

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Казахский национальный исследовательский технический университет имени
К.И.Сатпаева

Институт автоматизации и информационных технологий

Кафедра «Электроники, телекоммуникации и космических технологий»

Алмуханова Жансая Кажмуханкызы

Проектирование корпоративной сети на основе технологии IoT

ДИПЛОМНАЯ РАБОТА

Специальность 5В071900 – Радиотехника, электроника и телекоммуникации

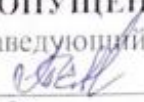
Алматы 2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Казахский национальный исследовательский технический университет имени
К.И.Сатпаева

Институт автоматизации и информационных технологий


Кафедра «Электроники, телекоммуникации и космических технологий»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой ЭТиКТ
 Таштай Е.Т.
«23» мая 2022 г.

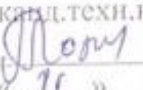
ДИПЛОМНАЯ РАБОТА


На тему: «Проектирование корпоративной сети на основе технологии IoT»

по специальности 5B071900 – Радиотехника, электроника и
телекоммуникации

Выполнил 

Алмуханова Ж.К.

Рецензент
Ассоц.проф. КазНАУ
канд.техн.наук
 Токмолдаев А.Б.
«21» 05 2022 г.

Научный руководитель
к.ф.-м.н, ассоц.-профессор
каф.ЭТиКТ
 Жунусов К.Х.
«23» 05 2022 г.

Алматы 2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Казахский национальный исследовательский технический университет имени
К.И.Сатпаева

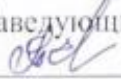
Институт автоматизации и информационных технологий

Кафедра «Электроники, телекоммуникации и космических технологий»

5B071900 – Радиотехника, электроника и телекоммуникации

УТВЕРЖДАЮ

Заведующий кафедрой ЭТиКТ

 Ташбай Е.Т.
« 21 » XII 2021 г.

ЗАДАНИЕ

на выполнение дипломной работы

Обучающемуся Алмуханова Жансая Кажмуханкызы

Тема: «Проектирование корпоративной сети на основе технологии IoT».

Утверждена приказом Ректора Университета №489-П/О от «24» декабря 2022 года.

Срок сдачи законченной работы «15» мая 2022 г.

Исходные данные к дипломной работе:

- 1) Архитектура IoT;
- 2) Классификация технологий передачи данных в IoT;

Краткое содержание к дипломной работе:

- а) Краткий обзор технологии IoT;
- б) Технология LoRaWAN;
- в) Радиочастотное обнаружение RFID.
- г) Расчет параметров сети LTE для IoT;
- д) Расчет бюджета потерь и зоны покрытия сетей GSM и LTE.

Перечень графического материала (с точным указанием обязательных чертежей): представлены 10-15 слайдов презентации работы.

1 Список литературы: Sun C. Application of RFID technology for logistics on internet of things // AASRI Procedia. 2012. Vol. 1.

2 Ngai E. W. T., Moon K. K., Riggins F. J., Yi C. Y. RFID research: An academic literature review (1995–2005) and future research directions // Int. J. Prod. Econ. 2008. Vol. 112, No. 2.

10 Сайт об основных продуктах и оборудовании для IoT сети URL: <http://www.moog-crossbow.com/> (дата обращения 25.04.2017)



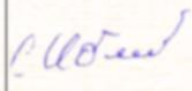
ГРАФИК

подготовки дипломной работы (проекта)

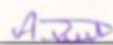
| Наименование разделов, перечень разрабатываемых вопросов | Сроки представления научному руководителю | Примечание |
|--|---|------------|
| Теоретическая часть | 10.01.2022-20.01.2022 | Выполнено |
| Основная часть | 20.01.2022-10.03.2022. | Выполнено |
| Расчетная часть | 11.03.2022-28.04.2022. | Выполнено |
| Заключение | 01.04.2022-10.05.2022 | Выполнено |

Подписи

консультантов и нормоконтролера на законченную дипломную работу с указанием относящихся к ним разделов работы

| Наименования разделов | Консультанты, И.О.Ф. (уч. степень, звание) | Дата подписания | Подпись |
|------------------------------|---|-----------------|---|
| Разбор темы дипломной работы | Лектор каф. ЭТиКТ Марксулы Сунгат | 20.05.2022 |  |
| Теоретическая часть | Лектор каф. ЭТиКТ Марксулы Сунгат | 20.05.2022 |  |
| Нормоконтролер | Магистр технических наук, лектор Ибекеев С.Е. | 20.05.2022 |  |

Научный руководитель _____  Жунусов К.Х.

Задание принял к исполнению обучающийся _____  Алмуханова Ж.К.

Дата _____ «15» _____ мая _____ 2022 г.

АННОТАЦИЯ

В данном дипломном проекте были рассмотрены вопросы Интернет вещей, организации IoT технологий, их влияние на новые информационно-коммуникационные технологии и на корпоративные системы промышленного комплекса РК.

Приведены технологии Интернета вещей, технология LoRaWAN, радиочастотное обнаружение RFID.

Приведены предпосылки и текущие исследования в области IoT технологий, сервис-ориентированная архитектура для «Интернета вещей» (IoT), рассмотрены сети связи для IoT.

Также были изложены вопросы корпоративных информационных систем на основе IoT процессов и приложений.

АҢДАТПА

Бұл дипломдық жобада интернет заттары, It технологияларды ұйымдастыру, олардың жаңа ақпараттық-коммуникациялық технологияларға және ҚР өнеркәсіптік кешенінің корпоративтік жүйелеріне әсері мәселелері қаралды.

Интернет заттары технологиясы, LoRaWAN технологиясы, RFID радиожілігін анықтау.

IoT технологиялары саласындағы алғышарттар мен ағымдағы зерттеулер, "Заттар интернеті" (IoT) үшін сервиске бағытталған архитектура келтірілген, IoT үшін байланыс желілері қарастырылған.

Сондай-ақ, it процестер мен қосымшалар негізінде корпоративтік ақпараттық жүйелердің мәселелері баяндалды.

ANNOTATION

In this diploma project, the issues of the Internet of Things, the organization of It technologies, their impact on new information and communication technologies and on corporate systems of the industrial complex of the Republic of Kazakhstan were considered.

The technologies of the Internet of Things, LoRaWAN technology, RFID radio frequency detection are given.

Prerequisites and current research in the field of IoT technologies, service-oriented architecture for the "Internet of Things" (IoT) are given, communication networks for IoT are considered.

The issues of corporate information systems based on It processes and applications were also outlined.

