинности и т.д. Потребности БСС в системе TSP должны быть классифицированы следующим образом: безопасность узлов, криптоалгоритмы, управление ключами, безопасная маршрутизация, группирование данных [49, 50].

Принимая во внимание вычислительную способность, потребление энергии и пропускную способность канала связи с узлами датчиков, защиту конфиденциальности и управление идентификацией, необходимо провести исследования в области структуры безопасности протокола, которая будет подходящей и общей моделью для каждого уровня БСС. Поскольку единое решение в области безопасности одного уровня не может быть наиболее эффективным решением, целостный подход к обеспечению безопасности будет включать все уровни общей

безопасности в сети [51]. Его цели направлены на повышение эффективности БСС в контексте безопасности, долговечности и возможностей подключения.

Основной принцип заключается в том, что затраты на обеспечение безопасности не должны превышать определенный уровень риска для безопасности в определенное время.

В настоящее время имеется множество методов обеспечения специальной безопасности уровней в БСС, таких как безопасное пробуждение узлов, защита от постороннего воздействия, аутентификация и шифрование для сетевых уровней, регистрация для уровней приложений. Тем не менее, порядок структурирования протокола других уровней и создания общей инфраструктуры протокола безопасности является серьезной проблемой для исследований в будущем.

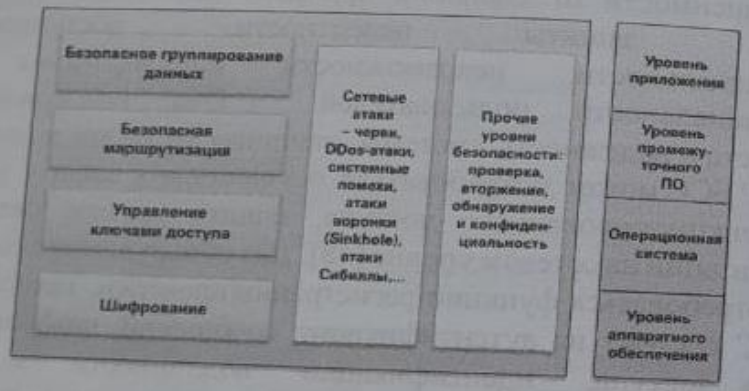


Рис. 12.2. TSP-архитектура беспроводных сенсорных сетей

В будущем будет создана общая модель, которая может объединить все механизмы уровни безопасности вместе. Другие механизмы позволят защитить БСС от атак, даже если на одном каком-то уровне защита будет преодолена. Тем не менее, экономическая эффективность и энерго эффективность могут по-прежнему являться большими проблемами для решения в рамках исследований в ближайшие годы.

Обеспечение конфиденциальности, прав человека на неприкосновенность частной жизни, безопасность данных и целостность обходится весьма дорого. Вопрос заключается в

следующем: каков коэффициент затрат и выгод при рассмотрении преимуществ, предоставляемых решением? Хочет ли человек утратить свои права для получения выгоды?

Компании Google и Apple смогли получить больше свободы при работе с личными данными в обмен на выгоды, которые перевешивают риски - по крайней мере, для многих потребителей. Инфраструктура персональных ключей и полномочия сертифицирующей компании в рамках неограниченного количества источников данных будут облагать налогом систему, и многие игроки будут стремиться свести к минимуму активные меры безопасности и противодействовать исключительно фактически имеющим место кибератакам - таким образом, подвергая риску всю систему. Сети IoT, отправляющие вредоносные пакеты данных всем подключенным системам, являются худшим кошмаром любого голливудского фильма жанра научной фантастики. Следовательно, важно, чтобы максимальное количество систем функционировали независимо друг от друга во избежание поражения всех остальных вследствие уязвимости одной системы. Такой потенциальный эффект домино является наихудшим сценарием, поскольку плохая целостность данных может привести к ошибкам, величина которых не была предусмотрена какой-либо одной системой. Эффективность активных систем безопасности будет зависеть от понимания того, что такое «нормальный» кибер физический поток данных, однако, это может быть чрезмерно дорогостоящим мероприятием, снизив выгоды или увеличив затраты на обязательные решения IoT.

Безопасность узла и «лишение сна»

Узел БСС может быть взломан через его логические интерфейсы или путем прямых физических атак; он может быть перемещен без разрешения или украден. Безопасность узла может включать функции безопасного пробуждения и безопасной загрузки. Легкий рабочий цикл имеет решающее значение для обеспечения длительного срока службы узлов датчиков с питанием от аккумуляторов. Существуют особые сервисные атаки, так называемые «атаки лишения сна» [52], которые препятствуют переходу узла датчика в

энергосберегающий спящий режим, что, в свою очередь, значительно сокращает срок службы атакуемого узла датчика.

Стандартные механизмы безопасности, такие как коды аутентификации сообщений или шифрование групп данных, не могут предотвратить «атаки лишения сна»: узел активируется, и энергия тратится на обработку полученного сообщения. Атака может быть замечена только тогда, когда заряд аккумулятора уже был израсходован. На рисунке 12.3 показан узел датчика с радиоприемником пробуждения с низким энергопотреблением. Радиоприемник пробуждения прослушивает канал, когда узел датчика находится в спящем режиме. Он вызывает срабатывание датчика при получении сигнала пробуждения.

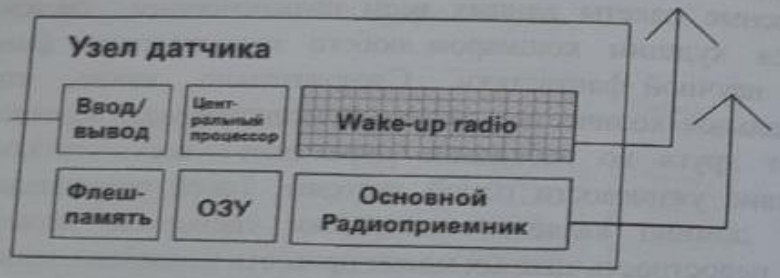


Рис. 12.3. Радиоприемник безопасного пробуждения

Для повышения уровня безопасности системы радио пробуждения, сигнал пробуждения является закодированным. Поскольку код пробуждения используется только один раз и, является индивидуальным для каждого узла, его можно отправлять в незашифрованном виде при пробуждении узла.

Криптографические алгоритмы

Шифрование - это специальный алгоритм для изменения исходной информации узла датчика данных, который не позволяет неавторизованному пользователю распознать исходную информацию при получении доступа к зашифрованной информации. Сети БСС государственной инфраструктуры неизбежно подвергаются множеству операций.

Традиционные коды проверки подлинности сообщений, симметричное шифрование и шифрование с открытым ключом показали множество недостатков. Поэтому возникла необходимость в новой системе шифрования для БСС. Испанская компания Libelium разработала библиотеки шифрования waspmote для обеспечения безопасности данных БСС умного города в 2010 году.

В основном их беспроводные сенсорные устройства поддерживали эти библиотеки. Библиотеки предназначены для разных механизмов шифрования и механизмов консультаций на уровне канала передачи данных, уровне сети и уровне приложения. При этом, они расширяют протокол Zigbee®, обеспечивая его большую безопасность (рис. 12.4).

Управление ключами БСС

В целом, система управления ключами призвана обеспечить безопасность БСС. Управление ключами включает в себя генерацию, распределение, верификацию, обновление, хранение, резервное копирование, обеспечение действительности и уничтожение ключей. Эффективная система управления ключами также является основой других механизмов безопасности, таких как безопасная маршрутизация, безопасное позиционирование, группирование данных. Типичные схемы управления ключами в БСС охватывают управление ключами общего применения, управление случайными ключами, управление ключами местоположений, управление ключами кластеризации и управление ключами общего пользования [53].

В ходе процедуры безопасной начальной загрузки создается безопасная конфигурация узла датчика, например, устанавливается ключ соединения. Поскольку существует множество процедур изначальной загрузки, и выбор соответствующей процедуры в значительной степени обусловлен конкретной средой, нормальное функционирование сети датчиков в некой степени отделено от начальной загрузки, следовательно, имеется возможность изменить процедуру начальной загрузки без каких-либо изменений в архитектуре безопасности для нормальной эксплуатации.

Соответствующая процедура начальной загрузки в значительной степени зависит от приложения и его среды.

Таким образом, было предложено несколько различных процедур начальной загрузки:

- аппаратный ключ (токен);
- предварительная конфигурация ключей при изготовлении узлов;
- физическая защита сообщений;
- внутриполосная связь в течение фазы настройки с низким уровнем безопасности;
- внеполосная коммуникация.

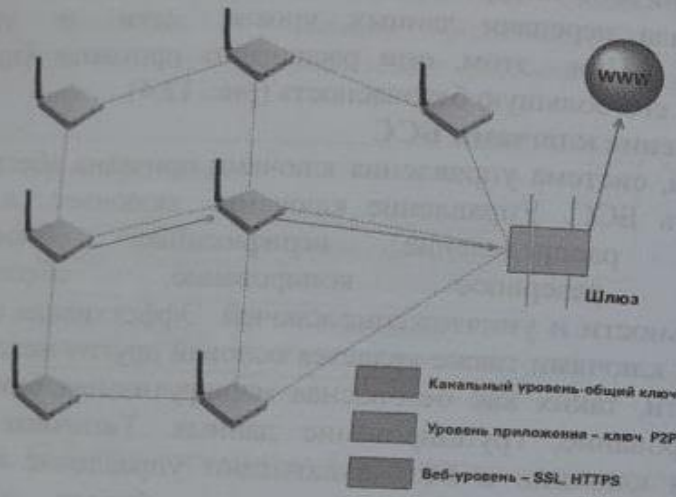


Рис. 12.4. Примеры типичного использования библиотек шифрования waspmote

Безопасная маршрутизация БСС

Поскольку БСС используют при передаче данных несколько транзитных шлюзов и самоорганизацию в сети, каждому узлу также требуется обнаружение маршрутизации, установление маршрутизации, обслуживание маршрутизации. Безопасный протокол маршрутизации представляет собой полное эффективное решение маршрутизации и может быть необходимым условием для группирования данных и безопасного удаления избыточности от исходного узла до принимающего узла. Мно Технология БСС защищенные

маршрутизированные сети были специально разработаны для БСС, их можно разделить на три группы в зависимости от структуры сети: линейная маршрутизация, иерархическая маршрутизация и географическая маршрутизация.

Типичные методы протоколов безопасной маршрутизации включают в себя методы на основе информации обратной связи, информации о местоположении, алгоритма шифрования, метода многоканального выбора и иерархических структур. Различные протоколы безопасной маршрутизации могут решать проблемы различных видов атак, например, протокол безопасной маршрутизации на основании информации обратной связи, которая включает в себя информацию о задержке, защите, местоположении, избыточной мощности в кадре подтверждения управления уровнем доступа к среде (MAC).

Хотя в рамках этого метода не используется шифрование, он может обеспечить защиту от типичных атак, например, ложной информации о маршрутизации, атаки cesspool и червей. Большинство современных протоколов безопасной маршрутизации предполагают, что сеть датчиков является стационарной, поэтому имеется необходимость разработать новые протоколы безопасной маршрутизации для обеспечения мобильности узлов датчиков.

Безопасное группирование данных БСС

Безопасное группирование данных призвано обеспечить безопасность каждого узла. Таким образом, общий алгоритм безопасного группирования данных состоит в следующем: первые узлы предоставляют надежные и достоверные данные и передают их на большие агрегирующие узлы. Большие агрегирующие узлы оценивают достоверность данных и проводят расчеты по группированию на основе избыточности. Каждый агрегирующий узел выбирает следующий безопасный и надежный транзитный шлюз и передает данные на центральный узел.

Центральные узлы оценивают достоверность данных и осуществляют окончательный расчет по группированию. Изначально группирование данных использовалось для экономии энергии, а при его осуществлении почти не учитывались вопросы безопасности. В настоящее время безопасное группирование данных в основном осуществляется посредством

аутентификации и шифрования на основе теории кластера, кольца и иерархии. Университет Мюнхена разработал прототип группирования данных, который основан на протоколе DTLS с целью практического осуществления защищенных схем передачи. Красный круг на рис.12.5 представляет собой их безопасный прототип группирования данных.

БСС повышенной безопасности

В настоящее время БСС тесно связывают инфраструктуру организаций и предприятий с информационной сетью. Ущерб, наносимый инфраструктуре (такой как система энергоснабжения, транспортная система, химическое предприятие и национальная безопасность) вирусными угрозами может привести к невообразимым последствиям. Сети БСС, как правило, являются более подверженными различным угрозам безопасности, поскольку неуправляемая среда передачи более подвержена атакам на систему безопасности, чем сети управляемой среды передачи. С самого начала необходимо учитывать проблемы TSP (защиты, безопасности и конфиденциальности). Угрозы, которым подвергается БСС, могут быть частично нивелированы при помощи технологий сетевой безопасности. Уровень защиты от сложных атак, таких как Sybil, Dos и аномальные узлы, является неудовлетворительным.

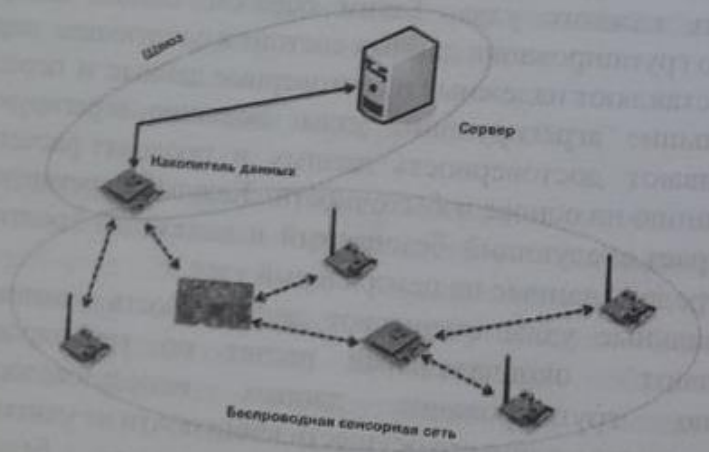


Рис. 12.5. Продукты безопасного группирования данных

Задачей TSP в отношении БСС-сетей является защита информации и ресурсов от атак и неправомерных действий. Следовательно, критерии для реализации этой цели весьма обширны и охватывают следующие области: доступность, авторизация, аутентификация, анонимность, конфиденциальность, актуальность, целостность, защита узлов, отказоустойчивость, конфиденциальность и т.д. В будущем масштаб БСС может стать более значительным, а взаимопроникновение БСС с интернетом станет более тесным. Несмотря на значительные исследовательские усилия в сфере безопасности узлов, шифрования, управления ключами, безопасной маршрутизации, безопасного группирования данных, необходимо предпринимать более серьезные меры для обеспечения безопасности БСС в будущем.

Структура протокола безопасности

Принимая во внимание вычислительную способность, потребление энергии и пропускную способность канала связи с узлами датчиков, защиту конфиденциальности и управление идентификацией, необходимо провести исследования в области структуры безопасности протокола, которая будет подходящей и общей моделью для каждого уровня БСС. Поскольку единое решение в области безопасности одного уровня не может быть наиболее эффективным решением, целостный подход к обеспечению безопасности будет включать все уровни общей безопасности в сети. Его цели направлены на повышение эффективности БСС в контексте безопасности, долговечности и возможностей подключения. Основной принцип заключается в том, что затраты на обеспечение безопасности не должны превышать определенный уровень риска для безопасности в определенное время.

В настоящее время имеется множество методов обеспечения специальной безопасности уровней в БСС, таких как безопасное пробуждение узлов, защита от постороннего воздействия, аутентификация и шифрование для сетевых уровней, регистрация для уровней приложений. Тем не менее, порядок структурирования протокола других уровней и создания общей инфраструктуры протокола безопасности является серьезной

проблемой для исследований в будущем. В будущем будет создана общая модель, которая может объединить все механизмы уровни безопасности вместе (рис. 12.6). Другие механизмы позволят защитить БСС от атак, даже если на одном каком-то уровне защита будет преодолена. Тем не менее, экономическая эффективность и энерго эффективность могут по-прежнему являться большими проблемами для решения в рамках исследований в ближайшие годы.

В целях безопасности структуры БСС имеют четыре качества. Во-первых, безопасность БСС уязвима для сетевых атак из-за широковещательной природы среды передачи данных и ограниченности вычислительных ресурсов узлов датчиков, таких как маленькая мощность и маленькая пропускная способность (рис. 12.7).