СОДЕРЖАНИЕ

| | |
|---|----|
| Введение | 9 |
| 1 Интернет вещей. Основные понятия | 10 |
| 1.1 Архитектура IoT | 13 |
| 1.2 Когнитивный интернет вещей | 14 |
| 1.3 Классификация технологий передачи данных в IoT | 17 |
| 1.4 Перспективы и прогнозы развития IoT | 18 |
| 2 Технологии Интернета вещей | 20 |
| 2.1 Технология LoRaWAN | 23 |
| 2.2 Радиочастотное обнаружение RFID | 25 |
| 2.3 Беспроводные сенсорные сети | 30 |
| 2.4 Межмашинная связь M2M | 35 |
| 3 Расчет параметров сети LTE для IoT | 38 |
| 3.1 Расчет бюджета потерь и зоны покрытия сетей GSM и LTE | 38 |
| 3.2 Расчет восходящей линии (UL) LTE | 39 |
| 3.3 Расчет нисходящей радиолинии (DL) LTE | 43 |
| 3.4 Расчет максимально допустимых потерь сети LTE | 46 |
| Заключение | 50 |
| Список использованной литературы | 51 |

ВВЕДЕНИЕ

Концепция "Интернета вещей" - одна из новых идей, которые не только радикально меняют внешний вид коммуникационных и информационных систем, но и влияют на уровень жизни людей.

В моей дипломной работе рассматривается одна из современных тенденций развития информационных технологий - Интернет вещей (IoT). Количество устройств, подключенных к Интернету, растет с каждым годом. Внедрение "Интернета вещей" будет способствовать экономическому развитию и повышению уровня жизни в стране при минимальных инвестициях.

Технология Интернета вещей обладает большим потенциалом, к сожалению, который не был использован в полной мере. Развитие "Умного города" основано на использовании этой технологии. В своей работе я хочу показать, насколько эффективно и полезно использование Интернета вещей в повседневной жизни, а также на национальном уровне. Насколько это поможет оптимизировать все процессы и получить прибыль с бытовой и промышленной точки зрения.

Если "Интернет вещей" стал невидимой, но неотъемлемой частью жизни людей, не усложняя жизненный процесс, то можно говорить о его полноценном и успешном внедрении. Интернет вещей ускоряет развитие умных городов. Сейчас в некоторых городах мы видим только начало этого процесса, но мы уже положительно оцениваем инновации в транспорте, связи, медицине и других сферах жизни, хотя на начальном этапе было много сомнений и недоверия.

Интернет вещей стал отличной бизнес-платформой. Поставщики могут покупать их услуги за небольшую плату и получать прибыль. Это может стать источником дохода для государственного бюджета. Для более полного понимания технологий в работе изучены передовые исследования в развитии «интернет вещей», также в работе проанализированы технологии, реализуемые в Казахстане, совместные проекты с зарубежными партнерами.

1 Интернет вещей. Основные понятия

Интернет вещей - это совокупность физических объектов, подключенных к Интернету и взаимодействующих друг с другом и с внешней средой. Это понятие заимствовано из английского понятия Internet of Things (IoT).

Впервые концепция и сроки беспроводной передачи данных были сформулированы Кевином Эштоном, основателем исследовательской группы Auto-ID в MIT в 1999 году. Суть концепции была представлена на презентации, посвященной руководству Procter & Gamble. Для оптимизации работы корпорации было предложено использовать внедрение радиочастотных меток для изменения системы управления цепями поставок.

NGC - это американская научная статья, посвященная теме дома, опубликованная в мае 2004 года. В этом посте наглядно показано, как работают «предметы», оснащенные бытовой техникой (кондиционеры, часы сигнализации, компьютеры), домашними системами (пожарная система, система освещения, орошение сада), тепловыми датчиками, датчиками движения и опознавательным знаком, взаимодействуют друг с другом через инфракрасное излучение. Беспроводные, мощные и малотоковые сети позволяют вам экономить энергию и управлять своими расходами [1].

Концепция автоматизированных домов не нова, но интеграция оборудования и «вещей» в единую сеть, обслуживание интернет-протоколов получили широкую популярность. В настоящее время технологии IoT быстро внедряются во все сферы общества. Благодаря активному использованию различных устройств мы облегчаем себе жизнь. Достижения в области аппаратного обеспечения предоставляют им возможность слышать, видеть, думать и иногда действовать.

Для быстрого принятия решения связанные с жизнью людей или безопасностью зданий, также для скоординированной и эффективной работы, устройства должны максимально правильно взаимодействовать друг с другом. Современные беспроводные технологии, различные встроенные датчики, новейшие технологии позволяют ставить задачи "интернет-вещам". В связи с огромным количеством производителей, технологий и устройств, возникают множество проблем. Поэтому необходимо сформулировать и утвердить определенные стандарты и протоколы связи [2].

Успешно разработанное приложение IoT имеет задачи, обеспечивающие мобильность: протоколы маршрутизации должны работать правильно, так как IP-адрес изменяется при движении устройства IoT; при сборе, передаче данных и принятии решений система должна отвечать уверенно и быстро; имеет расширенный спектр действий для пользователей Сети.

Сама концепция "интернет вещей" предполагает, что к сети подключаются миллионы устройств. Основная сложность заключается в обеспечении оптимального управления и доступности: мониторинг ошибок, настройка и производительность многих таких устройств с помощью протоколов управления. Кроме того, необходимо гарантировать

взаимодействие в сети: гетерогенные устройства и протоколы должны работать друг с другом в отношении обеспечения конфиденциальности и безопасности.

В интернете вещей принят следующий алгоритм: терминальные устройства, датчики и датчики соединяются между собой (так называемый D2D-Device to Device). Данные, собранные устройствами, отправляются на сервер для дальнейшего анализа и обработки (взаимодействие D2S - Device to Server). Сервер может содержать несколько компьютеров или объектов, которым необходимо взаимодействовать друг с другом (взаимодействие S2S-Server to Server). Для выполнения разных задач должны использоваться разные протоколы. Далее в тезисе приводятся наиболее распространенные и перспективные на сегодняшний день протоколы, каждому из которых дается краткое описание.

В нашей стране люди давно говорят об интернете вещей. Понимая важность развития этой сферы, государство взяло под контроль несколько проектов в рамках развития IoT. В настоящее время системы IoT внедряются в общественном транспорте и системе жилищно-коммунального хозяйства.

Реализация концепции Интернета вещей заключается в разработке средств доступа к информации, которые в большинстве случаев являются чувствительными сенсорными датчиками, и разработке методов доставки информации от этих датчиков к потребителям и системам обработки. Сегодня на современном уровне развития информационно-коммуникационных систем Интернета вещей существуют различные функции и компоненты [3].

Сети IoT могут использовать различные технологии для связи между узлами сети, различные сетевые архитектуры и различные технологии для сбора необработанных данных.

Источниками информации могут быть различные датчики, регистрирующие состояние физической среды, такие как акустические датчики (микрофоны) и датчики изображения (камеры). Поэтому требования к интернету вещей и интернету вещей могут сильно отличаться от требований к отправке редких коротких сообщений, состоящих из нескольких байтов, до отправки потоковых данных. Структура сети IoT часто определяется проблемой удобства использования, а структуры типа "звезда" и древовидные структуры могут быть одно- или многоуровневыми.

Коммуникационные линии могут быть проводными, так и беспроводными. Вышеизложенное необходимо для того, чтобы определить, какие конкретные сети в настоящее время могут быть классифицированы как сети IoT.

В настоящее время эти сети обычно строятся с использованием проводных или беспроводных технологий связи. Технологии беспроводной связи включают технологии, используемые операторами для сотовых сетей, или технологии для построения беспроводных локальных сетей, или технологии для сенсорных сетей. Функциональные возможности, часто реализуемые в современных сетях IoT, называются коммуникациями M2M

(machine-to-machine). Эта форма связи фактически является частью (в настоящее время наиболее распространенной) IoT.

Основное отличие IoT от других сетей заключается в том, что люди не являются непосредственными пользователями сети. Устройства (объекты), подключенные к IoT, не определяются напрямую поведением человека, как это происходит, например, в традиционных сетях связи, где терминал управляется непосредственно пользователем.

Распространение (проникновение) устройств, использующих связь M2M, в настоящее время является наиболее важным показателем эволюции IoT. Количество таких устройств, подключенных к информационно-коммуникационным системам одним из описанных выше способов, характерно для современного состояния Интернета вещей. Это число не зависит напрямую от демографических факторов, как в случае с мобильными терминалами, а определяется информационными потребностями и меняющейся сферой использования этих сетей.

Приложения IoT, естественно, зависят от определенного уровня территориальной связности, чему также способствуют специфические приложения этих сетей. На этом уровне развития наибольшее количество объектов IoT (плотность) сосредоточено в районах с высоким проникновением и другими видами коммуникаций высокой плотности. По мере развития IoT в ближайшем будущем можно ожидать, по крайней мере, такой модели развития. Плотность сетей IoT может быть выше на объектах и в районах с высокой плотностью населения.

На рисунке 1 представлены статистические данные и прогнозные значения устройств IoT в мире (на основе количества устройств M2M), полученные на основе данных из Cisco [4].

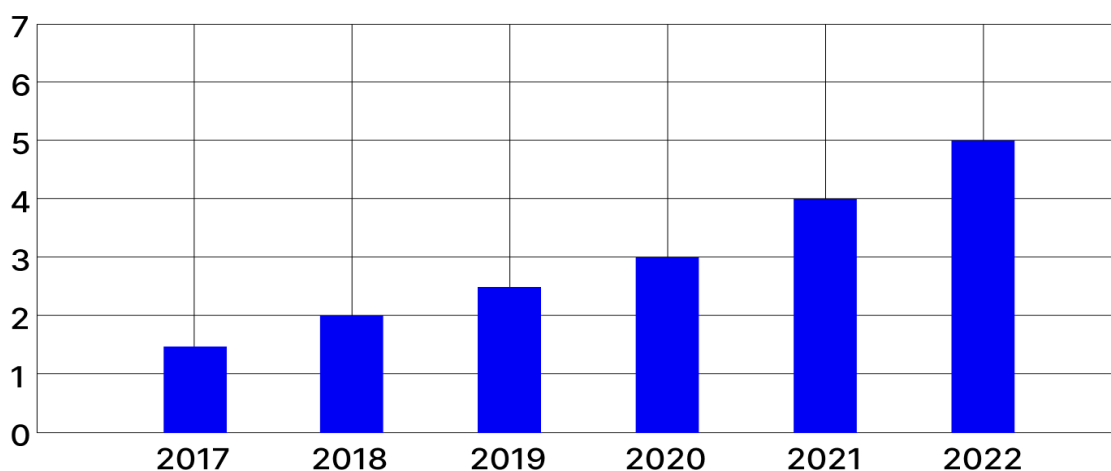


Рисунок 1.1 - Глобальный рост числа IoT-устройств (по данным Cisco), млн.штук

Гистограмма показывает, что в будущем количество IoT-устройств во всем мире значительно вырастет и к 2022 году удвоится. Общее количество

этих устройств будет близко к численности населения. Следует отметить, что оценку, представленную на этом графике, можно считать восходящим предположением, поскольку она основана только на анализе количества M2M-устройств, используемых в настоящее время в IoT, но по мере их роста она будет включать значительное количество объектов, которые не являются частью IoTs (бренды продуктов, виртуальные объекты, объекты дополненной реальности, объекты в быту и промышленности) [5].

1.1 Архитектура IoT

Архитектура Интернета вещей показывает, как различные ИКТ-технологии связаны между собой, чтобы обеспечить работу сети Интернет вещей.

Архитектура IoT состоит из четырех функциональных уровней, как показано на рисунке и описано ниже.

Уровень взаимодействия с окружающей средой (датчики и сенсорные сети) является наименьшим уровнем архитектуры IoT и состоит из умных объектов, встроенных в КС. Датчики осуществляют связь между физическим и виртуальным (цифровым) миром, собирая и обрабатывая информацию в режиме реального времени. Большинство датчиков необходимо подключить к агрегатору датчиков (шлюзу), который может быть установлен в локальной сети, например, Ethernet, Wi-Fi или персональной сети (PAN).

Сетевой уровень обеспечивает большие объемы данных, генерируемых различными сетевыми уровнями, и состоит из конвергентной сетевой инфраструктуры, которая создается путем объединения разнородных сетей в единую сетевую платформу.

Уровень сервиса включает комплекс информационных услуг, автоматизирующих технологические деловые операции в IoT: поддержка оперативно-деловой деятельности, обработка различной аналитической информации, хранение данных, информационная безопасность, управление бизнес-процессами и другие.