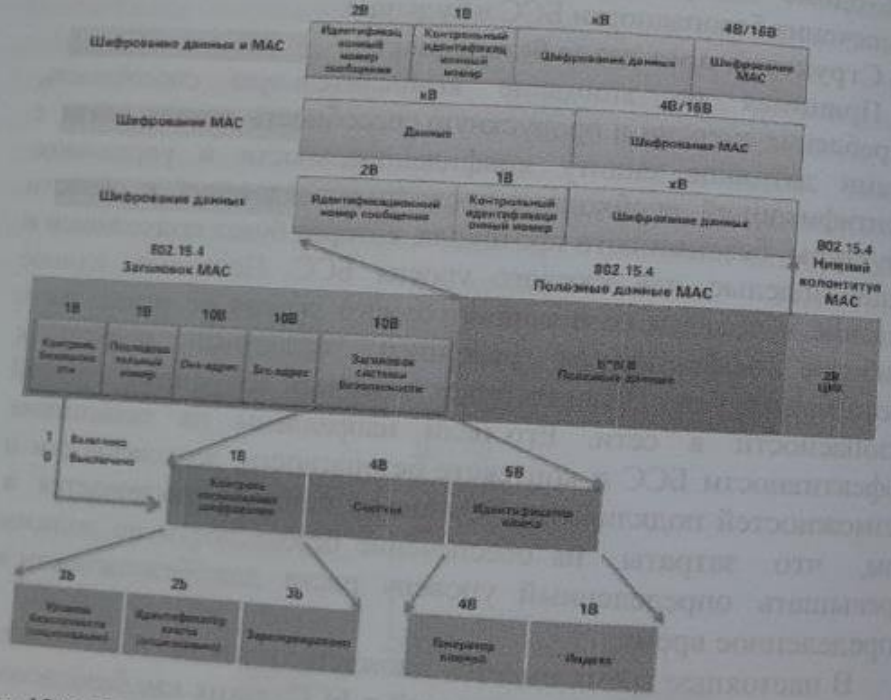


Рис. 12.6. Канальный уровень структуры протокола безопасности

Во-вторых, управление идентификацией и защитой является более сложным и комплексным по своей сути по причине глубокой интеграции информационного пространства с

физическим миром и повсеместного доступа к информационным технологиям. Таким образом, управление идентификацией и системы защиты сталкиваются с большими проблемами.

В-третьих, характеристики модели восприятия и вычисления БСС также являются серьезными проблемами для эффективной защиты целостности системы, целостности данных, конфиденциальности данных, конфиденциальности пользователей, таких как идентификация, поведение и окружающая среда. Наконец, поскольку БСС имеет большое количество терминалов, различные типы терминалов и динамические адаптивные сетевые структуры, размер и сложность данных среды являются серьезными проблемами для существующей системы контроля безопасности.

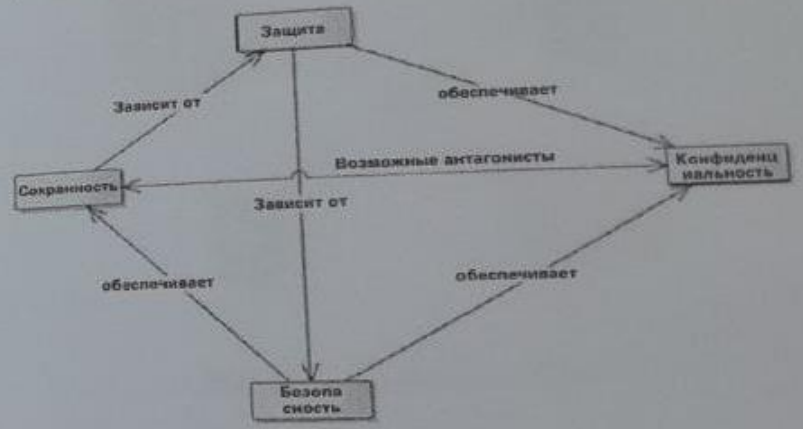


Рис. 12.7. Защита безопасности и конфиденциальности

Контрольные вопросы

1. Какие режимы работы доступны для беспроводных сенсорных сетей?
2. Для каких приложений предназначены реактивные сети?
3. Что представляет собой связь между узлами в беспроводных сенсорных сетях?
4. Какой диапазон частот выделен для беспроводных сенсорных сетей?

5. В каких диапазонах частот работают радиоустройства IEEE 803.15.4?

6. Как обеспечивается защита информации в беспроводных сенсорных сетях?

7. Приведите и объясните TSP-архитектуру беспроводных сенсорных сетей.

8. Приведите и объясните принципиальную схему защищенного соединения радиоприемника.

9. Приведите примеры использования библиотеки шифрования wasp mote.

10. Приведите и объясните структуру протокола безопасности.

Глава 13. СИСТЕМЫ M2M

13.1. Архитектура сетей M2M

M2M (Machine-to-Machine) означает «взаимодействие между машинами». Это означает как минимум два устройства, которые обмениваются данными друг с другом. Способ передачи данных не важен, важна передача данных между «машинами» (рис. 13.1) [55].

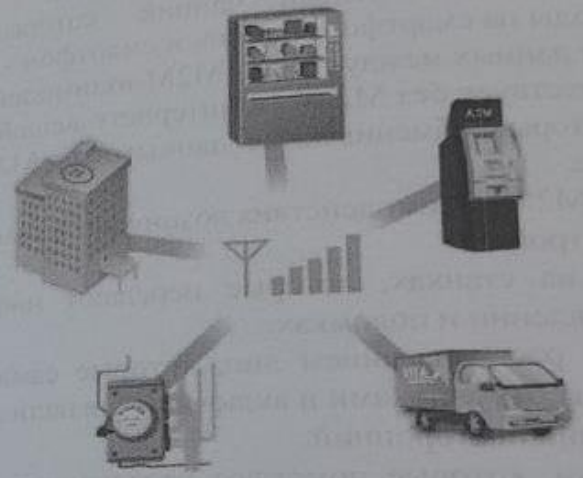


Рис.13.1. Принцип M2M

Технология M2M не включает взаимодействие человека и машины. Например, вы можете ввести числа в калькулятор и посмотреть результат, где нет второй машины, значит, нет технологии M2M. Но если калькулятор передает эти числа в какую-то базу данных, между калькулятором и базой данных происходит M2M-взаимодействие.

Интернет не требуется для взаимодействия M2M. Телевизор получает сигналы от телестанции - это взаимодействие M2M, ТВ и телевышки. При подключении смартфона к вышке БС или точке доступа Wi-Fi между ними происходит M2M-взаимодействие.

То есть M2M - это взаимодействие двух устройств посредством проводного или беспроводного соединения. В

прошлом веке все, от телефонных звонков через АТС до взаимодействия между умными колонками и системами освещения, заканчивалось передачей данных.

Разница между M2M и IoT

IoT - это интернет вещей, то есть сеть, которая включает в себя устройства, каналы связи, варианты взаимодействий и способы передачи данных. M2M - не такое глобальное понятие, оно описывает только само взаимодействие между устройствами. IoT всегда включает отдельные M2M-взаимодействия.

Например, имеется умный чайник, который передает температуру воды на смартфон. Чайник и смартфон - умные узлы IoT, а передача данных между ними - M2M-взаимодействие.

IoT не существует без M2M - в интернете вещей всегда есть устройства, которые обмениваются данными, и M2M - это их взаимодействие.

Например, M2M-взаимодействия возникают в коммуникациях таких умных устройств:

1. Датчики на станках, которые передают информацию о температуре, давлении и поломках.
2. Камеры с распознаванием лиц, которые сами открывают турникеты перед сотрудниками и включают сигнализацию, если в помещение проник посторонний.
3. GPS-маячки, которые помогают отслеживать транспорт и выстроить оптимальный маршрут для водителя.
4. Торговые автоматы, которые оповещают, если в них закончился товар или бумага для печати чеков.
5. Дроны, которые сами расставляют товар по полкам и даже доставляют его покупателям.

Такое взаимодействие между устройствами нужно там, где требуется автоматизировать процесс или собирать и анализировать много данных. Машины справляются с этим лучше, чем люди.

Архитектура сетей M2M

Стремительное развитие технологических возможностей современных сетей мобильной связи третьего, четвертого и следующего поколений (UMTS/LTE/EPS) и сетей с усовершенствованной технологией GSM (Evolved EDGE)

существенно опережает спрос на их услуги со стороны пользователей и заставляет операторов обращать внимание на смежные рынки. Таким рынком может стать рынок услуг M2M (machine-to-machine или mobile-to-machine) [55].

Появление инновационных решений в виде встроенных неперемещаемых SIM-карт в устройствах M2M (видеокамерах, музыкальных плеерах и других устройствах бытовой электроники) дает операторам возможность реализовывать новые бизнес-модели услуг путем создания сетей M2M для более широкого класса устройств бытовой электроники и медицинских устройств в мобильных сетях.

Текущая ситуация на рынке услуг M2M определяется прежде всего существующей экосистемой M2M и наличием спроса на эти услуги. Услуги M2M представляют услуги автоматизированного соединения двух или более устройств M2M для обмена информацией и управления ими. В ходе обмена информацией человеческое присутствие и влияние на внутренние телекоммуникационные процессы не предусматривается. Экосистему M2M создают следующие субъекты M2M телекоммуникаций:

- M2M сервис-провайдеры, обеспечивающие предоставление услуг M2M;
- Операторы связи (мобильные или фиксированные), предоставляющие для сетей M2M; инфраструктуру своих телекоммуникационных сетей;
- Конечные потребители услуг (пользователи M2M услуг) как абоненты сервис-провайдера услуг M2M.

Основные элементы архитектуры сетей M2M разделены на три домена [57]: домен устройств M2M (домен капиллярной сети); сетевой домен (ядро базовой сети M2M) и домен приложений. Кроме указанных доменов в состав сети M2M входят соответствующая сеть доступа и транспортная сеть, которые строятся на основе сетей 3GPP и NGN сетей. Взаимодействие различных доменов сети M2M показано на рис. 13.2.

Устройства M2M позволяют быстро воспользоваться услугами M2M и функциями доменной сети. Устройство M2M может быть соединено с сетью доступа либо напрямую, либо через локальную сеть M2M и шлюз M2M.

Локальные сети M2M предоставляют соединение между устройствами M2M и шлюзами M2M с использованием PAN-технологий (IEEE 802.15, SRD, UWB, Zigbee, Bluetooth) или локальных сетей (PLC, M-BUS, Wireless M-BUS).

Шлюзы M2M обеспечивают устройствам M2M гарантированное межсетевое взаимодействие и подключение к сети и прикладным доменам. Шлюз M2M может использоваться для различных приложений устройств M2M. Функционально шлюз M2M может быть объединен в одном модуле с устройством или группой устройств M2M.

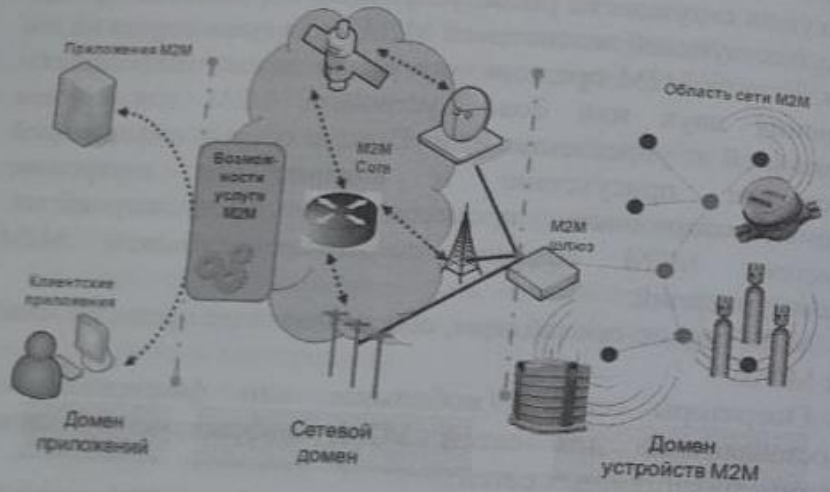


Рис. 13.2. Взаимодействие различных доменов сети M2M

Сети доступа позволяют домену устройств M2M обеспечивать соединение с ядром сети M2M (базовой сетью). Функциональные возможности сетей доступа M2M базируются на возможностях существующих сетей доступа (xDSL, HFC, PLC, VSAT, GERAN, UTRAN, LTE, W-LAN и WiMAX) и позволяют расширить как перечень услуг, так и их возможности.

Транспортная сеть обеспечивает транспортировку данных между сетевым доменом и доменом приложений. Функциональные возможности транспортных сетей в сетях M2M базируются на возможностях существующих транспортных сетей

и так же, как сети доступа, позволяют расширить перечень услуг M2M и их возможности.

Базовая сеть M2M предоставляет функциональные возможности IP-соединения элементов сети M2M, сервисные и сетевые функции управления, межсетевое взаимодействие, роуминг и обеспечивает безопасность сети. Функциональные возможности базовой сети M2M основываются на соответствующих функциональных возможностях существующих базовых сетей 3GPP CN (например, GPRS, EPC), ETSI TISPAN CN.

Основные функциональные возможности базовой сети M2M (Service Capability, SC), реализуемые соответствующими функциональными модулями сети M2M, включают [58]:

- управление возможностями приложений – Application Enablement (xAE);
- обеспечение общих взаимосвязей в сети – Generic Communication (xGC);
- обеспечение достижимости устройств/шлюзов, адресации и хранения данных – Reachability, Addressing and Repository (xRAR);
- выбор взаимосвязей – Communication Selection (xCS);
- удаленное управление устройствами – Remote Enttity Management (xREM);
- обеспечение безопасности – SECurity (xSEC);
- сохранение истории и данных – History and Data Retention (xHDR);
- управление обработкой запросов – Transaction Management (xTM);
- управление компенсацией – Compensation Broker (xCB);
- экспозицию базовой сети операторам связи – Telco Operator Exposure (xTOE);
- доверительное сетевое взаимодействие – Interworking Proxy (xIP), где x – переменная, означающая точку приложения этих функций в сети M2M и принимающая значения:

N – для сетей, содержащих инфраструктуру базовой сети M2M, соединенную со шлюзами и устройствами M2M;

G – для шлюзов, напрямую управляющих устройствах M2M в локальной сети M2M и соединенными с базовой сетью M2M;

D – для устройств M2M, которые могут напрямую присоединяться к базовой сети M2M или к шлюзу M2M.

Функциональные возможности сети M2M могут быть как специальными, поддерживающими приложения M2M, так и общими, поддерживающими общесетевые возможности: сбор и агрегацию данных, доставку многоадресных сообщений и др.

Интерфейсы mIa, dIa, mId сети M2M на основе принципов открытых интерфейсов обеспечивают взаимодействие между доменом приложений и базовой сетью M2M, между прикладным и функциональным уровнем домена устройств M2M, между устройствами M2M и шлюзом M2M соответственно [56].

Типовая функциональная архитектура и интерфейсы сети M2M показаны на рис. 13.3.

- Интерфейс mIa сети M2M обеспечивает взаимодействие приложения M2M с функциональными модулями сети M2M или домена приложений.

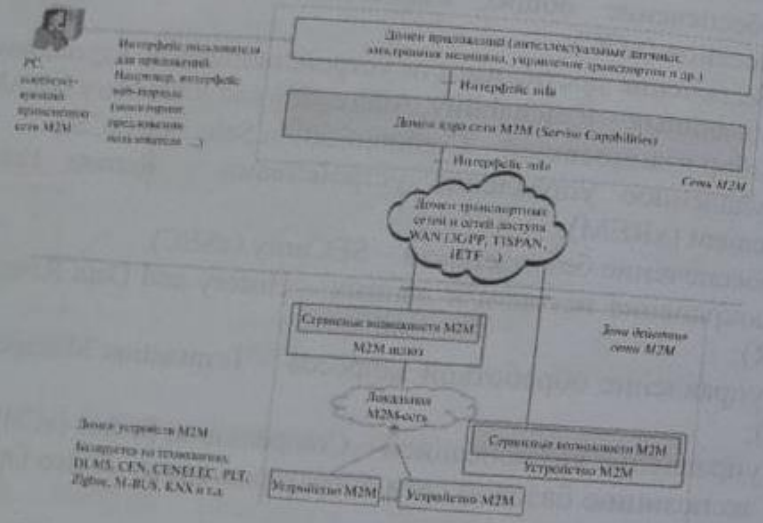


Рис. 13.3. Типовая функциональная архитектура и интерфейсы сети M2M

- Интерфейс dIa сети M2M обеспечивает взаимодействие приложения M2M, активированного в M2M-устройстве, и доступ к функциональным модулям этого M2M-устройства или M2M-шлюза, а также взаимодействие приложения M2M,

активированного в M2M-шлюзе, и иметь доступ к функциональным модулям этого M2M-шлюза

- Интерфейс mId сети M2M обеспечивает взаимодействие M2M-устройства или M2M-шлюза с модулями основных функций M2M в сети и доменом приложений. Интерфейс mId использует функции присоединения базовой сети в качестве своего базового уровня.

13.2. Общие принципы, технологии, области применения M2M

Деятельность рабочих групп 3GPP по формированию технических требований к M2M

Впервые партнерский проект 3GPP начал разработку технологий связи 3GPP для использования в сетях M2M в 2007 г., когда исследовался вопрос оказания услуг связи «машина-машина» при помощи мобильных сетей, стандартизованных 3GPP (GSM/EDGE/ UMTS/HSPA) [59].

Это исследование определило потенциал услуг M2M и показало возможность их движения к премиальному сегменту мобильного рынка. В 2010 г. рабочие группы 3GPP начали процесс внедрения результатов исследований по M2M в разработку технических спецификаций на основе технических отчетов TS 22.368 [60] и TR 23.888 [61].

Технические спецификации TS 22.368 [60] определили общие и специфические требования к технологии связи M2M. Работа над их созданием инициировала два дополнительных исследования, которые были сфокусированы на альтернативах использования нумерации E.164 для M2M и совершенствовании требований M2M (TR 22.888) [62].

Кроме рабочей группы 3GPP SA (Services and System Aspects), еще две рабочие группы: по сетям радиодоступа (Radio Access Network, RAN) и GERAN (GSM Edge Radio Access Network) - также активно работали над улучшениями Релиза 10 для сетей и услуг M2M при подготовке технических отчетов TR 37.868 (Study on RAN Improvements for MTC) и TR 43.868 (Study on GERAN Improvements for MTC).

Технический отчет TR 33.812 содержит результаты исследования возможностей сетевой безопасности удаленного резервирования и изменения подписки на услуги для оконечного оборудования M2M. В техническом отчете TR 33.868 также рассмотрены аспекты сетевой безопасности M2M.