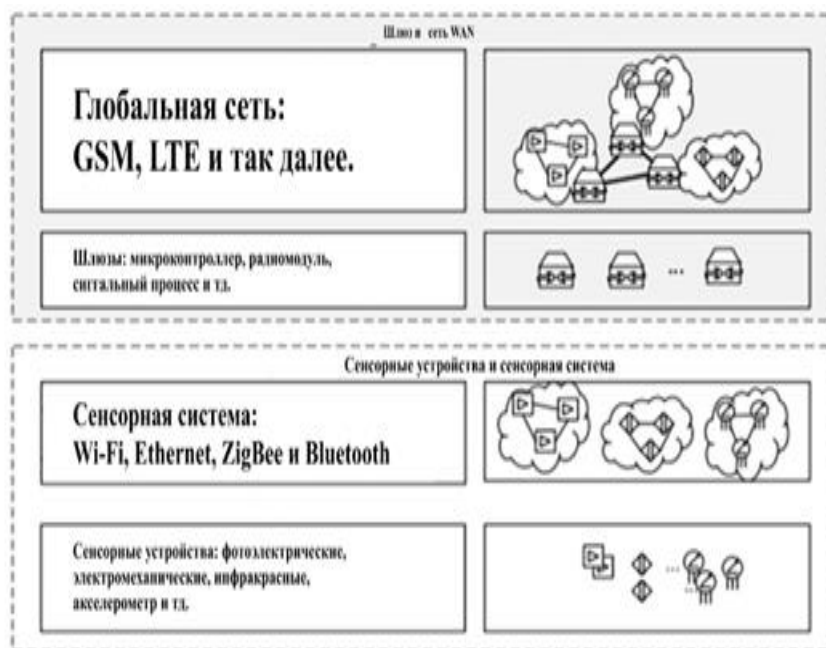


Рисунок 1.2 - Архитектура IoT

Прикладной уровень включает широкий спектр приложений в энергетике, транспорте, коммерции, медицине, образовании и других областях. Приложения могут быть вертикальными, т.е. специфическими для конкретной отрасли, или горизонтальными, т.е. общепромышленными [7].

На практике используется один из трех способов взаимодействия с Интернетом:

- прямого доступа к,
- взаимодействие через шлюз,
- взаимодействие через сервер.

В дополнение к преимуществам вышеуказанных методов доступа, сервер предоставляет услуги хранения и обработки данных в виде облачных сервисов. Такой подход не исключает использования шлюзов для подключения локальных беспроводных сетей к серверу [9].

1.2 Когнитивный интернет вещей

Идея когнитивного радио в контексте свойств радиоэлектронных средств (РЭС) была впервые предложена в 1999 году и с тех пор превратилась в концепцию когнитивного радио (КР). Суть КР заключается в том, что беспроводные абонентские устройства (например, смартфоны) и их сети могут быть относительно автономными и "интеллектуальными" в выборе и использовании доступных радиоресурсов и сетевых соединений. Правила для этих устройств зависят от того, нужен ли пользователям доступ к

определенным услугам. В то же время РЭС должна обеспечивать оптимальную работу радиочастот без помех.

Когнитивные РЭС могут использовать зондирование для временного определения местоположения свободных участков спектра, которые ранее были выделены для других видов использования. Когнитивные РЭС временно занимают эти свободные радиодиапазоны или каналы для приема и передачи информации, не создавая помех для радиосредств в выбранном диапазоне. Описанные характеристики когнитивной радиосети (Cognitive Radio Network, CRN) в основном проявляются в программном управлении сетью и ее элементами [10].

Пользователь может использовать терминал для получения услуг в сетях когнитивного радио на основе принципа управления протоколами и параметрами интерфейса программно определяемого радио SDR (Software – Defined Radio). Эти устройства имеют широкие технические возможности для выбора различных линий связи для получения необходимых услуг. SDR-устройства могут работать с несколькими беспроводными стандартами - GSM/GPRS/EDGE, UMTS, Wi-Fi, LTE - и использовать диапазон телевизионных частот, определенный стандартом IEEE 802.22-2011. Следует отметить, что принципы и когнитивные свойства SDR также применимы к устройствам базовых станций и могут быть использованы в устройствах IoT.

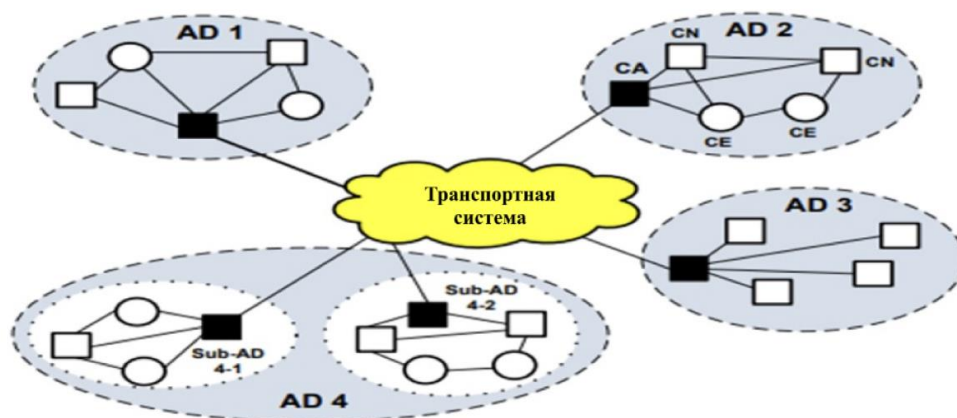


Рисунок 1.3 - Архитектура CIoT

Когнитивный Интернет вещей (CIoT) - это новая концепция информационных сетей, в которых объекты (физические или виртуальные) подключены и общаются между собой с минимальным вмешательством человека. Объекты в такой сети могут формировать четкое представление о собственном состоянии и состоянии окружающих объектов, воспринимать знания об окружающей среде, делать из них логические выводы, адаптироваться к внешним и внутренним условиям.

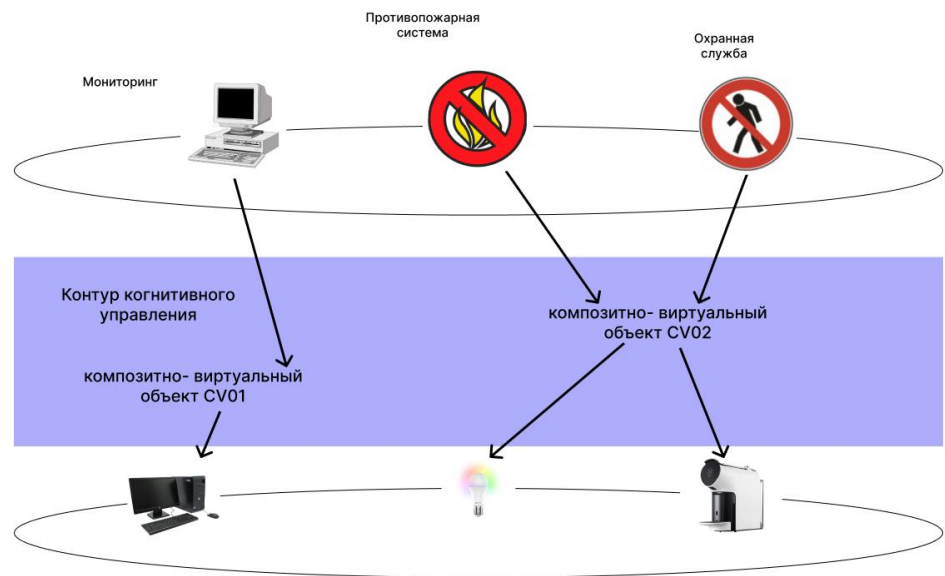


Рисунок 1.4 - Общая схема управления IoT

Каждый автономный домен использует когнитивный агент, который взаимодействует с узлами, и когнитивные или простые элементы, которые организуют взаимодействие. Таким образом, взаимодействие с доменом возможно, как на уровне всего домена, так и на уровне отдельных когнитивных элементов. Важно отметить, что домен может также состоять из некогнитивных узлов.

Последним компонентом текущей системы является реализация операционной логики, которая распространяет требования IoT-приложения или IoT-пользователя на составной виртуальный объект, предоставляющий услугу.

В результате в схеме когнитивного управления CIoT возникают три системных уровня:

- 1) уровень виртуальных объектов;
- 2) уровень композитных виртуальных объектов;
- 3) уровень обслуживания.

Он позволяет осуществлять независимое управление и независимую конфигурацию для непрерывного взаимодействия с физическим когнитивным объектом на уровне виртуального объекта, а также контролировать информационный поток.

Когнитивный IoT на уровне сервиса необходим для обработки запросов приложений и выбора составного виртуального объекта на более низком уровне. Таким образом, система CIoT может действовать от имени пользователя на основе анализа предпочтений пользователя в базе знаний и результатов машинного обучения. Кроме того, для использования определенных объектов действуют процедуры безопасности, авторизации и определения приоритетов.

1.3 Классификация технологий передачи данных в IoT

Одна из основных проблем в организации интернета вещей:

- Интернет вещей;
- пользователи и интернет-товары;
- изучение отношений между удаленным сервером и интернет-объектами.

Интернет вещей использует ряд различных коммуникационных сетей для передачи данных, включая сеть Body Area Network (BAN), которая работает в теле человека на расстоянии десятков сантиметров до сети Интернет. В локальных сетях используются технологии RFID, NFC, Bluetooth, Wi-Fi и т.д. Связь на большие расстояния зависит от различных мобильных сетей (2G/3G/4G), беспроводных широкополосных сетей WiMAX и систем GPS/Глонасс.

С точки зрения охвата телекоммуникационные сети, используемые в интернете вещей, можно разделить на 4 основных типа.

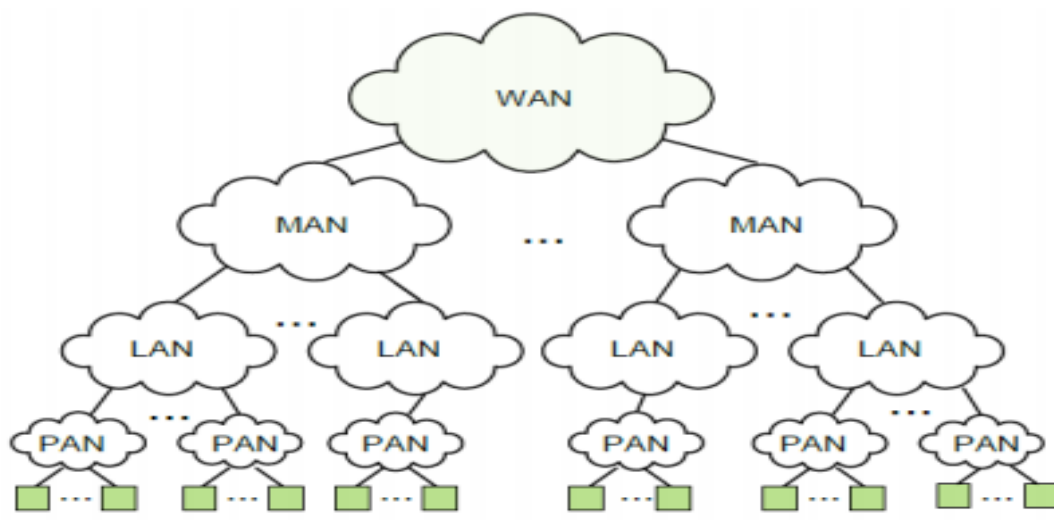


Рисунок 1.5 - Взаимосвязь между телекоммуникационными системами в Интернете вещей

(а) Частная сеть (PAN) - это сеть, построенная "вокруг" отдельного человека. Эти сети предназначены для интеграции всех персональных устройств пользователя (телефонов, смартфонов, КПК, ноутбуков, гарнитур и т.д.). В случае IoT такая сеть строится "вокруг" устройства,

(б) Локальная сеть обычно относится к сети, охватывающей относительно небольшую территорию или группу зданий (дома, офисы, предприятия). Локальные сети могут также включать в себя сети блоков управления. Это производственная сеть, основной целью которой является соединение различных исполнительных механизмов и датчиков предприятия в единую сеть.

(c) Metropolitan Area Network (MAN) - соединяет отдельных пользователей в городе с локальной сетью, которая больше, чем локальная сеть, но меньше, чем глобальная сеть.

(d) Глобальная сеть (WAN) - включает пользователей и сети, охватывающие сотни или тысячи километров.

IoT практически не предъявляет особых требований к технологиям LAN, MAN и WAN, которые также они хорошо освещены в технической литературе. Поэтому здесь рассматриваются только стандарты и протоколы, обычно используемые для малых и средних сетей IoT.

1.4 Перспективы и прогнозы развития IoT

Интернет вещей - это следующий шаг в эволюции интернет-технологий. Это набор объектов с точно определенными идентификаторами, необходимыми для связи с внешней средой (объекты Интернета). Эта технология с ее способностью идентифицировать, собирать, обрабатывать и передавать данные позволяет эффективно использовать "вещи" для различных целей. Основное требование к "вещам", используемым в этих сетях, заключается в том, что они должны быть способны передавать данные. В IoT каждый объект имеет свой собственный идентификатор и образует коллекцию объектов, которые могут общаться друг с другом и формировать сеть внутри более крупной сети. Каждый объект IoT предлагает различные услуги и, следовательно, предоставляет определенный сервис. Кроме того, устройства в такой сети могут получать команды от всех остальных узлов. Это означает, что все объекты IoT могут общаться друг с другом и предлагать различные услуги.

Интернет вещей основан на следующих принципах:

- везде инфраструктура связи,
- глобальная идентификация каждого объекта,
- возможность передачи и приема данных через сеть или Интернет, к которым подключен сам каждый объект.



Рисунок 1.6 - Платформа IoT

С развитием этой технологии можно говорить о следующих преимуществах: перенос повседневной деятельности в цифровой мир, умные часы и носимые устройства, оптимизирующие доступ к городским услугам. Для города мы также можем отметить следующие преимущества: отказ от светофоров и использование 3D-устройств, позволяющих избежать задержек в движении; "умные" здания, которые не только контролируют потребление энергии и безопасность, но и способствуют проведению оздоровительных мероприятий.