Технический отчет TR 23.888 [61] выделяет ключевые вопросы M2M и предлагает возможные решения. Технические требования Релиза 10 в части технологии связи M2M направлены на совершенствование требований, связанных с перегрузками и контролем этих перегрузок в сетях LTE/3GPP, а остальные вопросы перенесены на дальнейшие релизы.

В техническом отчете TR 22.888 [60], подготовленном в рамках исследований по Релизу 10, было сформулировано более 14 новых специфических требований к сетям и услугам M2M:

- *низкая мобильность*, что определяется моделями поведения устройств M2M, которые могут быть статичными (неперемещаемыми), иметь ограниченную мобильность (nomadic) или быть мобильными, но в пределах строго определенного региона. Эти свойства M2M-устройств позволяют снижать служебный трафик сигнализации, отвечающий за мобильность, и частоту передаваемых отчетов от устройств M2M;
- *контроль времени связи*, когда данные от устройств M2M могут быть переданы или приняты только в строго определенный период и служебный трафик за пределами этих заранее определенных временных окон минимизирован;
- *толерантность к моменту* проведения сеанса связи и задержкам сообщений, которая реализуется за счет того, что приложения для передачи данных могут обеспечивать независимость от таких задержек;
- *реализация только принципов коммутации пакетов*, вследствие чего доступ в сеть разрешен для ранее установленных услуг и переключение возможно как с применением, так и без применения мобильных терминалов;
- *использование международного номера абонента* для нумерации *(International Subscriber Directory Number, MSISDN)*;
- *передача небольших объемов данных* (Small Data Transmissions), так как большинство M2M-устройств передает небольшие потоки данных в линии вверх;

- *инициализация только мобильного вызова* (Mobile Originated Only), так как сеть предоставляет механизмы снижения управляющего служебного трафика, создаваемого устройствами M2M;
- *завершение мобильного вызова* (Infrequent Mobile Terminated) на сетях LTE/3GPP;
- *мониторинг M2M-сети*, осуществляемый, поскольку сеть M2M не предназначена для предотвращения краж M2M-устройств, для выявления таких событий в сети M2M, как необъяснимое поведение и потеря соединения, уведомление конечного пользователя о результатах мониторинга;
- *приоритетная передача аварийных сообщений* (Priority Alarm Message, PAM), требующих немедленного внимания оператора и пользователей сети M2M, в случаях краж, срочных или чрезвычайных ситуаций;
- *безопасность соединений*, особенно при соединении через роуминговых операторов;
- *переключение M2M-устройств с учетом особенностей расположения* (оператор хранит информацию о расположении и может «разбудить» или переключить M2M-устройство в определенной области сети M2M);
- *обеспечение достижения места назначения данными в сети M2M для данных*, передаваемых в линии вверх, за счет их передачи, по возможности, на особые адреса;
- *поддержка редких передач*, для чего ресурсы сети доступа LTE/3GPP распределяются только по мере необходимости;
- *возможности группового использования устройств M2M* для вещания на выделенные группы M2M-устройств, на которые при этом распространяются требования политик, тарификации, адресации и QoS.

Взаимодействие сетей LTE/3GPP и M2M при оказании услуг.

Техническими спецификациями 3GPP TS 22.368 [60] определено три модели использования различных вариантов управления сетью M2M и взаимодействия между устройствами M2M и M2M-сервером, а также M2M-приложением:

– *модель A* обеспечивает прямое взаимодействие между устройствами M2M по принципу «каждый с каждым» без промежуточного M2M-сервера, а также прямое взаимодействие с M2M-приложениями как с приложениями верхнего уровня оператора сети LTE/3GPP. Пример на рис. 13.4 реализуется только Релизом 12;

– *модель B* обеспечивает взаимодействие устройств M2M с использованием M2M-сервера, расположенного за пределами домена оператора, и оператор сети LTE/3GPP поддерживает это сетевое взаимодействие с M2M-сервером. В качестве точек взаимодействия используются MTCsp и MTCsms, которые могут являться как внешними интерфейсами для оператора сети M2M (сервис-провайдера), так и внутренними при управлении сетью M2M со стороны оператора сети LTE/3GPP (рис. 13.5);

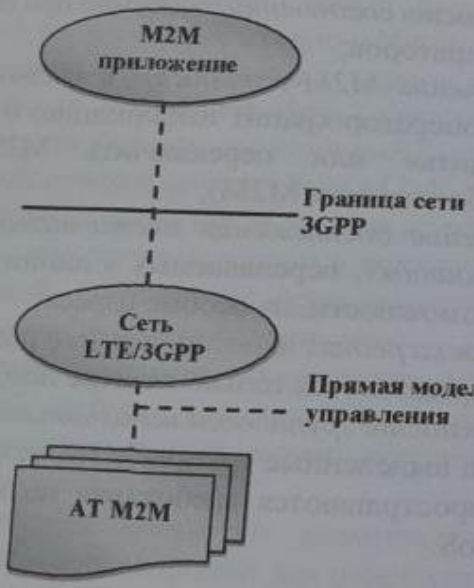


Рис. 13.4. Прямое взаимодействие между устройствами M2M с приложениями верхнего уровня оператора сети LTE/3GPP (модель A)

– *модель C* обеспечивает взаимодействие устройств M2M

посредством M2M-сервера, расположенного в домене оператора. Сеть домена оператора предлагает программируемый интерфейс приложений (API) на M2M-сервере, и потребитель M2M-услуг соответственно имеет доступ к M2M- серверу посредством этого API (рис.13.6).

При реализации сценария, когда M2M-устройства взаимодействуют с одним M2M-сервером или более, оператор сети LTE предоставляет соединение к одному или нескольким M2M-серверам. При этом используемый M2M-сервер управляется оператором сети так, как показано на рис. 13.4, либо сервер M2M может не контролироваться оператором сети (рис. 13.7).

M2M-приложения для конечных услуг используют службы передачи данных, предоставляемые сетью LTE/3GPP, и частично службы M2M-сервера. Сеть LTE/3GPP обеспечивает для сети M2M услуги транспортной сети и сетевого взаимодействия (включая услуги служб передачи данных 3GPP (Bearer Services), IMS и SMS), а также возможности оптимизации сетей, которые способствуют повышению эффективности взаимодействия устройств M2M.

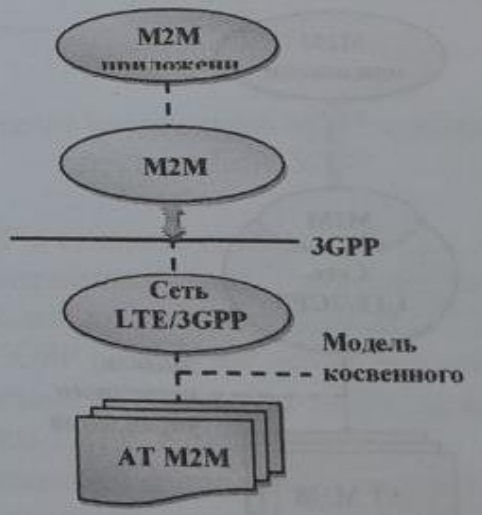


Рис.13.5. Взаимодействие устройств M2M с использованием M2M-сервера, расположенного за пределами домена оператора (модель B)

На рис. 13.6 представлена архитектура сети LTE/3GPP, в которой абонентский терминал (АТ) M2M используется для взаимодействия с сетью M2M посредством соответствующей сети доступа интерфейса LTE-Uu/Uu/Um.

Здесь же показаны варианты моделей взаимодействия A и B, а также возможность использования гибридной модели (A+B), в которой для трафика плоскости пользователя реализуется модель прямого взаимодействия (A), а для служебного трафика плоскости управления сети M2M - модель непрямого взаимодействия (B).

Как следует из рис. 13.7, сервер M2M-приложений, поддерживающий различные варианты услуг M2M, и точка сопряжения с программируемым интерфейсом API находятся за пределами границы сети LTE/3GPP.

Однако M2M-сервер располагается как за пределами домена оператора, так и внутри. Точки сопряжения MTCsp и MTCsms могут быть частью функционального модуля межсетевого взаимодействия M2M-IWF (таблица), обеспечивая доступ к M2M-серверу, при использовании сетей с технологией ТО-3GPP (CDMA-2000, WiMAX и др.).

Рис. 13.6. Взаимодействие устройств M2M посредством M2M-сервера, расположенного в домене оператора (модель C)

Приложения M2M могут иметь совмещенное размещение на сервере M2M, который является элементом сети M2M, соединенным с сетью и взаимодействующим как с устройствами M2M, так и с узлами сети мобильного доступа LTE/3GPP. Архитектура сети LTE/3GPP обеспечивает поддержку роуминга устройств M2M и доступ к M2M-услугам за счет использования интерфейса LTE-Uu/Uu/Um визитной сети LTE/3GPP.

При роуминге устройства M2M используют точку взаимодействия MTCu визитной сети мобильного оператора LTE/3GPP для доступа к услугам M2M домашней сети.

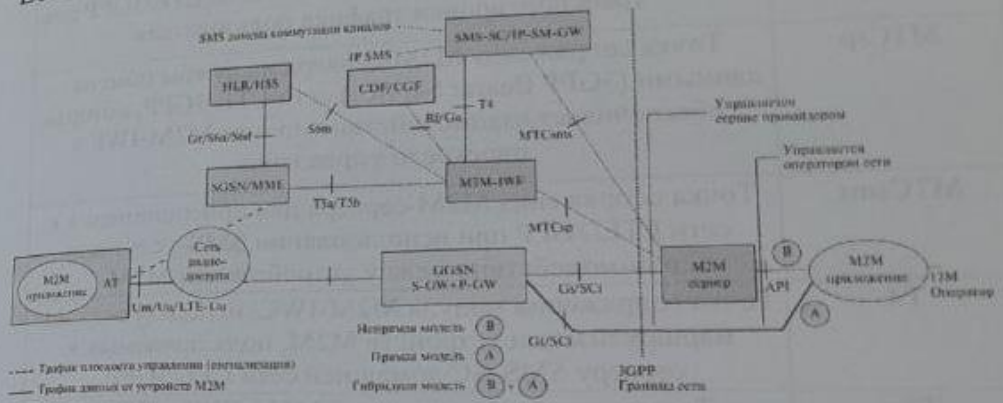


Рис. 13.7. Сетевая архитектура M2M с использованием сети доступа LTE/3GPP

Сеть LTE/3GPP в качестве сети доступа для M2M-сети, кроме традиционных, выполняет ряд дополнительных функций, определяемых моделью взаимодействия. Соответственно и модули сети LTE/3GPP реализуют новые функции, что зависит от степени их вовлеченности в решение задач управления и оказания услуг M2M (таблица 13.1):

- *M2M-IWF* выполняет функцию межсетевого взаимодействия и размещается у оператора домашней сети LTE/3GPP. Обычно этот модуль, обеспечивающий передачу или трансляцию протоколов управления и сигнализации, используемых в точке сопряжения MTCsp, скрыт внутри топологии сети LTE/3GPP. Кроме того, M2M-IWF производит аутентификацию M2M-сервера

авторизацию запросов M2M-сервера в плоскости управления;

Таблица 13.1

Главные элементы архитектуры сети LTE/3GPP и точки сопряжения сетей M2M и LTE/3GPP

Элементы архитектуры и точки	Назначение
MTCu (LTE-Uu)	Точка сопряжения M2M-устройств и сети LTE/3GPP для транспортировки трафика пользователя
MTCsp	Точка сопряжения M2M-сервера и службы обмена данными (3GPP Bearer Service) сети LTE/3GPP, которая обеспечивает взаимодействие модуля M2M-IWF в плоскости управления
MTCsms	Точка сопряжения M2M-сервера для присоединения к сети LTE/3GPP при использовании SMS-услуг для взаимодействия между устройствами M2M
T4	Точка сопряжения модуля M2M-IWC, используемая для маршрутизации устройств M2M, подключаемых к серверу SMS-SC домашней сети LTE/3GPP
T5a	Точка сопряжения модулей M2M-IWC и SGSN
T5b	точка сопряжения модулей M2M-IWC и MME
S6m	Точка сопряжения модуля M2M-IWF, опрашиваемая модулем HSS для адресации при использовании нумерации E.164 на основе MSISDN
M2M-пользователь	Юридическое лицо, которое использует объединенные в сеть абонентские терминалы M2M (обычно контрактный партнер оператора сети связи)
Абонентский терминал M2M (AT M2M)	Оборудование пользователя сети M2M для взаимодействия с M2M-сервером и другими устройствами M2M в сети
M2M-сервер	Модуль для обеспечения взаимодействия M2M-устройств с мобильной сетью LTE/3GPP

- *HSS* осуществляет терминацию присоединений к модулю M2M-IWF в точке сопряжения S6m, сохранение и обеспечение

нумерации устройств M2M на базе E. 164 с использованием MSISDN и внешних абонентов на основе IMSI, а также маршрутизацию сетевой информации об адресах используемых модулей MME/SGSN/MSC для модуля M2M-IWF;

- *PGW* обеспечивает прямое взаимодействие между устройствами M2M по принципу «каждый с каждым» без промежуточного M2M-сервера или непрямое взаимодействие с использованием M2M-сервера, а также реализует гибридные модели взаимодействия;

- *MME* осуществляет терминацию присоединений в точках взаимодействия T5b/T5a, получает команды на переключение устройств M2M из модуля M2M-IWF и сохраняет историю этих переключений, инкапсулируя данные в NAS- сообщения для передачи их устройствам M2M.

Модели трафика M2M и управление перегрузками в сети LTE/3GPP

Трафик, создаваемый в сети LTE/3GPP при оказании услуг M2M, характеризуется следующими особенностями [63-66]:

- спорадическим характером взаимодействия оконечных устройств M2M в сети и короткой продолжительностью этих сеансов;
- незначительным объемом передаваемых данных, требующим небольшой пропускной способности сети доступа, но при этом большим количеством подключенных оконечных M2M-устройств;
- низкой мобильностью оконечных M2M-устройств или полным отсутствием таковой, а также низкой активностью в линии вверх;
- большими группами оконечных M2M-устройств с одновременным запросом соединения в сети;
- низким потреблением энергии оконечными M2M-устройствами, что является следствием небольшого трафика;
- низкими запросами на вычислительные мощности и низкой стоимостью оконечных M2M-устройств как следствие небольшого трафика;
- высокими требованиями к безопасности данных.

Трафик, генерируемый в сетях M2M, можно разделить на два класса: класс для низкого уровня трафика от устройств M2M и класс для высокого уровня трафика от устройств M2M (услуги видеонаблюдения).

M2M-устройства способны генерировать большие объемы служебного трафика (Signaling), который может вызывать перегрузку сети, как минимум, в следующих двух ситуациях:

- M2M-приложение, используемое во многих AT M2M, запрашивает множество AT выполнить какое-то действие (например, команду Attach/Connect Requests) посредством сети LTE/3GPP одновременно;
- большое количество роуминговых AT M2M (in- roamers) движутся и собираются в одном месте, вследствие чего локальные сети устройств M2M переполняются, что ведет к нехватке ресурсов обслуживающей сети LTE/3GPP.

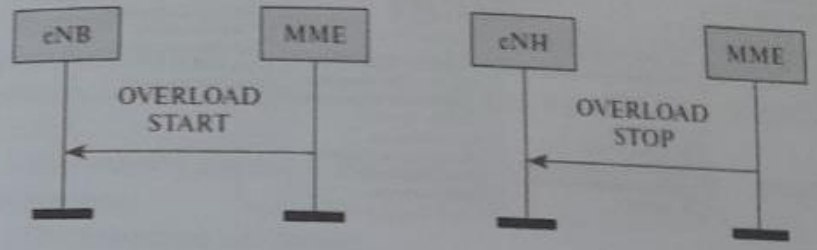
Эти ситуации могут отрицательно влиять как на характеристики сети доступа LTE/3GPP, вызывая перегрузки внутри сети, так и на качество услуг M2M и даже на восприятие пользователя (QoS/End-User Experiences) таких высокодоходных услуг, как передача речи и другие мультимедийные услуги.

При управлении в сети LTE/EPC перегрузками трафика услуг M2M используются следующие способы:

- назначение абонентскому терминалу низкого приоритета доступа при помощи команды Low Access Priority для дифференциации низкого приоритета и задержки для обеспечения толерантности служебного трафика M2M-устройств;
- установление соединения, инициируемого абонентским терминалом, с использованием протокола управления радиоресурсами RRC с низким приоритетом обслуживания, причем терминал может быть индицирован в сети радиодоступа E-UTRAN;
- управление служебным трафиком протокола RRC для обеспечения использования расширенного времени ожидания обслуживания в случае режекции сообщений от M2M- устройств;
- инициирование модулем управления мобильностью MME режекции установления соединения в сети радиодоступа E-UTRAN посредством протокола RRC.

На рис. 13.8 показаны диаграммы обмена командами в сети E-UTRAN между базовой станцией и модулем управления мобильностью при управлении перегрузками M2M-трафика.

Базовая станция eNB, получив сообщение OVERLOAD START (содержащее команду «Начало перегрузки сети» на режекцию установления соединения по протоколу RRC в сети радиодоступа E-UTRAN) от модуля управления MME, работающего с перегрузкой, должна снизить уровень служебного и пользовательского трафика.



13.8-расм. Управление перегрузками M2M трафика

При получении сообщения OVERLOAD STOP («Конец перегрузки сети») базовая станция eNB вернется к нормальной работе с модулем управления мобильностью MME без ограничений на генерируемый ею трафик.