В целом, основными условиями для продвижения этой технологии являются следующие:

- Значительное увеличение количества подключенных к Интернету устройств. Ожидается, что к 2020 году количество устройств достигнет 25 миллиардов;
- Необходимость оптимизации обработки данных и управления бизнесом;
- Необходимость снижения затрат на организацию безопасности и управление устройствами;
- Необходимость организации удаленной работы, т.е. работы без физического присутствия на рабочем месте;
- Необходимость получения реальных значений в реальном времени;
- Необходимо разработать топологию сети.

2 Технологии Интернета вещей

Где используется Интернет вещей?

Телевизоры, холодильники, принтеры и весь "умный дом" могут быть полностью автоматизированы. Когда IoT подключен к сети, люди избавлены от навязчивых мыслей (не забыли ли они закрыть дверь или выключить плиту) - они могут просматривать всю информацию на своем смартфоне и удаленно запускать несовершенный алгоритм. А "умный" пылесос предупредит о золотых серьгах, лежащих на стуле.

Безопасность. внедрение технологии IoT в систему безопасности позволяет сканировать и загружать фотографии и видео, а искусственный интеллект может запоминать и идентифицировать людей.

Производство. Производство будет автоматизировано: системы мониторинга будут предоставлять информацию о потенциальных проблемах и сбоях оборудования, а клиенты смогут размещать заказы дистанционно.

Медицина. Интернет вещей - это ключ к персонализации устройств, которые помогают контролировать и отслеживать жизненные показатели человека и при необходимости вызывать врача.

Транспорт. В мире Интернета нет пробок - сеть датчиков и счетчиков обнаруживает пробки и оптимизирует маршруты движения.

Розничная торговля. Обычные магазины снова конкурируют с интернет-магазинами - внедряется автоматическая передача и анализ данных о покупателях через POS-терминалы.

В настоящее время к IoT подключено менее одного процента устройств в мире, но их число постепенно растет.



Рисунок 2.1 - Среда использования IoT

Интернет вещей - это технология будущего, которая меняет наш сегодняшний образ жизни.

Пластырь-термометр. В 2016 году компания Isitherm выпустила инновацию - умный термопластик, который измеряет температуру тела с течением времени. Это устройство передает данные через приложение для смартфона и направляет их врачу.

MTS IoT Lab. В январе 2017 года в столице была открыта лаборатория IoT. В залах демонстрируются инновационные IoT-решения для различных отраслей промышленности, а технологию можно протестировать на планшете или смартфоне.

"Animo - это умный электроинструмент. Эта новинка позволяет кормить питомца дистанционно и управляется с помощью приложения на смартфоне. Животное не может пересилить устройство и открыть его - кормушка подает определенное количество пищи в определенное время.

Проблемы и недостатки IoT.

1. Единой системы нет. Проблема интеграции ИИ заключается в том, что при отсутствии общих правил и стандартов сложно внедрить универсальное решение без понимания общей картины.

2. Энергопотребление. Для полноценной работы IoT должен получить автономность сети и получать энергию из окружающей среды.

3. Отсутствие конфиденциальности. Основной риск - в открытых базах данных. Мошенники имеют возможность взломать не только счета и компьютеры, но даже холодильники.

4. Системные затраты. Техника дорога, несмотря на то, что ее использование окупится в будущем: система "Умный дом" поможет сэкономить на электричестве и водоснабжении; предупредит о риске поломки оборудования на производстве; кухонная техника предотвратит порчу продуктов.

Новые возможности для будущего. Трудно сказать, как будет выглядеть Интернет вещей через десять лет, но несомненно, что применение инновационных алгоритмов будет активно использоваться на рынке услуг и принесет много пользы для улучшения качества жизни в России и других странах, открывая перспективные возможности в бизнесе и в целом.

Важность интернета промышленным компаниям

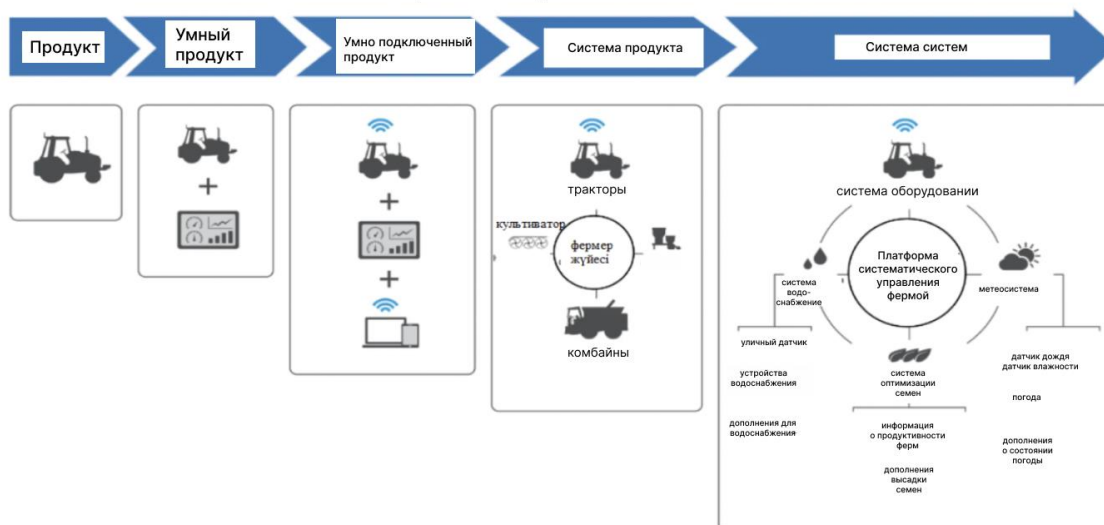


Рисунок 2.2 - Преимущества технологии IoT для промышленных компаний

Интернет вещей - это взаимодействие между машинами при минимальном вмешательстве человека.

Примером того, как работает IoT, является умная кофеварка. Сегодня среднестатистический кофеман включает машину, кладет зерна в специальный отсек, наполняет емкость водой, выбирает нужный режим и получает чашку кофе. Но это не IoT, это просто автоматизация процесса.

Для достижения максимальной "независимости" система должна взять под контроль несколько действий:

- Учет растрат кофе;
- Расписание момента покупки;

Для передачи трафика IoT используются различные технологии, включая беспроводные и проводные сети.

Беспроводная сенсорная сеть - это самоорганизующаяся сеть из множества датчиков и исполнительных устройств, соединенных радиоканалом.

Беспроводные сети можно разделить на следующие типы:

- Сети с малым радиусом действия и низким энергопотреблением;
- Широкополосные маломощные сети большой протяженности (LPWAN): сети большой протяженности с низким энергопотреблением;
- Сотовые сети: технологии, основанные на использовании стандартов сотовой связи в лицензированном частотном диапазоне.

Из проводных технологий важную роль в развертывании Интернета играет технология PLC, использующая воздушные сети, поскольку большинство устройств имеют доступ к электросети. К ним относятся различные торговые автоматы, банкоматы, счетчики и датчики света, которые

подключены к электрической сети. Многие из этих технологий также используются при разработке Интернета вещей.

2.1 Технология LoRaWAN

В марте 2015 года корпорация Semtech объявила о новом значительном достижении в области технологий беспроводной передачи данных. Они представили сетевой протокол с низким энергопотреблением под названием LoRaWAN (Long Range Wide Area Networks).

Этот протокол предлагает ряд преимуществ перед Wi-Fi и сотовыми сетями за счет использования технологий M2M (machine-to-machine communication). Эта технология вызвала большой интерес со стороны производителей и провайдеров на рынке мобильных устройств. LoRa Alliance был создан для продвижения, развития и стандартизации этой технологии.

Основная цель Альянса была сформулирована следующим образом: интеграция аппаратного и программного обеспечения на основе стандарта LoRaWAN. Это позволит операторам связи предлагать интернет-продукты предприятиям и частным лицам. Использование этого стандарта значительно упростит взаимодействие со все более быстро развивающимися устройствами. Технология Lora относится к классу LPWAN, что позволяет проникать сигналу в самые глубины городов и стабильно работать в сельской местности. Все это позволяет разрабатывать и совершенствовать различные приложения "умного города" на основе технологии LoRa.

Корпорация Semtech является одним из основателей Lora Alliance и производителем устройств LoRa и беспроводной технологии LoRaWAN.

LoRaWAN - это открытый протокол для сетей высокой пропускной способности (около 1 миллиона устройств) с низким энергопотреблением и большим радиусом действия (до 15 км на открытой местности). Протокол обеспечивает связь между узлами сети и использует уникальные методы шифрования для обеспечения надежности и безопасности системы.

2.1.1 Архитектура сети LoRaWAN

К составным частям технологии LoraWAN относятся:

1. конечные узлы;
2. шлюзы (Gateway);
3. сетевой сервер;
4. серверы приложений.

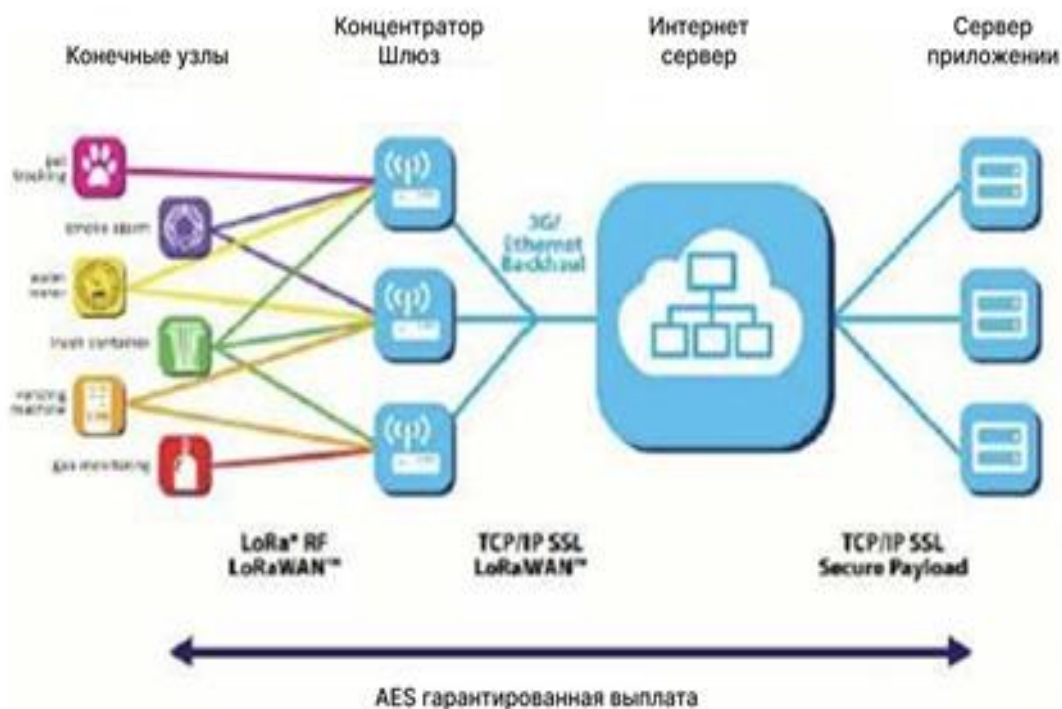


Рисунок 2.3 – Архитектура сети LoRaWAN

Конечные узлы (End Points) - являются элементами сети системы LoRa, где они выполняют такие функции, как измерение или управление и контроль. Они располагаются удаленно и имеют батарейное питание. Используя сетевой протокол LoRaWAN, эти конечные точки могут быть настроены для связи с шлюзом LoRa (концентратором или базовой станцией).

Шлюзы - предназначены для использования в радиальных звездообразных сетевых архитектурах большого радиуса действия, они используются в системе LoRaWAN. Из-за свойств технологии LoRa эти шлюзы могут представлять собой многоканальные мультимодемные трансиверы, которые способны выполнять демодуляцию сразу нескольких каналах одновременно, и даже одновременную демодуляцию множества сигналов на одном и том же канале. Эти шлюзы используют иные радиочастотные компоненты, чем те, которые применяются в конечной точке для обеспечения высокой мощности излучения непосредственно радиосигнала. Шлюзы служат в качестве интерфейса в виде прозрачного моста для передачи сообщений между конечными устройствами и центральным сервером сети.

Шлюзы подключаются к сетевому серверу через стандартные IP-соединения, а конечные также поддерживают функционирование в режиме, обеспечивающим возможность осуществления группового обновления программного обеспечения по радиоканалу или передачу иных массовых сообщений, что позволяет сократить активное время на их передачу. В зависимости от желаемой их канальной емкости и мест установки доступны

разные версии шлюзов, они могут устанавливаться внутри помещений или на вышках.

2.2 Радиочастотное обнаружение RFID

RFID (Radio Frequency Identification) - это современная технология автоматического распознавания объектов, т.е. бесконтактной идентификации. Технология RFID имеет сегодня очень широкий спектр применения - это платежная система, система безопасности "электронный ключ", сбор данных в крупных аэропортах, система обнаружения прохода, которая в данном случае сигнализирует о краже товара из магазина, и т.д. Предметом изучения является изучение особенностей применения технологии RFID в различных сферах деятельности на основе анализа опыта и методик применения. В этом контексте курс направлен на поиск решений для практического применения технологии RFID в различных областях, в частности, в оптимизации складов и цепочек поставок. Для достижения этой цели были сформулированы следующие задачи: во-первых, изучить историю развития технологии RFID; во-вторых, изучить структуру и принцип работы технологии RFID; в-третьих, проанализировать применение технологии RFID в различных сферах деятельности; в-четвертых, изучить возможности технологии RFID в организации транспортировки товаров.