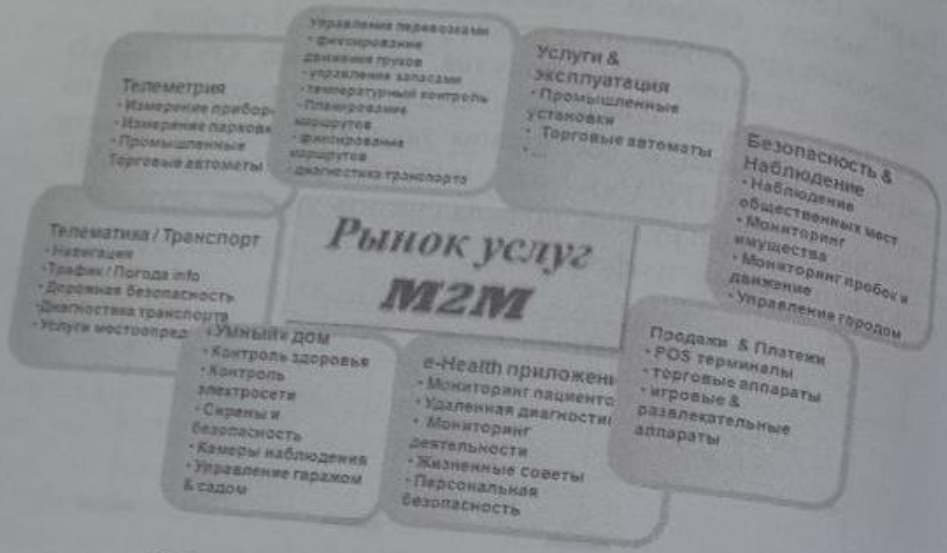
Перспективные модели M2M и ниши рынка услуг

Основными нишами рынка услуг M2M являются услуги систем мониторинга услуг ЖКХ и энергопотребления, систем безопасности, медицинские услуги, управление транспортом, автоматизация промышленных процессов и другие приложения. Более детально эти приложения показаны на рис. 13.9.

Наиболее важными из них в ближайшие годы будут;

- **Промышленная автоматизация и мониторинг производства**
  - Работа промышленных производственных линий заводов и фабрик-прохождение производственных процессов-диагностика-обслуживание текущих запросов,
- **Телемедицина и электронная охрана здоровья**
  - Нательные датчики-сенсоры и текущая диагностика

- Удаленные медицинские консультации



13.9-расм. Перспективные модели M2M

- **Безопасность и видеонаблюдение**
  - Мониторинг датчиков домашней безопасности, сирены, удаленный контроль доступа в помещения и терморегулирования, видео приложения
- **Телеметрия**
  - Интеллектуальные измерения, датчики для энергетических сетей,
- **Отслеживание и управление имуществом**
  - Управление инвентаризацией имущества, гео-контроль границ объектов недвижимости
- **Управление движением больших групп транспорта (Fleet Management)**
  - Расположение и доступность, движение транспортных средств
- **Телематика бытовых электронных и электрических приборов**
  - приборная среда автомобиля/навигация, удаленные диагностика/безопасность/обслуживание
- **Реклама**

  - Цифровые табло, внутри магазинные устройства, специальные приложения
- **Потребительские приложения (Consumer Applications)**
  - Внутридомовой мониторинг, оплата и продажа через POS-терминалы/электронные киоски
  - Цифровые видеокамеры, электронные книги, медиа плееры, игровые приставки и устройства.
- **Беспроводные модули для персональных компьютеров, ноутбуков, UMPC.**

Основные бизнес-модели услуг M2M

Исходя из выделенных нишевых услуг M2M ведущими международными организациями связи исследованы пять основных бизнес-моделей для внедрения и реализации услуг M2M [57, 58]:

- Интеллектуальные измерения в домах и нежилых помещениях;
- Электронное здоровье;
- Управление бытовой электроникой;
- Автоматизация управления транспортом;
- Автоматизация управления транспорта города.

Бизнес модель «Интеллектуальные измерения в домах

Бизнес модель «Интеллектуальные измерения в домах и нежилых помещениях», показанная на рис. 13.10 реализует последние достижения в области грид-технологий и энергосбережения.

Позволяет с высокой эффективностью управлять всеми энергетическими и ресурсными датчиками в домах и офисах, производственных помещениях, минимизируя потребление тепла, электричества, воды, газа.

Позволяет дистанционно контролировать уровень потребления этих ресурсов, управлять их потреблением, осуществлять их тарификацию и оптимизацию расходов.

Потенциальный объем рынка определяется количеством домохозяйств и промышленных предприятий.

Рис. 13.10. Бизнес модель «Интеллектуальные измерения в домах

Бизнес модель «Электронное здоровье»

Бизнес модель «Электронное здоровье», показанная на рис. 13.11 является самой социально-ориентированной моделью. Текущая ситуация в здравоохранении благополучной Европы и США характеризуется в существенной потребности использования M2M устройств, что определяется тем, что более 600 млн. населения развитых стран мира старше 60 лет; наблюдается рост хронических заболеваний – более 860 млн. пациентов требуют ежедневного мониторинга состояния здоровья; 1 млрд. взрослого населения имеют избыточный вес; затраты на здравоохранение только в США составили более 2 триллионов долл. США в 2009 году; 75-85% расходов здравоохранение тратится на лечение хронических заболеваний. Поэтому использование медицинских датчиков и устройств мониторинга состояния здоровья больных на основе M2M-технологий является одним из главных приложение услуг M2M в будущем.

Потенциальный объем рынка определяется количеством платежеспособных абонентов, нуждающихся в мониторинге состояния здоровья.

Рис.13.11. Бизнес модель «Электронное здоровье»

Бизнес-модель «Управление бытовой электроникой»

Бизнес-модель «Управление бытовой электроникой» (рис. 13.12) становится все более востребованной для повышения возможностей управления ресурсами бытовых электронных приборов и устройств, а также объединения их в группы.

В бытовой электронике (благодаря разработке инновационных решений для технологии M2M) появились встроенные процессоры и SIM-карты, реализующие возможность управления и обмена информацией между устройствами в сетях M2M (например, «умный дом» и «умный офис»). Данная бизнес-модель позволяет решать задачи наблюдения за всеми объектами в домашнем окружении, контролировать запасы и автоматически запрашивать расходные материалы бытовой техники, связывать фото- и видеокамеры с социальными сетями, автоматически посещать электронные библиотеки и др.

Потенциальный объем такого рынка определяется количеством домохозяйств, подписавшихся на услугу M2M, и количеством активно действующих предприятий.

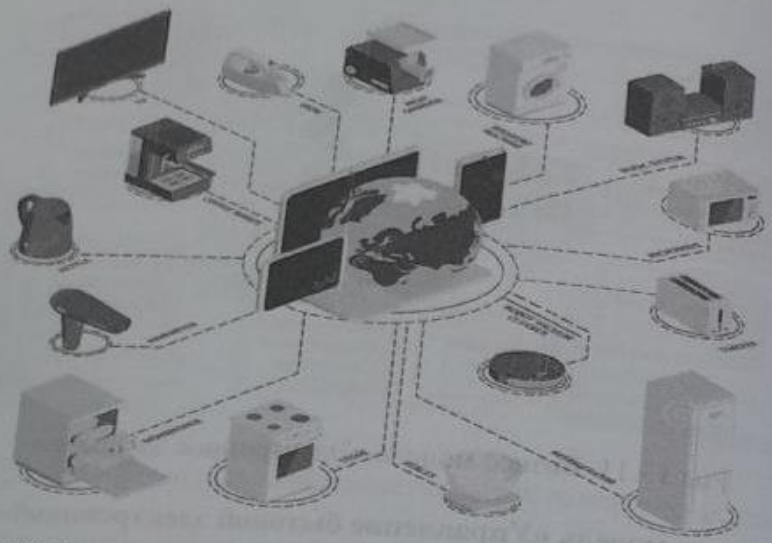


Рис. 13.12. Бизнес модель «Управление бытовой электроникой»

Бизнес-модель «Автоматизация управления транспортом»

Бизнес-модель «Автоматизация управления транспортом» (рис. 13.13) позволяет осуществлять на основе сетей M2M информационный обмен между устройствами контроля движения и устройствами управления транспортным средством в интересах обеспечения безопасности движения, управление группами автомобилей, управление маршрутами движения, предупреждение воровства грузов и транспорта.

Потенциальный объем рынка определяется количеством транспортных средств, оснащенных датчиками для информационного обмена в сетях M2M.

Бизнес-модель «Автоматизация управления городским транспортом»

Бизнес-модель «Автоматизация управления городским транспортом» (рис. 13.14) нацелена на решение задач, связанных с управлением транспортными потоками, работой светофоров, мониторингом и управлением работой городского общественного

транспорта, управлением освещенностью магистралей и улиц города и др.

Потенциальный объем рынка определяется количеством городов, нуждающихся в автоматизированной поддержке управления городскими транспортными потоками и общественным транспортом.

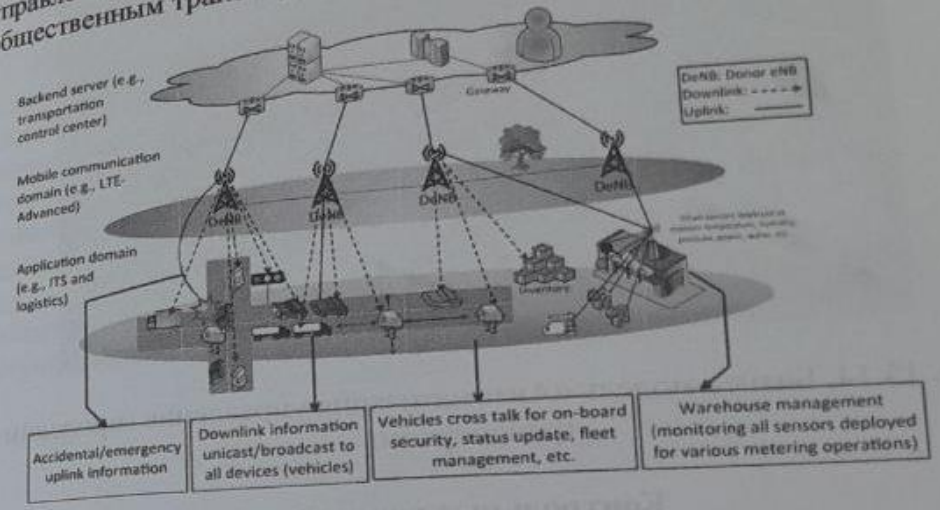


Рис.13.13. Бизнес-модель «Автоматизация управления транспортом»

Главной отличительной особенностью сетей M2M от мобильных сетей связи является низкий уровень трафика оконечных устройств и необходимость сведения огромного количества оконечных M2M-устройств, на порядок превышающего число абонентов мобильных сетей, в единые сети. Несмотря на низкий уровень трафика, генерируемого в сетях M2M, и относительную дороговизну на данном этапе абонентских терминалов M2M (сравнительно с терминалами 2G/3G), сети LTE/3GPP рассматриваются как важнейшее решение для создания сетей доступа операторами сетей M2M.

Архитектура сети доступа LTE/3GPP, а также модели управления и взаимодействия с сетью M2M определяются наличием в этой сети отдельного M2M-сервера, реализующего

различные M2M-приложения, и расположением этого сервера в границах или за пределами сети LTE/3GPP.

Рис. 13.14. Бизнес-модель «Автоматизация управления городским транспортом»

Контрольные вопросы

1. Что означает межмашинное взаимодействие M2M?
2. Объясните разницу между M2M и IoT.
3. Приведите и объясните архитектуру сетей M2M.
4. Какие интерфейсы используются в сетевой архитектуре M2M и что их обеспечивает?
5. Объяснить модели взаимодействия сетей LTE/3GPP и M2M при оказании услуг.
6. Приведите и объясните архитектуру сети M2M с использованием сети подключения LTE / 3GPP.
7. Расскажите об основных тенденциях рынка M2M-услуг.
8. Приведите и объясните бизнес-модель интеллектуальных измерений в нежилых зданиях.
9. Что предоставляет собой бизнес-модель электронного здравоохранения?
10. Бизнес-модель автоматизации управления транспортом и его основная цель.

14.1. Общие сведения о радиочастотной идентификации

Радиочастотная идентификация RFID (Radio Frequency Identification) - общий термин, используемый для обозначения систем, которые беспроводным путем посредством радиоволн считывают идентификационный номер (в форме уникального серийного номера) какого-либо предмета или человека. RFID относится к обширной области технологий автоматической идентификации (Auto-ID), которые включают в себя также штриховые коды, оптические считыватели и некоторые биометрические технологии, как например, сканирование сетчатки глаза (рис. 14.1) [67-72].

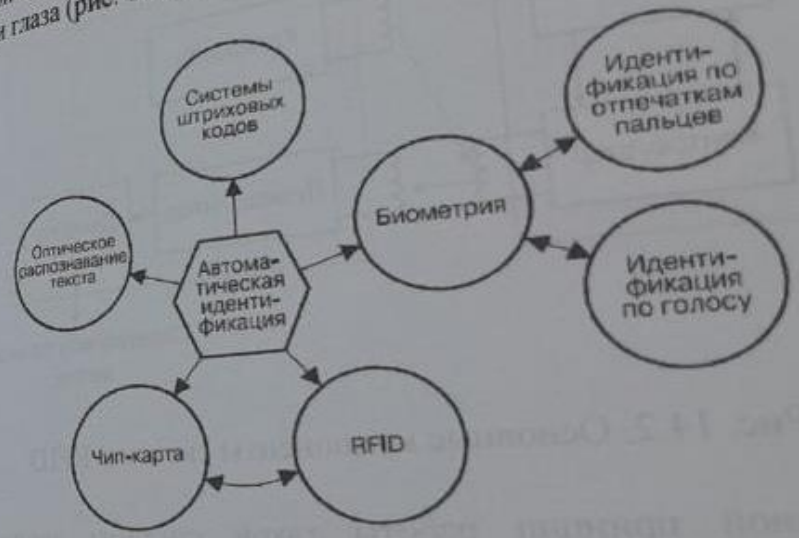


Рис. 14.1. Основные системы автоматической идентификации

Любая RFID-система состоит из считывающего устройства (ридера) и небольших идентифицирующих устройств (RFID-меток), которые содержат обычно резонансный LC- контур, контроллер и электрически стираемое перепрограммируемое постоянное запоминающее устройство EEPROM (Electrically

Содержимое памяти специфично для каждой метки и позволяет идентифицировать носителя метки (человека или объект).

В общем случае технологии Auto-ID используются с целью экономии времени и труда, затрачиваемых на ввод данных вручную и улучшения точности информации. Некоторые Auto-ID технологии, такие как системы штрихового кода, зачастую требуют участия человека, для сканирования и фиксирования информации вручную. Система RFID же сконструирована таким образом, что дает возможность считать и передавать данные в компьютерную систему без участия человека и в реальном масштабе времени. Технология RFID способна принести пользу в самых разных областях человеческой деятельности, включая промышленность, торговлю, образование, медицину и др.

Рис. 14.2. Основные компоненты системы RFID

Основной принцип работы такой системы сводится к следующему. Считыватель излучает радиоволну, которая принимается единственной меткой. Метка, таким образом, получает энергию и отражает радиоволну той же частоты (благодаря индуктивной связи), модулированную кодированным содержимым памяти. Считыватель принимает этот сигнал, демодулирует и декодирует его, чтобы определить содержимое

памяти. Затем идентификационная система верхнего уровня проверяет эти данные и, соответственно, управляет процессом.

Привлекательность такой системы состоит в том, что она обеспечивает бесконтактное взаимодействие между считывателем и RFID-метками (избегая, таким образом, ограничений на позиционирование объекта с меткой), причем метки не требуют источника питания.

Однако когда в поле считывателя находятся две метки, они обе отвечают на излученный считывателем сигнал. При этом демодулированный сигнал считывателя является смесью двух компонент от двух меток и не может быть декодирован. Такая система неспособна одновременно идентифицировать два объекта. Известны несколько способов решения этой проблемы. Некоторые из них состоят в том, что считыватель и метки взаимодействуют в соответствии с заранее определенным протоколом, так что сигналы каждой метки успешно разделяются. Другой подход состоит в использовании меток на различных частотах.

По дальности считывания RFID-системы можно подразделить на следующие типы:

- ближней идентификации (считывание производится на расстоянии до 20 см);
- идентификации средней дальности (от 20 см до 5 м);
- дальней идентификации (от 5 м до 100 м).

Несмотря на то, что RFID-технология не нова и ее используют уже достаточно долго, о ее массовом применении заговорили не так давно. Это произошло потому, что до недавнего времени RFID-метки - основной компонент системы - стоили довольно дорого. И только некоторые компании могли себе позволить использование RFID-метки, цена на которые до недавнего времени превышала доллар и больше за единицу. Поэтому, в основном их использовали компании, которые выпускали продукцию многократного использования. В таком случае код продукта сохранялся и его можно было использовать в дальнейшем. Однако наиболее практичные современные RFID-метки являются одноразовыми, конечный потребитель может их выбросить вместе с ненужной ему упаковкой.

Использование RFID-систем наиболее актуально для компаний, которые участвуют в процессе производства, поставки и реализации различных товаров. Во-первых, используя RFID-системы, упрощается проведение инвентаризации товаров на складе. Также значительно упрощаются их прием и отгрузка. Кроме того, благодаря наличию RFID-меток и RFID-считывателей и специального компьютерного оборудования стало возможным создавать объемные базы данных по учету и движению товара.

По своему функционалу метод сбора данных на основе RFID-меток в значительной степени похож на технологию штрих-кода, широко применяемой во всем мире при маркировке различных товаров. Однако у RFID-систем есть много преимуществ по сравнению с системами на базе штрих-кода (таблица 14.1).

Таблица 14.1

Сравнение характеристик систем RFID и на базе штрих-кода

Характеристики технологии	RFID	Штрих-код
Необходимость в прямой видимости метки	Чтение даже скрытых меток	Чтение без прямой видимости
Объём памяти	От 10 до 10 000 байт	До 100 байт
Возможность перезаписи данных и многократного использования	Есть	Нет
Дальность регистрации	До 100 м	До 4 м
Одновременная идентификация нескольких	До 200 меток в секунду	Невозможна
Устойчивость к воздействиям окружающей среды	Повышенная прочность и	Зависит от материала, на который наносится
Срок жизни метки	Более 10 лет	Зависит от способа печати и материала
Безопасность и защита от подделки	Подделка практически невозможна	Подделать легко
Работа при повреждении	Невозможна	Затруднена
Идентификация движущихся объектов	Да	Затруднена

Подверженность электромагнитным помехам	Есть	Нет
Идентификация металлических объектов	Возможна	Возможна
Использование стационарных и ручных считывателей	Да	Да
Возможность введения в тело человека/ животного	Возможна	Затруднена
Габаритные характеристики	Средние и малые	Малые
Стоимость	Средняя и высокая	Низкая

14.2. Структура сети RFID

Метки RFID

Основой технологии RFID и главным ее компонентом является метка (англ. tag) или транспондер (transmitter - передатчик, responder - ответчик), содержащая определенную информацию (например, о продукте, о производстве, месте назначения, сроке реализации и др.), передаваемую на считыватель, когда тот проводит опрос метки. Большинство RFID-меток состоит из двух частей (рис. 14.3).

Первая - интегральная схема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций. Вторая - антенна для приёма и передачи сигнала.

RFID система работает по следующему принципу: радиосигнал посылается считывателем транспондеру (метке), который принимает его и отражает (пассивная метка) или генерирует выходной сигнал (активная метка). В процессе считывания метки происходит передача данных из ее памяти в компьютер, где информация обрабатывается и выводится в понятном для восприятия виде. Конструктивно RFID-метка обычно состоит из микрочипа, прикрепленного к радиоантенне. Компактность RFID-меток зависит от размеров внешних антенн,

которые по размерам превосходят чип во много раз и, как правило, определяют габариты меток.

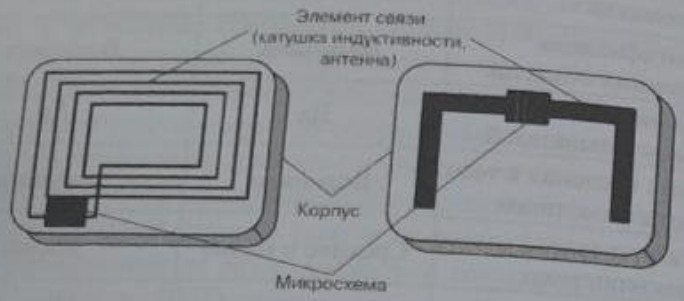


Рис. 14.3. Принципиальная схема RFID метки: слева - метка с индуктивной связью, справа - микроволновая метка с антенной-диполем

RFID метки бывают *пассивные* и *активные* (рис. 14.4). Пассивные метки дешевле и не имеют батареи питания. В метке используется энергия электромагнитных волн, которые излучает считыватель. Такие метки применяются при отслеживании товаров, при контроле доступа, промышленной автоматизации и электронного слежения за товарами.

Рис. 14.4. Пассивная (слева) и активная (справа) RFID метки

Активные RFID метки имеют батарею питания, которая позволяет работать с большей точностью и дальностью считывания. Но из-за наличия батареи активные метки имеют ограниченный срок службы и они более дорогие. Наиболее

распространенный вариант их применения - удаленное слежение за объектами, имеющими высокую ценность и стоимость.

Существуют также *полуактивные (полупассивные)* метки, в которых имеется внутренний источник питания (например, батарея) и электроника для выполнения специализированных задач. Внутренний источник питания дает энергию для работы метки. Однако для передачи своих данных полуактивная метка использует энергию, излучаемую считывателем (ридером). Полуактивная метка также называется меткой со вспомогательной батареей. Обмен информацией между ридером и меткой такого типа всегда инициирует ридер, а затем начинает работу метка.

В свое время индустрия RFID столкнулась с проблемой «замкнутого круга» - метки не станут дешевле, пока не повысится спрос на них, а он не повысится, пока они не станут дешевле. До недавнего времени относительно высокая стоимость RFID ограничивала ее использование. В настоящее время пассивные метки стоят от 20 центов, активные метки - от 10 до 50 долларов и выше.

По конструктивному исполнению выделяют следующие виды RFID меток: карты (пластиковые), самоклеящиеся этикетки бумажные и лавсановые, брелоки и диски.

Память метки - важный элемент RFID системы. В памяти может храниться различная информация, например, уникальный идентификатор объекта, место и дата выпуска продукта и т.п. Обычно объем памяти меток составляет от 16 бит до сотен килобит.

По типу памяти RFID-метки бывают следующих типов:

1) *только с чтением RO (Read Only)* - данные в них записывают только единожды, при их изготовлении, эти метки используются только для идентификации объекта;

2) с *однократной записью и многократным чтением WORM (Write Once Read Many)* - эти метки, кроме идентификатора содержат еще блок памяти, в которую можно однократно записать информацию и которую затем можно неоднократно считывать;

3) *с неоднократными записью и чтением RW* (англ. *Read and Write)* - содержат блок памяти и идентификатор, данные в этих метках можно перезаписывать неоднократно и соответственно стоят они дороже всех остальных меток;

4) *метки SAW-типа*, работающие на принципе поверхностной акустической волны ПАВ (Surface Acoustic Wave - SAW).

Метка SAW-типа в корне отличается от меток на основе микрочипов. Для работы меток SAW-типа используются радиоволны малой мощности в частотном диапазоне 2,45 ГГц. В отличие от меток с микрочипами SAW-метке не нужен источник постоянного тока для ее питания при передаче данных. SAW-метка состоит из дипольной антенны, присоединенной к встречно-штыревому преобразователю IDT (Interdigital TransDucer), расположенному на пьезоэлектрической подложке из ниобата лития или танталата лития (рис. 14.5).

На подложке в точно рассчитанных местах расположены отдельные электроды, действующие как рефлекторы, изготовленные из алюминия или вытравленные на подложке. Антенна после приема радиочастотного сигнала от SAW-ридера подает электрический импульс на IDT. Этот импульс генерирует поверхностные волны, также называемые волнами Рэлея, и эти волны обычно проходят по подложке со скоростью от 3000 до 4000 м/с. Часть этих волн отражается рефлекторами обратно в IDT, а остальная часть поглощается подложкой. Отраженные волны образуют уникальную структуру, определяемую позициями рефлекторов и представляющую собой данные метки. Эти волны преобразуются в IDT обратно в радиосигнал и передаются через антенну метки назад RFID-ридеру. Затем ридер декодирует принятый сигнал и извлекает данные метки.

Рис. 14.5. Конструкция SAW-метки

Основные технические характеристики системы радиочастотной идентификации на SAW-радиометках приведены в таблице 14.2.

Таблица 14.2

Характеристики системы RFID на SAW-радиометках

Характеристика	Значение
Диапазон рабочих частот, ГГц	2,4 - 2,483
Средняя мощность на выходе считывателя, мВт	не более100
Вероятность ошибочного считывания или пропуска	10^{-5}
Количество кодов радиометок, шт.	10^7-10^9
Рабочая температура считывателя, °С	-40 .... +50
Рабочая температура радиометки, °С	-55 ... +150
Дальность считывания, м	6 - 8

SAW-метка имеет следующие преимущества:

- очень малое потребление энергии, так как ей не нужен источник постоянного тока для своего питания;
- с ее помощью можно с хорошими результатами отмечать радионепрозрачные и радиопоглощающие материалы, например, металл и воду соответственно;
- большее расстояние чтения, чем у метки с микрочипом, работающей в том же частотном диапазоне;
- может работать с более короткими пачками радиосигналов в отличие от меток на микрочипах, требующих более продолжительного сигнала от ридера к метке;
- высокая степень точности чтения данных с метки;
- большая прочность вследствие простоты конструкции;
- не требует применения антиколлизионных протоколов;
- антиколлизионные протоколы необходимо реализовывать только на уровне ридера в отличие от меток с микрочипами, для которых такие протоколы нужны как на уровне ридера, так и на уровне метки (это снижает стоимость SAW-метки);
- SAW-ридеры менее подвержены влиянию помех от других SAW-ридеров.

SAW-метки могут, скорее всего, оказаться единственным вариантом в определенных

ситуациях нанесения меток, и вероятно получат широкое распространение в будущем.

Рабочая частота метки - одна из самых важных характеристик соединения метки и считывателя. Значение используемой частоты зависит от приложений и мировых стандартов. Частоты определяют скорость передачи данных между меткой и считывателем. Чем ниже частота связи, тем меньше скорость. Однако здесь также огромную роль оказывает окружающая среда и тот объект, на котором размещается метка.

В RFID метках используется следующие диапазоны частот:

1. *Низкие частоты (НЧ) LF (Low Frequency)* - до 135 кГц. Регулирующий стандарт - ISO/IEC 18000-2. Такие метки лучше других работают вблизи жидкостей и металлов, из-за чего этот стандарт стал особенно популярным в области опознавания животных. НЧ метки могут считываться с расстояния в несколько сантиметров и имеют самую низкую скорость передачи данных. Пассивные метки данного диапазона имеют низкие цены, однако в связи с большой длиной волны существуют проблемы со считыванием на большие расстояния, а также проблемы, связанные с появлением коллизий при считывании.

2. *Высокая частота (ВЧ) HF (High Frequency)* - 13,56 МГц. Регулирующий стандарт - ISO/IEC 18000-3. Метки 13 МГц дешевые, не имеют экологических и лицензионных проблем, хорошо стандартизованы, имеют широкую линейку решений, в них используются стандартизованные алгоритмы шифрования. Широко применяются в таких областях, как карты контроля доступа, платежные карты, борьба с подделкой товаров, отслеживание книг и т.д. ВЧ метки могут считываться на расстоянии до 1м. Как и для диапазона LF, в системах, построенных в HF-диапазоне, существуют проблемы со считыванием на большие расстояния, считывание в условиях высокой влажности, при наличии металла, а также проблемы, связанные с появлением коллизий при считывании.

3. *Сверхвысокая частота UHF (Ultra High Frequency)* - 433 МГц. Регулирующий стандарт - ISO/IEC 18000-7. Метки данной частоты обладают наибольшей дальностью регистрации, во

многих стандартах данного диапазона присутствуют антиколлизионные механизмы. В UHF RFID-системах по сравнению с LF и HF ниже стоимость меток, при этом выше стоимость прочего оборудования. Активные метки (радиометками с элементами питания) обеспечивают максимальную дальность считывания (до 1 км) и надежность считывания (100%). Основным минусом данных систем является стоимость меток, на порядок превышающая стоимость пассивных UHF меток.

5. *Сверхвысокие частоты (СВЧ) UHF (Ultra High Frequency)* - диапазон 860-930 МГц. Регулирующий стандарт - ISO/IEC 18000-6. Самый популярный диапазон в современных RFID системах. UHF метки могут считываться на расстоянии до 10 метров, и обеспечивают скорость передачи данных более 128 кбит/сек. Данный стандарт стал основным в таких областях, как логистика и управление цепочками поставок, благодаря усилиям мировых лидеров в этой области (Walmart, Metro Group, Департамент обороны США и др.). В настоящее время частотный диапазон СВЧ открыт для свободного использования в так называемом «европейском» диапазоне - 863-868 МГц.

6. *Микроволновые частоты SHF (Super High Frequency)* - 2,45-5,8 ГГц. Регулирующий стандарт - ISO/IEC 18000-3. Используются в таких областях, как промышленная автоматизация, электронный сбор платежей и контроль доступа. Имеют диапазон считывания, сопоставимый с UHF (СВЧ), и более высокие скорости передачи данных. Используемые метки являются в основном активными или полуактивными, что ограничивает области их применения.

Имеются также СВЧ метки UHF *ближнего поля (Near-Field)*, которые, не являясь непосредственно радиометками, а используя магнитное поле антенны, позволяют решить проблему считывания в условиях высокой влажности, присутствия воды и металла. С помощью данной технологии ожидается начало массового применения RFID-меток в розничной торговле фармацевтическими товарами (нуждающимися в контроле подлинности, учёте, но при этом зачастую содержащими воду и металлические детали в упаковке) и в других областях.

В мире в основном используют HF и UHF частоты, поэтому в таблице 14.3 приведены различия между этими типами меток.

Характеристики и области применения HF и UHF меток

Таблица 14.3

Частоты	Основные характеристики	Область применения
HF 13,56 МГц (высокая частота)	Соответствие общемировым стандартам Размер метки больше, чем UHF Дистанция считывания 1,2 м Низкая погрешность при чтении защитных ворот Цена меток выше, чем UHF Вблизи металлов работают недостаточно эффективно	Платежные карты и карты лояльности (смарт-карты) Контроль доступа Борьба с подделкой Различные решения для поштучного отслеживания книг, багажа, одежды и т.д. "Умные полки" Опознавание людей и
UHF 860-930 МГц (сверхвысокие частоты)	Несовместимы из-за различия существующих региональных правил и нормативов Размер метки меньше, чем у HF Имеют больший, чем у HF-метки, диапазон считывания (более 3 м) Цена меток ниже, чем HF Получают развитие благодаря усилиям участников розничных цепочек поставок товаров Чувствительность к жидкостям и	Логистика и цепочки поставок, включая: Управление запасами Складской менеджмент Отслеживание активов

Считывающие устройства RFID

Для извлечения данных, хранящихся на RFID-метке, используется считывающее устройство - ридер (англ., *reader).* Типичный ридер имеет одну или несколько антенн, которые излучают радиоволны и принимают сигналы от метки (рис. 14.6). Далее полученная информация (идентификационный номер метки, ID считывающего устройства и время, когда метка была

прочитана) в цифровом виде передается в компь
для дальнейшей обработки. Следует учитывать, что считыватели
должны работать на той частоте, для которой предназначены
метки.

Функции, выполняемые RFID-считывателем:

1. Энергоснабжение пассивных меток за счет передачи энергии меткам с использованием электромагнитного поля.
2. Чтение данных, которые хранятся на метке.
3. Запись данных на метку - используя метки с возможностью чтения-записи, данные можно менять, добавлять новые и удалять старые, в любое время на протяжении всего жизненного цикла продукта.
4. Связь с компьютерной системой - считыватель отвечает за транспортировку информации между метками и компьютерной системой, это происходит посредством порта Bluetooth, сети Ethernet или других проводных или беспроводных технологий.

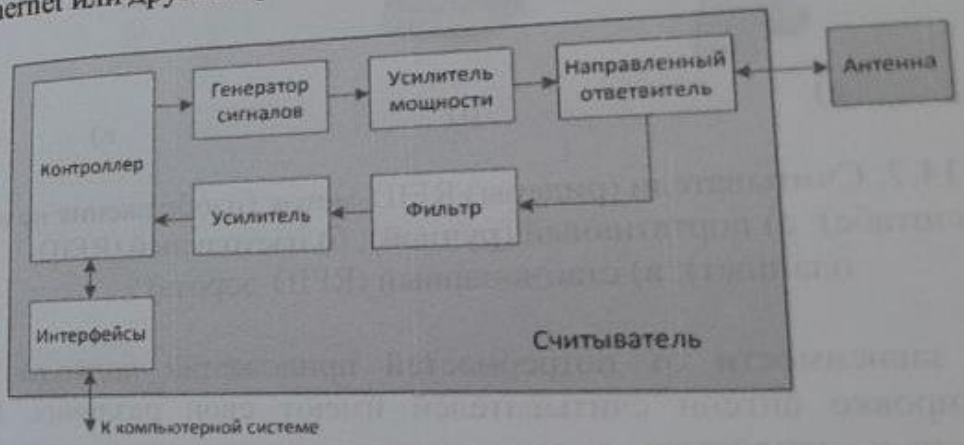


Рис.14.6. Структурная схема RFID-считывателя

Конструктивно считыватели бывают ручные, настольные стационарные (рис. 14.7). Каждый из них используется зависимости от необходимых потребностей. Ручные считывате применяются для поиска нужных товаров и применяются складах, в библиотеках, в розничных магазинах и Стационарные считыватели используются как для считывания, и для программирования RFID меток. С помощью них мо

стереть, перезаписать информацию с метки. В основном они используется в библиотеках, на складах.

Метку и считыватель соединяет радиоканал связи для передачи данных, который организуется с использованием антенн. Очевидно, что дальность действия системы RFID зависит от размеров антенн, имеющихся у меток и считывателей. Антенны могут быть двух видов: вмонтированные в метку и корпусированные. В первом случае антенна RFID-метки монтируется на ту же поверхность, что и микрочип и помещается с ней в один корпус. Размеры корпуса метки обычно определяется размером и формой антенны. Сам микрочип метки же может быть крайне мал.

а) б) в)

Рис. 14.7. Считыватели (ридеры) RFID-меток (изображения не в масштабе): а) портативный (ручной); б) настольный (RFID-планшет); в) стационарный (RFID-ворота)

В зависимости от потребностей приложений подходы к корпусировке антенн считывателей имеют свои различия. В переносных устройствах, антенна крепится на сам считыватель, в других, размещается на расстоянии от него. Здесь может быть смонтировано сразу несколько антенн (так называемые RFID-ворота, рис. 14.7в), которые расположен таким образом, что позволяет повысить качество считывания и дальность сигналов радиоволн.

14.3. Стандартизация технологии RFID

В настоящее время не существует единых международных стандартов в технологии RFID. Далее представлен краткий обзор важнейших из них.

Международная организация по стандартизации ISO (International Organization for Standardization) совместно с Международным инженерным консорциумом IEC (International Electrotechnical Commission) разработала серию RFID-стандартов ISO/IEC 18000 для автоматической идентификации и контроля предметов снабжения. Эта серия охватывает протокол радиоинтерфейса для систем, используемых в системах поставок, и включает 7 основных радиочастот RFID-технологии со всего мира.

ISO разработала также международные стандарты, которые регулируют радиочастотную идентификацию животных, которая обычно осуществляется имплантацией транспондера (микрочипа) под кожу животного. Так ISO/IEC 11784 определяет, каким образом данные записаны на метку, а ISO/IEC 11785 устанавливает протокол радиоинтерфейса. Кроме этого ISO создала стандарт протокола для RFID-меток, используемых в платежных системах и бесконтактных смарт-картах (ISO/IEC 14443) и картах дальнего действия (ISO/IEC 15693). Организация также установила стандарты для тестирования RFID-меток и считывателей на соответствия техническим требованиям (ISO/IEC 18047) и на требования к проведению испытаний технических характеристик устройств (ISO/IEC 18046).

Центр Auto-ID, который был создан для разработки *электронного кода продукта EPC* (*Electronic Product Code*), предложил свой собственный протокол радиоинтерфейса (отличный от стандарта ISO) для отслеживания товаров в международной логистической цепи. Первоначально Центр планировал создать единый протокол, который бы мог связываться с различными типами (классами) меток. Каждый последующий тип меток должен быть более сложным, чем предыдущий:

характеристик радиоидентификационных систем;

- сложности в снижении цены RFID-метки.

Наиболее востребованной технология RFID оказалась в сфере государственных проектов, розничной торговле, логистике и на транспорте. Помимо перечисленных направлений, ежегодно производители и интеграторы готовых решений выводят на рынок все больше идей по использованию RFID, что, несомненно, расширяет сферы применения этой технологии.

В целом, несмотря на сильную переоценку RFID-рынка в прошлом, следует отметить его сегодняшнее постепенное развитие. В настоящее время применение RFID-систем активно продвигается в тех отраслях, где-либо отсутствует возможность идентификации с помощью других технологий, либо же их применение экономически не оправдано. Таким образом, массовое внедрение RFID-технологий - это реальность, но далеко не всех сфер экономики.

14.4. Области применения RFID-технологий

Радиочастотная идентификация относится к ключевым технологиям будущего и является базовой технологий в Интернете вещей. Рассмотрим характерные примеры применения RFID в различных областях человеческой деятельности.

Промышленность и сельское хозяйство

Технология RFID обеспечивает улучшенное управление складскими запасами и позволяет значительно повысить эффективность логистических процессов в промышленности. Например, промышленные компании используют RFID-систему для контроля над важными комплектующими, перемещающимися от одного цеха к другому, что обеспечивает автоматический контроль, уменьшение количества ошибок и затрат на поиск необходимых деталей на производственной линии.

Реализованы проекты автоматизации заправки автотранспортных средств и автоматической идентификации автотранспорта с использованием технологии RFID. Система обеспечивает прозрачный и достоверный учет топлива при проведении всех технологических и документарных операций,

эффективное планирование и контроль потребления моторного топлива по каждой единице автотехники, безоператорный отпуск топлива только авторизованным автомашинам при помощи RFID-меток без использования бумажных носителей и смарт-карт.

Чтобы защитить свою продукцию от подделок, фармацевтические предприятия помещают транспондеры на упаковках медикаментов. Благодаря этому удается отслеживать путь препаратов от изготовителя до аптеки.

Во многих странах фермеры маркируют крупный рогатый скот посредством помещения транспондеров на ухо животного. Таким образом, при внезапной вспышке болезни или эпидемии стадо становится возможным быстро изолировать.

Государственные и общественные учреждения

Некоторые библиотеки внедрили RFID в свои системы книгообмена. При этом в книгах, на пленках и на компакт-дисках размещаются транспондеры. В результате посетители могут самостоятельно оперативно получать выбранные ими носители информации, причем благодаря транспондерам эти носители надежно защищены от кражи. Использование RFID-меток позволяет автоматизировать процесс выдачи и возврата носителей, более эффективно проводить инвентаризацию и защитить фонд от краж. Кроме того, читательские билеты также можно оснастить RFID-метками, что позволит бороться с их подменами и подделками.

Больницы также используют радиочастотную идентификацию для того, чтобы облегчить идентификацию пациентов и оптимизировать их размещение в палатах. Пациенты снабжаются ручными браслетами с интегрированными в них транспондерами, в которых закодированы имя пациента и номер истории его болезни, хранящейся в электронной базе данных. Посредством мобильного компьютера со считывающим устройством лечащий врач получает оперативный доступ к историям болезни своих пациентов.

В музеях посетители могут при помощи персонального цифрового помощника PDA (Personal Digital Assistant) запрашивать информацию о выставочных экспонатах, для чего экспонаты снабжаются транспондерами RFID. При этом

Класс 1: простая, пассивная метка обратного рассеяния, доступная только для считывания, с программируемой долговременной памятью однократного использования.

Класс 2: пассивная метка обратного рассеяния с объемом памяти 65 Кбит, которую можно считывать и перезаписывать.

Класс 3: полупассивная метка обратного рассеяния с объемом памяти 65 Кбит, которую можно считывать и перезаписывать; фактически это Класс 2 со встроенной батареей для поддержания расширенной зоны действия считывателей.

Класс 4: активная метка со встроенной батареей для управления схемой микрочипа и снабжения радиопередатчика электроэнергией, чтобы излучать сигнал считывателю.

Класс 5: активная RFID-метка, которая может связываться с другими метками Класса 5 и/или другими устройствами.

Позже типы меток изменились и со временем Центр Auto-ID утвердил также метки Класса 0, доступные только для чтения и программируемые в момент сборки. Метка Класса 0 использовала отличный от Класса 1 протокол, а это означало, что потребителям приходилось покупать многопротокольные считыватели, чтобы иметь возможность считывать метки и Класса 1, и Класса 0.

Протоколы Класса 0 и Класса 1 имеют пару недостатков, включая тот факт, что они не могут взаимодействовать друг с другом. Одна из проблем заключается в том, что они несовместимы со стандартами ISO. Другая проблема - невозможность применения повсеместно. К примеру, Класс 0 излучает сигнал на одной частоте и принимает обратный уже на другой, но в СВЧ диапазоне, что запрещено в Европе.

С 2003 года после закрытия центра Auto ID Labs разработкой стандартов в области сверхвысоких частот UHF занимается организация EPCglobal Inc., целью которой является установление всемирных стандартов для разработки, реализации и принятия электронного кода продукта EPC и создание сети EPCglobal. Спецификация EPCglobal, нацеленная на операции в сетях сбыта, является наиболее глобальной спецификацией для RFID и применяется в очень широком наборе прикладных систем. Существует два поколения стандартов EPC. Первое поколение определяло только метки класса 0 и класса 1. Метки класса 0 программировались во время изготовления «R/O». В метки класса

1 информация могла быть записана только один раз пользователем, при создании метки для конкретного приложения «WORM». Класс 0 и класс 1 имеют различные протоколы для работы со считывателем.

Существуют модификации классов, которые поддерживаются «открытыми» стандартами EPC Global. Наиболее широко используемые модификации это класс 0 g1, который отличается размером памяти (96 бит вместо принятых изначально 64 бита) и класс 1b (dbg2), где всего 128 бит, 96 бит из которых (EPC-код) доступны для многократной перезаписи.

Для устранения проблем, возникающих при работе с метками первого поколения, в 2004 году EPC Global введен стандарт второго поколения для транспондеров, работающих в области ультравысоких частот, именуемый EPC Generation 2 - общий протокол обмена данными для всех продуктов второго поколения. Протокол разработан для меток Класса 1 gen2, но должен подходить для работы с разрабатываемыми в перспективе классами (планируется создание меток класса 2, 3, 4 и 5).

Современное состояние и перспективы развития технологии RFID

Технологию радиочастотной идентификации вооруженные силы стали применять в середине XX века, а отправной точкой ее активного внедрения для гражданских нужд считают 1990-е годы, когда Международная организация по стандартизации (ISO) приняла ряд основополагающих стандартов в области RFID. В начале XXI века технология радиочастотной идентификации стала активно внедряться на практике, например компания Walmart и Министерство вооруженных сил США обязывали своих поставщиков использовать RFID для маркировки поставляемой им продукции. Прогнозировалось, что производство RFID-систем в скором времени выйдет на промышленные масштабы и технология начнет применяться повсеместно. Но к 2005 году темпы развития RFID- технологии несколько замедлились, и интерес к ее использованию снизился.

Основными причинами этого принято считать:

- появление ряда научных исследований, заверяющих о небезопасности использования радиометок;
- сложность изменения некоторых технических

характеристик
радиоидентификационных систем;
- сложности в снижении цены RFID-метки.

Наиболее востребованной технология RFID оказалась в сфере государственных проектов, розничной торговле, логистике и на транспорте. Помимо перечисленных направлений, ежегодно производители и интеграторы готовых решений выводят на рынок все больше идей по использованию RFID, что, несомненно, расширяет сферы применения этой технологии.

В целом, несмотря на сильную переоценку RFID-рынка в прошлом, следует отметить его сегодняшнее постепенное развитие. В настоящее время применение RFID-систем активно продвигается в тех отраслях, где-либо отсутствует возможность идентификации с помощью других технологий, либо же их применение экономически не оправдано. Таким образом, массовое внедрение RFID-технологий - это реальность, но далеко не всех сфер экономики.

14.4. Области применения RFID-технологий

Радиочастотная идентификация относится к ключевым технологиям будущего и является базовой технологий в Интернете вещей. Рассмотрим характерные примеры применения RFID в различных областях человеческой деятельности.

Промышленность и сельское хозяйство

Технология RFID обеспечивает улучшенное управление складскими запасами и позволяет значительно повысить эффективность логистических процессов в промышленности. Например, промышленные компании используют RFID-систему для контроля над важными комплектующими, перемещающимися от одного цеха к другому, что обеспечивает автоматический контроль, уменьшение количества ошибок и затрат на поиск необходимых деталей на производственной линии.

Реализованы проекты автоматизации заправки автотранспортных средств и автоматической идентификации автотранспорта с использованием технологии RFID. Система обеспечивает прозрачный и достоверный учет топлива при проведении всех технологических и документарных операций,

эффективное планирование и контроль потребления моторного топлива по каждой единице автотехники, безоператорный отпуск топлива только авторизованным автомашинам при помощи RFID-меток без использования бумажных носителей и смарт-карт.

Чтобы защитить свою продукцию от подделок, фармацевтические предприятия помещают транспондеры на упаковках медикаментов. Благодаря этому удается отслеживать путь препаратов от изготовителя до аптеки.

Во многих странах фермеры маркируют крупный рогатый скот посредством помещения транспондеров на ухо животного. Таким образом, при внезапной вспышке болезни или эпидемии стадо становится возможным быстро изолировать.

Государственные и общественные учреждения

Некоторые библиотеки внедрили RFID в свои системы книгообмена. При этом в книгах, на пленках и на компакт-дисках размещаются транспондеры. В результате посетители могут самостоятельно оперативно получать выбранные ими носители информации, причем благодаря транспондерам эти носители надежно защищены от кражи. Использование RFID-меток позволяет автоматизировать процесс выдачи и возврата носителей, более эффективно проводить инвентаризацию и защитить фонд от краж. Кроме того, читательские билеты также можно оснастить RFID-метками, что позволит бороться с их подменами и подделками.

Больницы также используют радиочастотную идентификацию для того, чтобы облегчить идентификацию пациентов и оптимизировать их размещение в палатах. Пациенты снабжаются ручными браслетами с интегрированными в них транспондерами, в которых закодированы имя пациента и номер истории его болезни, хранящейся в электронной базе данных. Посредством мобильного компьютера со считывающим устройством лечащий врач получает оперативный доступ к историям болезни своих пациентов.

В музеях посетители могут при помощи персонального цифрового помощника PDA (Personal Digital Assistant) запрашивать информацию о выставочных экспонатах, для чего экспонаты снабжаются транспондерами RFID. При этом

сотрудники музеев получают информацию о том, какими экспонатами интересуются особенно часто.

Наука

Исследователи прослеживали с помощью технологии RFID жизнь пчел. Крошечные чипы приклеивались на спинки насекомых. Полученная при этом информация о деятельности пчел, помимо прочего, помогает эффективнее бороться с болезнями.

Ученые с помощью технологии RFID наблюдали рост генетически измененных деревьев. Эта система заметно превосходила все прежние методы маркировки, поскольку транспондер, помещенный внутрь дерева, защищен от воздействия окружающей среды.

Быт и досуг

Потребители уже сегодня практически ежедневно сталкиваются с системами RFID. Например, во многих странах транспондеры интегрируются в заграничные паспорта, а в некоторых клубах — в членские карточки.

Технология RFID уже долго и успешно используется как электронный ключ для управления доступом в помещения. Преимущество RFID-карты по сравнению с магнитной картой в том, что нет никакого контакта между картой и считывателем, она меньше изнашивается, меньше дополнительного обслуживания.

RFID технология также завоевывает популярность как удобный способ оплаты различных услуг. Один из популярных способов - оплата дорожных пошлин без остановки автомобиля. RFID также начинает использоваться как удобный способ оплаты проезда в автобусах, метро и поездах. Многие города в мире перешли от карт с магнитной полосой к RFID-картам, так как это позволяет людям быстрее проходить через турникеты, уменьшает скопление и ускоряет обслуживание в кассах.

В некоторых парках отдыха посетители могут с помощью RFID поддерживать связь друг с другом. Считывающие приборы регистрируют браслет с интегрированным транспондером и указывают местоположение пользователя на стационарно расположенных экранах. Посредством этих сенсорных экранов посетители могут посылать и принимать сообщения.

RFID также используется для охраны собственности. Большинство современных автомобилей идет в комплекте со считывающим RFID-устройством в рулевой колонке. Ретранслятор вставлен в пластмассу вокруг основы ключа. Ридер должен получить удостоверение личности от ключа или автомобиль не будет заводиться.

Активные RFID-метки могут быть объединены с датчиками тревоги: например, если оружие на объектах переносится без разрешения - раздается сигнал тревоги. RFID-метки могут быть в компьютерах с ценной информацией: так файл не будет удалён без удостоверения личности и проверки прав доступа.

Приведенные примеры далеко не исчерпывают перечень основных приложений, в которых применение бесконтактной идентификации не только удобно, но и экономически оправдано.

Контрольные вопросы

1. Назначение системы радиочастотной идентификации (RFID)?
2. Какие элементы входят в состав RFID-системы?
3. В чём отличие систем идентификации RFID и штрих-кода.
4. Как устроена RFID-метка? Какие метки бывают?
5. В чем особенность RFID-меток, работающих на принципе поверхностной акустической волны ПАВ?
6. Какие частотные диапазоны используются в RFID-метках?
7. Поясните функции и устройство считывающих устройств RFID-систем.
8. Каково состояние стандартизации технологии RFID?
9. Какие проблемы мешают более массовому внедрению технологии RFID?
10. Приведите примеры применений технологии RFID в различных областях деятельности.

Глава 15. ПЕРСПЕКТИВЫ ДАЛЬНЕЙШЕГО РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ И БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

15.1. Рост интеллектуальных сенсорных технологий Интернета вещей

Датчики, используемые для измерения физических характеристик или контроля за использованием устройств, восходят к истории изобретения микропроцессоров в 1960-х годах. Однако считается, что первое в мире устройство IoT было изобретено в начале 1980-х годов в Университете Карнеги-Меллона. Он использовал реконнекторы, установленные на подключенном торговом автомате Coca-ColaC, чтобы указать, сколько в нем коробок колы.

Зародившись как малоиспользуемая технология, сегодня она широко используется в автомобилях и бытовой технике, что позволяет ей играть важную роль в жизни многих людей. Датчики IoT также начали использовать в офисных зданиях, а пандемия COVID-19 стала поворотным моментом в их использовании, и с введением политик гибридной производительности компании продолжат расширять эту технологию.

В то время как разнообразие типов датчиков и видов использования, а также спрос на них увеличиваются, стоимость и сложность установки в большинстве случаев снижаются. Это снимает значительную нагрузку с разработчиков, которые теперь могут сосредоточиться на программном обеспечении, не беспокоясь о подключении.

Мировой рынок датчиков IoT оценивался в 9,6 млрд долларов в 2018 году и, как ожидается, достигнет 34,4 млрд долларов в 2024 году.

15.2. Будущее сенсорной технологии IoT

Существует еще много возможностей для развития сенсорной технологии IoT и дальнейшей модификации многих областей в ближайшие годы. Поскольку гибридная модель

производительности продолжает распространяться среди предприятий, ее использование может позволить сотрудникам, которые не предпочитают работать в помещениях компании, выполнять задачи удаленно. Кроме того, с развитием умных городов датчики IoT также становятся важной частью жизни горожан [3].

По мере того, как продолжается работа по созданию национальной инфраструктуры, включающей датчики IoT по всему миру, предприятия смогут извлечь выгоду из расширения возможностей подключения и снижения затрат, а также сокращения выбросов углерода для достижения национальных и глобальных целей в области устойчивого развития.

Внедрение технологий 5G также обещает стимулировать развитие пространства IoT, поскольку все больше и больше устройств становятся более гибкими благодаря новым беспроводным технологиям. Однако это не означает, что технологии LPWAN теряют свою актуальность - организации по-прежнему находят ценное применение небольшим объемам данных, которыми легче управлять и передавать между устройствами. Также необходимо учитывать стремительное развитие таких стандартов, как LTE-M и NB-IoT [28].

Устройства с датчиками IoT более разнообразны, компактны и портативны, а альтернативным носителем может стать технология нанороботов. Это, например, приносит пользу здравоохранению, позволяя специалистам быстрее диагностировать и лечить травмы и заболевания благодаря повышению удобства использования. По оценкам, к 2025 году мировой рынок нанороботов превысит 8,6 млрд долларов.

15.3. Потребности и перспективы в области стандартизации

Сети БСС и IoT не являются цельной технологией, а представляют собой сложные системы, использующие различные технологии от уровней физической связи до прикладных программ. Кроме того, они используются во многих областях и в разных средах. Последствием этих факторов является сложная среда стандартизации [14].

На сегодняшний день уже существует большой набор действующих стандартов и проводится ряд мероприятий по стандартизации. Однако, они охватывают только определенные аспекты и области применения системы в общем или основное внимание уделяют конкретным сценариям использования.

Интернет вещей и БСС являются базовыми технологиями для существующих и будущих областей стандартизации МЭК, таких как умная электросеть, промышленность 4.0 и умные города. Следовательно, важно, чтобы МЭК имела глубокое понимание их сути, среды стандартизации и специфические потребности практических областей МЭК с целью обеспечения стандартизации в нужном направлении, а также выявления и заполнения пробелов стандартизации. Это необходимо делать в тесном сотрудничестве с другими органами по стандартизации.

Начиная со сценариев использования конкретных областей применения (т.е. умной электросети, промышленности 4.0, умных городов) необходимо определить требования и структуру архитектуры, соответствующую потребностям МЭК. Это позволит определить перечень существующих стандартов, которые могут быть использованы в дальнейшем, а также ряд пробелов, которые необходимо устранить.

Сети БСС – это новая технология, которая охватывает различные уровни и аспекты информационных технологий. Поэтому стандартизация этого типа сетей имеет свою уникальную сложность:

- Разобщенность: связь, координация и единое планирование отсутствуют в разных организациях по стандартизации и между ними.

- Несовместимость: БСС использует различные аспекты информационных технологий, следовательно, ее стандарты имеют сложную структуру и разнообразны по своей природе. Тем не менее, разные стандарты, разработанные различными организациями по стандартизации, являются несовместимыми.

- Отсутствие гармонизации: на сегодняшний день некоторые прикладные области БСС были уже реализованы. Несмотря на то, что различные организации по стандартизации проводили работы по стандартизации с разных точек зрения и с разной глубиной,

большая часть такой работы находится на начальном этапе и не готова к применению на рынке.

- Противоречивость: поскольку приложения не прошли синхронизацию, а стандарты еще не были разработаны, конструкции приложений не соответствуют разработкам в рамках стандартов, что влияет на повторное использование и взаимодействие между приложениями, препятствуя дальнейшей индустриализации.

Для решения вышеуказанных проблем необходимо, чтобы стандартизация БСС улучшала связь и координацию действий между различными организациями по стандартизации, позволяла осуществлять единое планирование, оптимизацию распределения ресурсов и сокращение повторения однотипной работы.

Указанные выше факторы обуславливают их привлекательность в современных и будущих инфраструктурных решениях. IoT и БСС основаны на технологических областях, регулируемых МЭК, например, умная электросеть, промышленность 4.0 и умные города, следовательно, важно, чтобы МЭК имела глубокое понимание их сути, среды стандартизации и специфические потребности заинтересованных сторон МЭК в области БСС.

Для проведения стандартизации в правильном направлении, выявления и заполнения пробелов в стандартах требуется тесное сотрудничество как внутри, так и вне МЭК (т.е. с другими действующими органами по стандартизации).

15.4. Тенденции развития технологий сетевого доступа

В соответствии с текущими требованиями в отношении приложений БСС развитие технологий сетевого доступа достигло значительного прогресса. Наиболее распространенной и используемой технологией представительского доступа является Bluetooth 4.0 с уклоном на использование БСС в медицинских целях, а также IEEE 802.15.4e с уклоном на использование БСС в промышленных целях, а также WLAN IEEE 802.11™ с точки зрения IoT. A.1.1 Bluetooth 4.0 [24].

Bluetooth 4.0

Учитывая характеристики и требования медицинских и некоторых других прикладныхобластей IoT, в частности, требование низкого потребления мощности, Bluetooth SIG опубликовал последнюю редакцию стандарта Bluetooth 4.0 в 2012 году. Ориентированный на компактные устройства с высокой степенью интеграции, Bluetooth 4.0 использует технологию легкого доступа для работы в режиме ожидания с низким энергопотреблением, что обеспечивает чрезвычайно низкое энергопотребление, как в рабочем режиме, так и в режиме ожидания. Даже аккумулятор кнопочного типа может поддерживать бесперебойную работу устройства Bluetooth®4.0 в течение нескольких лет.

В таблице 15.1 представлены параметры Bluetooth 4.0 и традиционной технологии Bluetooth.

Таблица 15.1
Сравнительная характеристика Bluetooth 4.0 с традиционной технологией Bluetooth

Техническая характеристика	Традиционная технология Bluetooth	Bluetooth с низким энергопотреблением
Расстояние/диапазон	100 м (330 футов)	50 м (160 футов)
Скорость передачи данных по воздуху	1 Мбит/с - 3 Мбит/с	1 Мбит/с
Пропускная способность приложения	0,7 Мбит/с – 2,1 Мбит/с	0,27 Мбит/с
Количество активных подчиненных	7	Не определено, зависит от модели
Безопасность	56/128-бит и уровень приложения, определенный пользователем	128-битная AES со счетчиком CBC-MAC и уровень приложения, определенный пользователем
Надежность	Адаптивность к резким скачкам частоты, FEC, быстрый ACK	Пассивное подтверждение приема, 24-битный ЦИК,

		проверка целостности 32-битных сообщений
Задержка (при отсутствии подключения)	Обычно 100 мс	6 мс
Общее время отправки данных (определение срока службы батареи)	100 мс	3 мс, <3 мс
Голосовое управление	Да	Нет
Сетевая топология	Scatternet	Звезда-шина
Потребляемая мощность	1 Вт качестве эталона	от 0,01 до 0,5 Вт (в зависимости от способа использования)
Потребление тока	<30 мА	<15 мА

IEEE 802.15.4e

Характеристики БСС очень похожи на низкоскоростную WPAN, следовательно, большинство БСС принимают IEEE 802.15.4 в качестве основного стандарта связи. Более того, ZigBee®, WirelessHART, ISA100.11a и WIA-PA созданы на базе стандарта IEEE 802.15.4. Поэтому, для достижения высокой надежности, жестких требований функционирования в режиме реального времени использования IoT в промышленности, Рабочая группа IEEE 802.15.4 предложила использовать IEEE 802.15.4e в 2012 году.

Технология IEEE 802.15.4e в основном используется в промышленных целях и расширяет IEEE 802.15.4 при помощи четырех методов доступа, включая неконкурентный метод расширения GTS на базе Beacon (технологии бесперебойной связи). Этот метод поддерживает WIA-PA, ориентированный на автоматизацию производства, неконкурентный метод TDMA, не поддерживающий технологию бесперебойной связи, поддерживающий ориентированный на автоматизацию WirelessHART и ISA100.11a, являющейся сопоставимой технологией доступа на базе Beacon, поддерживающий приложения для автоматизации производства, и метод конкурентного доступа, не поддерживающий технологию

бесперебойной связи, с поддержкой Zigbee® и IEEE 802.15.5 (рис. 15.1).

WLAN IEEE 802.11™

Основными преимуществами WLAN IEEE 802.11™ в контексте IoT являются:

- простая интеграция WLAN-клиентов и устройств с Интернетом;
- его широкое использование в качестве технологии беспроводной связи в домашних хозяйствах, офисах и промышленности;
- ее поддержка мобильными устройствами;
- низкое энергопотребление, приемлемое для промышленных целей и сенсорных сетей.

Беспроводные локальные сети, основанные на стандарте IEEE 802.11™, как правило, используются для беспроводной передачи данных в офисах, на конференциях и встречах, домашних хозяйствах, а также в промышленности. Сети WLAN IEEE 802.11 обеспечивают легкую интеграцию в Интернет при помощи спецификаций с сетевым ориентированием и подобно Ethernet-сетям, а также при помощи их стабильной, коммерчески успешной и широко распространенной экологически безопасной системы. Преобладающими сетевыми топологиями сетей IEEE 802.11™ WLAN являются WLAN-клиенты, подключенные к точкам доступа сети WLAN.

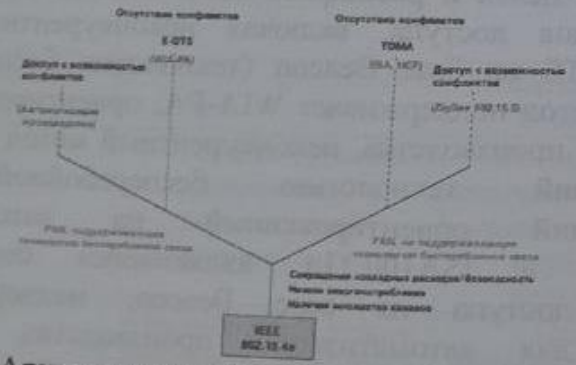


Рис. 15.1. Архитектура технологии сетевого доступа IEEE 802.15.4e

Также возможно использование и других сетевых топологий, в частности, беспроводных многосвязных сетей (IEEE 802.11s). WLAN IEEE 802.11™, обеспечивающая скорость передачи данных 56 Мбит/с при использовании IEEE 802.11a/g, 150 Мбит / с и более при использовании IEEE 802.11n, и до 1 Гбит/с при использовании IEEE 802.11ac. Кроме того, WLAN также внедряются в беспроводную связь промышленного сектора и сенсорные сети. Такие компании, как GainSpan, предлагают так называемые маломощные Wi-Fi-клиенты (рис. 15.2).

Низкое энергопотребление достигается при помощи энергоэффективного оборудования и последующего использования возможностей энергосбережения спецификации IEEE 802.11™. Wi-Fi Alliance планирует осуществить сертификацию этой технологии.

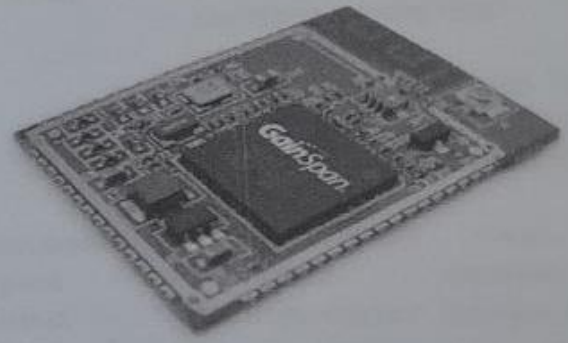


Рис. 15.2. Маломощный Wi-Fi модуль GainSpan GS1011M

Контрольные вопросы

1. Роль сенсорной технологии IoT в контексте карантинных ограничений COVID-19?
2. Расскажите о росте интеллектуальных сенсорных технологий Интернета вещей.
3. Какие возможности для развития сенсорной технологии IoT.
4. Потребности и перспективы в области стандартизации сенсорных технологий IoT.

5. Какие проблемы существуют для БСС в соответствии потребностями МКЭ.

6. Какие направления будет развиваться с развитием технологий сетевого доступа.

7. Приведите параметры технологии Bluetooth 4.0.

8. Расскажите о развитии технологии IEEE802.15.4e.

9. Дайте и объясните архитектуру технологии сетевого соединения IEEE 802.15.4e.

10. Каковы основные преимущества технологий WLAN IEEE 802.11™ в контексте IoT?

СПИСОК ТЕРМИНОВ

Интернет вещей **uz** – Buyumlar interneti **en** – Internet of things	Объединение уникально идентифицируемых встроенных вычислительных устройств в рамках развернутой интернет инфраструктуры Qurilgan internet infratuzilma doirasida noyob identifikatsiyalanadigan o‘rnatilgan hisoblash qurilmalarini birlashtirish
Система на чипе **uz** – kristalldagi tizim **en** - system on a chip	Интегральная схема (ИС), которая объединяет все компоненты компьютера или другой электронной системы в один чип Kompyuterning barcha komponentlari yoki boshqa elektron tizimni bitta mikrosxemaga birlashtiradigan integral sxema (IS)
Уровень управления доступом к среде передачи данных **uz** - ma’lumotlarni uzatish muhitiga ulanishni boshqarish qatlami **en** - media Access Control Layer	MAC-уровень часть протокола передачи данных, которая контролирует доступ к физической среде передачи в сетях IEEE 802 (LAN) MAC-qatlam – IEEE 802 (LAN) tarmoqlarida fizik uzatish muhitiga ulanishni nazorat qiladigan ma’lumotlarni uzatish protokolining qismi
Синхронизованный временной mesh-протокол **uz** - sinxronlashtirilgan vaqt mesh-protokoli	Сетевой протокол, являющийся центральным элементом беспроводной сенсорной сети с низким энергопотреблением.

en - synchronized Time mesh-Protocol

Беспроводная локальная сеть (WLAN)
uz - simsiz lokal tarmoq
en - wireless LAN

Past energiya iste'molili simsiz sensorlar tarmog'ining markaziy elementi bo'lgan tarmoq protokoli
Локальная сеть, в которой данные передаются без использования проводов

Ma'lumotlar simlardan foydalanmasdan uzatiladigan lokal tarmoq
Другое название – беспроводной абонентский доступ (WLL). В основу WMAN положен стандарт IEEE 802.16. Эффективная скорость беспроводного абонентского доступа составляет от 1 до 10 Мбит /секунду на удалении от 4 до 10 километров

Беспроводная городская сеть (WMAN)
uz - simsiz shahar tarmog'i
en - wireless metropolitan area network

Boshqa nomi – simsiz abonentlar ulanishi (WLL). WMAN asosiga IEEE 802.16 standarti qo'yilgan. Simsiz abonentlar ulanishining samarali tezligi 4 dan 10 kilometrlargacha masofalarda 1 dan 10 Mbit /sekundgachani tashkil etadi
Беспроводная сеть малого радиуса действия, которая занимает площадь всего несколько десятков метров

Беспроводная персональная сеть (WPAN)
uz - simsiz personal tarmoq
en - wireless Personal Area Network

Atigi bir necha o'nlab metrlardagi maydonni egallaydigan kichik ishlash radiusili simsiz tarmoq
Самоорганизующиеся сети с множеством переходов беспроводных сенсорных узлов, используемых для мониторинга и управления физическими явлениями

Беспроводная сенсорная сеть (WSN)
uz - simsiz sensorlar tarmog'i

en - wireless sensor network

Fizik hodisalarni monitoring qilish va boshqarish uchun ishlatiladigan simsiz sensorli tugunlarning ko'plab o'tishlariga ega bo'lgan o'z-o'zidan tashkil etiladigan tarmoq
Беспроводная сеть, обеспечивающая коммуникационные услуги в пределах географической области большей, чем территория одного города. Этот вид сетей является наиболее распространенным из всех беспроводных сетей

Беспроводная глобальная сеть (WWAN)
uz -simsiz global tarmoq
en - wireless wide area network

Bitta shahardan kattaroq geografik hududda aloqa xizmatlarini ko'rsatadigan simsiz tarmoq. Bu turdagi tarmoq barcha simsiz tarmoqlarning eng keng tarqalgani hisiblanadi

Приемопередатчик
uz - qabul qilgich-uzatkich
en - transceiver

Устройство, которое как передает, так и получает информацию; размещается в радиоплате интерфейса сети

Axborotni ham uzatadigan, ham qabul qiladigan qurilma; tarmoq interfeysining radioplatasida joylashtiriladi

Радиосигнал
uz - radiosignal
en - RF signal

Сигнал, частота которого соответствует диапазону радиоволн, используется для передачи информации через воздушную среду

Chastotasi radioto'lqinlar diapazoniga mos keladigan signal. Havo muhiti orqali axborot uzatish uchun foydalaniladi

Фазовая манипуляция (PSK)
uz - fazaviy manipulyasiya
en - phase shift keying

Процесс модуляции, при котором для представления информации используются небольшие изменения фазы несущей, в результате чего возможна передача данных через радиоэфир

Частотная манипуляция (FSK)
uz - chastotaviy manipulyasiya
en - frequency shift keying

Modulyasiya jarayoni bo‘lib, axborotni taqdim etish uchun eltuvchi fazasi sal o‘zgartiriladi, natijada ma’lumotlarni radioefir orqali uzatish mumkin bo‘ladi
Метод модуляции, при котором слегка изменяется частота несущего сигнала, за счет чего осуществляется представление информации способом, подходящим для ее передачи через воздушную среду.

Дуплекс; дуплексная передача
uz - dupleks; dupleks uzatish
en - duplex

Modulyasiya metodi, bunda eltuvchi signal chastotasi sal o‘zgartirilishi hisobiga, axborotni havo muhiti orqali uzatish uchun qulay bo‘lgan usulda taqdim etish amalga oshiriladi
Процесс передачи сообщений по каналам связи одновременно в двух направлениях. Данный термин часто употребляется как прилагательное, означающее «дуплексный, одновременно двусторонний». В этом случае он характеризует тип канала связи или режим работы устройства, способного одновременно передавать и принимать информацию.

Aloqa kanallari bo‘ylab xabarlarni bir vaqtning o‘zida ikki yo‘nalishda uzatish jarayoni. Bu atama «dupleks,

bir vaqtning o‘zida ikki tomonlama» ma’nosida ishlatiladi. Bunda u bir vaqtning o‘zida ham uzatish, ham qabul qilish qobiliyatiga ega bo‘lgan kanal turi yoki qurilmaning ishlash rejimini tavsiflaydi
Часть системы связи или сквозного соединения, состоящего из нескольких последовательных участков

Звено; тракт
uz - zveno; trakt
en - link

Aloqa tizimining yoki ketma-ketlikdagi bir nechta uchastkadan iborat bo‘lgan, boshdan oxir daxldorlikdagi birikmaning bir qismi
Процесс преобразования исходной информации в кодированную форму

Кодирование
uz - kodlash
en - encoding

Dastlabki axborotni kodlangan shaklga o‘zgartirish jarayoni
Совокупность различных типов наземных средств радиосвязи, спутниковых, кабельных и волоконно-оптических линий, используемых для передачи информации

Передающая среда
uz - uzatuvchi muhit
en - transmission media

Axborotni uzatish uchun foydalaniladigan turli er usti radioaloqa vositalari, yo‘ldoshli, kabelli va optik tolali liniyalar yig‘indisi
Замена одного сигнала другим, получаемым из первого по определенным правилам.

Преобразование
uz - o‘zgartirish
en - transformation

Birinchi signalni undan ma’lum qoidalar bo‘yicha olinadigan boshqa signal bilan almashtirish

прямая видимость
uz - to‘g‘ridan-to‘g‘ri ko‘rinish
en - Line-Of-Sight (LOS)

Наличие геометрической (оптической) видимости между передающей и приемной антеннами. Терм ин также употребляется как прилагательное «в пределах прямой видимости» или «радиорелейный» (о трассе).

Uzatuvchi va qabul qiluvchi antennalar o‘rtasida geometrik (optik) ko‘rinishning mavjudligi. Atama, shuningdek, «to‘g‘ridan-to‘g‘ri ko‘rinish chegarasida» yoki «radioreleli» (trassa haqida) mazmunlarida ham qo‘llaniladi

Радиоканал
uz - radiokanal
en - radio channel

Полоса частот, образующая канал, достаточная для организации информационного обмена между передающим и приемным пунктами. Максимальная ширина полосы канала зависит от вида передаваемой информации, нестабильности частоты, величины доплеровского сдвига, а также частотно-селективных свойств передающей среды

Uzatuvchi va qabul qiluvchi punktlar o‘rtasida axborot almashuvini ta’minlash uchun etarli kanal hosil qiladigan chastotalar polosasi. Kanal polosasining maksimal kengligi uzatiladigan axborot turi, chastota nostabilligi, Doppler siljishi kattaligi, shuningdek, uzatuvchi muhitning chastotaviy-selektiv xossalariga bog‘liq bo‘ladi

Сигнал
uz - signal
en - signal

Изменяющаяся физическая величина, для передачи различных информации, а также оповещения о каких-либо или состояниях объектов событиях

Vaqt bo‘yicha o‘zgaruvchi, turli xildagi axborotlarni uzatish, shuningdek, qandaydir voqea yoki ob’ektlarning holati haqida xabar berish uchun foydalaniladigan fizik kattalik Функция, описывающая зависимость изменения амплитуды и фазы сигнала от частоты и однозначно определяющая его характеристики и свойства. Спектр любого сигнала может быть представлен в виде суммы большого числа гармонических колебаний с различными частотами, амплитудами и фазами. Такое разложение на гармонические составляющие называется спектральным разложением, а его свойства могут быть описаны с помощью распределения спектра амплитуд (энергетический спектр) и спектра фаз.

Спектр
uz - spektr
en - spectrum

Signal amplitudasi va fazasining chastotaga bog‘liq ravishda o‘zgarishini tavsiflovchi hamda signalning xarakteristika va xossalarini qat’iy belgilovchi funksiya. Har qanday signalning spektri turli chastota, amplituda va fazadagi garmonik tebranishlarning yig‘indisi tarzida

ifodalanishi mumkin. Garmonik tashkil etuvchilarga bunday ajratish spektral parchalanish deyiladi, uning xossalari esa amplitudalar spektri (energetik spektr) va fazalar spektrini taqsimlash yordamida tavsiflanishi mumkin

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Кабинета Министров Республики Узбекистан, от 18.01.2019 г. № 48. «Об утверждении концепции внедрения технологий «Умный город» в Республике Узбекистан». http://lex.uz/docs/

2. Д.А.Давронбеков, У.Т.Алиев. Беспроводные сети. Учебник, Ташкент, 2021-495 с.

3. Интернет вещей: учебное пособие/А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

4. Гиббс М. Интернет вещей – не только для «умных» // Сети/network world. – 2013. – №3.

5. Гайкович, Г.Ф. Стандартизация в области промышленных сетей. Развитие беспроводных стандартов для АСУ ТП [текст] / Г.Ф. Гайкович // Электронные компоненты. – 2014. – №1. – С. 48-53.

6. Голышко, А. Строим «интеллектуальный городок» // Мобильные телекоммуникации. – 2018. - №10. – С. 46-51.

7. Колыбельников, А. И. Обзор технологий беспроводных сетей // Труды МФТИ. – 2017. – Том 4. – № 2. – С. 3-29.

8. Сети связи пост-NGN / Б.С. Гольдштейн, А.Е. Кучерявый. – СПб.: БХВ-Петербург, 2018. – 160 с.

9. Григорьева, А. Массовое внедрение RFID-технологии – миф или реальность? Компоненты и технологии. – 2018. – №12.

10. Есауленко, А. Альфа и омега M2M. Платформенные решения – основа основ мира межмашинного взаимодействия [текст] / А. Есауленко // Сети/network world. – 2018. – №3. – С. 21-22.

11. Восков, Л.С. Web вещей – новый этап развития интернета вещей / Л.С. Восков, Н.А. Пилипенко // Качество. Инновации. Образование. – 2018. – № 2. – С. 44-49.

12. Интернет вещей в умном городе / М. Самсонов, А. Гребешков, А. Росляков, С. Ваняшин // ИнформКурьер-Связь. – 2018. – №10. – С. 58-61.

13. ASHTON, K. That ‘Internet of Things’ Thing. In the real world, things matter more than ideas. RFID Journal, 22 June 2019. Available from: http://www.rfidjournal.com/articles/view.

14. Стандартизация Интернета вещей / М.Ю. Самсонов, А.Ю. Гребешков, А.В. Росляков, С.В. Ваняшин // Электросвязь. – 2018. – №8. – С. 10-13.

15. От интернета людей к интернету вещей / М.Ю. Самсонов, А.В. Росляков, С.В. Ваняшин // ИнформКурьер-Связь. – 2013. – №5. – С. 62-64.

16. Всеобъемлющий Интернет: прогнозы и реальность / П. Храмцов // Открытые системы. СУБД. – 2018. – №4. – С. 19-22.

17M2M – новые возможности для развития сотового бизнеса [текст] / И.А. Богородицкая // Электросвязь. – 2017. – №1. – С. 38-39.

18. Круз, Л. Сотовые телефоны станут датчиками? / Л. Круз // Мобильные телекоммуникации. – 2018. – №4-5. – С. 36-38.

19. Стандарты беспроводной связи диапазона ISM / Д. Петров // Электронные компоненты. – 2015. – № 10. – С. 28-32.

20. LTE и беспроводные сенсорные сети / А. Футахи, Е. Кучерявый, А. Кучерявый // Мобильные телекоммуникации. – 2017. - №6-10. – С. 38-41.

21. Партнерский проект oneM2M / В.О. Тихвинский // Электросвязь. – 2017. – №11. – С. 18-20.

22. Инфокоммуникации для «умного» города / В.Г. Рогов // Вестник связи. – 2018. – №8. – С. 39-41.

23. Чувство планеты (Интернет Вещей и следующая технологическая революция) / В.В. Чеклецов. – М.: 2018. – 132 с.

24. Рекомендация МСЭ-Т Y.3001. Будущие сети: целевые установки и цели проектирования, 2016 [электронный ресурс]. – 26 с.

25. Интернет вещей: новые вызовы и новые технологии / Л. Черняк // Открытые системы. СУБД. – 2018. – №4. – С. 14-18.

26. От первых радиометок до Интернета вещей / Л.Черняк // Открытые системы. СУБД. – 2015. – №07-08. – С. 92-94.

27. Eurotech, «интернет вещей» и «облако устройств» / С. Дроздов, С. Золотарев // Control Engineering, Россия. – 2017. - № 8(78). – С. 18-24.

28. Андреев С. Д. Разработка и исследование моделей множественного доступа и алгоритмов управления потоками трафика для гетерогенных беспроводных сетей. Специальность 05.12.13 — «Системы, сети и устройства телекоммуникаций».

Диссертация на соискание ученой степени доктора технических наук. Москва / 2018

29. Приложения беспроводных сенсорных сетей / Д.А.Молчанов, Е. А. Кучерявый [текст] // Электросвязь. - 2016. - №6. - С.20-23.

30. Когнитивные системы и телекоммуникационные сети / В.И. Комашинский, Н.А. Соколов // Вестник связи. – 2017. – №10. – С. 4-8.

31. Обучение поколения Интернета вещей / Г. Кортьюэм, А. Бандара, Н. Смит, М. Ричардс, М. Петре // Открытые системы. СУБД. – 2018. – №4. – С. 23-28.

32. Интернет нановещей и наносети / Е.А. Кучерявый, С. Баласубраманиям // Электросвязь. – 2014. – №4. – С. 24-26.

33. Самоорганизующиеся сети / А.Е. Кучерявый, А.В. Прокопьев, Е.А. Кучерявый. – СПб, «Любавич», 2016.

34. Принципы построения сенсоров и сенсорных сетей / Е. А. Кучерявый, С. А. Молчан, В. В. Кондратьев // Электросвязь. – 2016. – №6. – С.10–15.

35. Беспроводные сенсорные сети, малые системы – большие баксы / В. Майская // Электроника: Наука, Технология, Бизнес. – 2015. – №10. – С. 18–22.

36. Беспроводные сенсорные сети / М. Сергиевский – М. Сергиевский // КомпьютерПресс. – 20017. – №8. – С. 4-10.

37. Интернет-дом: вчера, сегодня, завтра [текст] / А. Прохоров // КомпьютерПресс. – 2012. – №2. – С. 32-38.

38. ZigBee specification overview. Available from: http://www.zigbee.org/Specifications/ ZigBee/GreenPower.aspx

39. IEEE Std 802.15.4e-2012, Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer. April 2012.

40. «Интернет вещей»: Беспроводные сенсорные сети. Белая книга. Международная электротехническая комиссия. IEC, Женева, Швейцария – 2014.

41. Инновационное развитие электроэнергетики на базе концепции Smart Grid / Б.Б. Кобец, И.О. Волкова. – НАЦ Энергия, 2015. – 208 с.

42. Платформа Интернета вещей / Л. Черняк // Открытые системы. СУБД. – 2017. – №7. – С. 44-45.

43. Для мобильных стражей: беспроводной стандарт Bluetooth low energy в системах безопасности / А. Калачев // Новости электроники. – 2018. – № 1. – С. 10-18.

44. Протоколы маршрутизации в беспроводных сенсорных сетях: основанные на местоположении узлов и направленные на агрегацию данных / С.Д. Ерохин, С.С. Макаров // Телекоммуникации и транспорт. T-Com. – 2018. – №3. – С. 44- 47.

45. Приложение к Решению ГКРЧ РУз № 256 от 11.07.2011 г.

46. Решение Республиканского совета по радиочастотам №521 от 30.12.2021 полосы радиочастот 863 - 870 МГц и 922 - 928 МГц на вторичной основе выделены для применения юридическими и физическими лицами оборудования узкополосных беспроводных сетей связи стандартов технологии LPWAN на территории Республики Узбекистан.

47. Опасный Интернет вещей / В. Коржов // Открытые системы. СУБД. – 2013. – №4. – С. 29-30.

48. BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, M. Wireless sensor network: Security challenges. Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor-Network. pdf

49. JAIN, A., K ANT, K. and TRIPATHY, M. R. Security solutions for wireless sensor networks[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT '12). IEEE Computer Society, 2012, pp. 430433.

50. WANG, Y., ATTEBURY, G. and RAMAMURTHY, B. A survey of security issues in wireless sensor networks IEEE Communications Surveys and Tutorials 8, 2006, pp. 223.

51. PATHAN, A. S. K., LEE, H. W. and HONG, C. S. Security in wireless sensor networks: issues and challenges. The 8th International Conference on Advanced Communication Technology (ICACT 2006). IEEE, 2006, Vol. 2, 6 pp.-1048. Available from: http://arxiv.org/ftp/arxiv/papers/0712/0712.4169.pdf

52. MARTIN, T., HSIAO, M., HA, D. and KRISHNASWAMI, J. Denial-of-service attacks on battery- powered mobile computers. Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), IEEE, 2004, pp. 309318. Available from: http://www.ece.vt.edu/ tlmartin/power-secure/ percom_martin_camera-final.pdf

53. KALITA, H. K. and K AR, A. Key management in secure self-organized wireless sensor network: a new approach. Proceedings of the International Conference and Workshop on Emerging Trends in Technology (ICWET '11). ACM, 2011, pp. 865870.

54. Задачи производства изделий M2M: от простого к сложному / М.А. Шнепс-Шнеппе // Вестник связи. – 2013. – №9. – С. 11-16.

55. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture» [электронный ресурс], V1.1.1. – 2016. – 280 p.

56. ETSI TS 102 921 «Machine-to-machine communications (M2M); mIa, dIa and mId interfaces» V1.1.1 [электронный ресурс]. – 2017. – 538 p.

57. ETSI TS 102690 Machine-to-Machine communications (M2M); Functional architecture.

58. M2M(10)0231 M2M applied to the IMS_architecture, ETSI, 2019.

59. 3rd Generation Partnership Project; Technical Specifi cation Group Services and System Aspects; TR 22.868: Study on Facilitating Machine to Machine Communication in 3GPP Systems (Release 8).

60. 3rd Generation Partnership Project; Technical Specifi cation Group Services and System Aspects; TS 22.368: Service requirements for Machine-Type Communications (MTC) (Release 11).

61. 3rdGeneration Partnership Project; Technical Specifi cation Group Services and System Aspects; TR 23.888: System Improvements for Machine-Type Communications (Release 10).

62. 3rd Generation Partnership Project; Technical Specifi cation Group Services and System Aspects; TR 22.888: Study on Enhancements for MTC (Release 11).

63. Тихвинский В.О. Перспективы и модели услуг в сетях M2M// Connect! Мир связи. – 2016. – № 2.

64. Тихвинский В.О., Терентьев С.В., Высочин В.П. Использование IMS-платформы для управления услугами в сетях M2M// Электросвязь. – 2016. – № 4.

65. Machine-to-machine (M2M) – the rise of machine// White Paper, Juniper, 2016.

66. Proceedings of M2M World Congress // M2M World Congress. – London, 2017.

67. Лахири, С. RFID. Руководство по внедрению [текст] / С. Лахири. – М.: Кудиц-Пресс, 2017. – 312 с.

68. Стандарты и тенденции развития RFID-технологий / М. Федоров // Компоненты и технологии. – 2016. – № 1. – С. 108-110.

69. В. Технология RFID сегодня [текст] / В. Филин //Мир этикетки. – 2015. – №9.

70. Системы RFID низкой стоимости / Т. Шарфельд / Под ред. С. Корнеева. – М., 20016. – 197 с.

71. Технология RFID: реалии и перспективы / М. Гудин, В. Зайцев // Компоненты и технологии. – 2013. – №4.

72. Электронная идентификация. Бесконтактные идентификаторы и смарт карты / В.Л. Джхунян, В.Ф. Шаньгин. – М.: «Издательство АСТ»: Издательство «НТ Пресс», 2014. – 695 с.

ОГЛАВЛЕНИЕ

Давронбеков Дилмурод Абдужалилович
Алиев Улугбек Тураевич

БЕСПРОВОДНЫЕ СИСТЕМЫ IoT

Учебник

Ташкент - "METODIST NASHRIYOTI" - 2024

Muharrir: Bakirov Nurmuhammad

Texnik muharrir: Tashatov Farrux
Musahhih: Xolmurodova Zahro
Dizayner: Ochilova Zarnigor

Bosishga 1.04.2024.da ruxsat etildi.
Bichimi 60x90. "Times New Roman" garniturasi.
Ofset bosma usulida bosildi.
Shartli bosma tabog'i 18. Nashr bosma tabog'i 17,25.
Adadi 300 nusxa.

"METODIST NASHRIYOTI" MCHJ matbaa bo'limida chop etildi.
Manzil: Toshkent shahri, Shota Rustaveli 2-vagon tor ko'chasi, 1-uy.

+99893 552-11-21

ISBN 978-9910-03-108-3