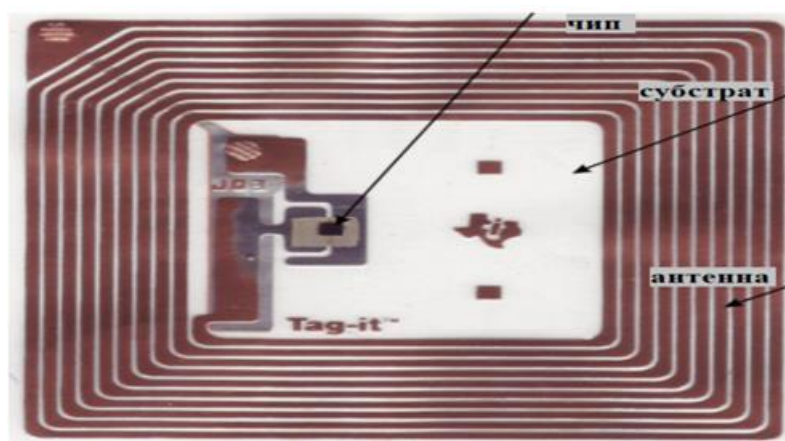


Рисунок 2.4 - Устройство RFID-тегов

Система RFID проста и состоит из трех компонентов:

- информация (ридер).
- транспондер (RFID-метки) .
- ПО (программное обеспечение для обработки данных).

Сканер испускает электромагнитные волны и излучает их в пространство. Как только метка RFID попадает в зону действия

электромагнитных волн считывающего устройства, информация сканируется и отправляется на компьютер или в программное обеспечение для обработки.

Каждая метка (объект) должна иметь свой уникальный номер, который ее идентифицирует. Без этого механизма идентификаторы были бы запутанными, а информация - искаженной.

Общий принцип работы систем RFID очень прост. Система всегда состоит из трех основных компонентов: считывающего устройства, идентификатора (карта, бейдж, метка) и компьютера. Считывающее устройство передает электромагнитную энергию в окружающее пространство. Метка получает сигнал от считывателя и генерирует ответный сигнал, который принимается антенной считывателя, обрабатывается электронным блоком и передается на компьютер через интерфейс.



Рисунок 2.5 - RFID-состав метки

Считыватель имеет приемник и антенну, которая посылает сигнал на метку и получает ответ, микропроцессор, который проверяет и декодирует данные, и память, которая хранит данные для последующей передачи при необходимости.

Основными компонентами транспондера (метки) являются интегральная схема и антенна, которые управляют связью с учеником. Чип имеет память, в которой хранится идентификационный код или другие данные. Метка обнаруживает сигнал от считывателя и начинает отправлять данные, хранящиеся в памяти, на считыватель. Между считывателем и меткой не требуется линия связи, поскольку радиосигнал легко проникает через неметаллические материалы. Таким образом, метки могут быть скрыты в объектах, которые необходимо идентифицировать. Метки могут быть активными или пассивными. Активные метки питаются от подключенного или встроенного аккумулятора. Они требуют меньше энергии для считывания и, как правило, имеют больший радиус действия. Пассивная метка работает без источника питания и получает питание от сигнала считывания. Пассивные метки меньше и легче активных, дешевле и имеют практически неограниченный срок службы.

Активные и пассивные метки могут быть:

- Только для чтения;
- Читайте и пишете;
- Данные записываются один раз и могут быть введены пользователем.

По принципу действия RFID-системы можно разделить на пассивные и интерактивные. В простой пассивной системе излучение от считывателя постоянно (немодулировано) во времени и используется только для управления меткой. При достижении желаемого уровня мощности идентификатор активируется, и излучение от считывателя модулируется кодом, полученным считывателем. По этому принципу работают многие системы контроля доступа, которым требуется только серийный идентификационный номер. Например, системы, используемые в логистике, работают в интерактивном режиме. В такой системе считыватель генерирует модулированные колебания, т.е. формирует запрос. Идентификатор шифрует запрос и при необходимости генерирует соответствующий ответ.

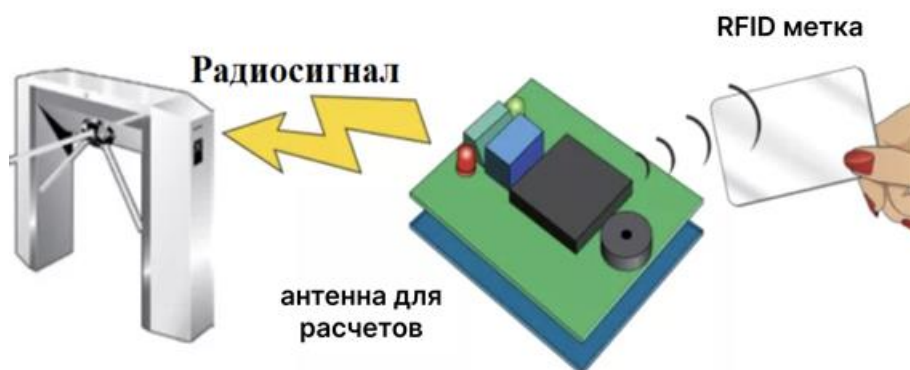


Рисунок 2.6 - Принцип работы RFID

Анти-коллизия. Необходимость в интерактивных системах возникла потому, что одновременно нужно было обрабатывать несколько идентификаторов. Например, когда кладовщик должен прочитать все этикетки на упаковке товара. В таких случаях не обойтись без антиколлизсионного механизма, который обеспечивает выборочную и поочередную обработку нескольких идентификаторов, одновременно находящихся в поле считывания. Без этого механизма сигналы идентификации накладывались бы друг на друга. В методе антиколлизии считывающее устройство идентифицирует все идентификаторы с помощью уникальных серийных номеров, а затем последовательно обрабатывает их.

Расшифровываемые идентификаторы. Каждому идентификатору нужен только свой уникальный номер, чтобы решить, впустить ли человека в комнату или посчитать коробки на поддоне. Однако существует большая группа задач, для которых требуется дополнительная информация на метке. В этом случае используются перезаписываемые идентификаторы с дополнительной энергонезависимой памятью для сохранения информации даже после

отключения питания. В зависимости от применения, объем этой памяти может составлять от нескольких десятков бит до нескольких килобайт.

Существует два основных определения технологии RFID:

- Бесконтактные идентификаторы (карты и ключи) - идентификаторы малого радиуса действия, обычно около 10 см, используемые в системах контроля доступа и транспортных приложениях;

- Экологические идентификаторы средней дальности (около 1,5 метров); используются для идентификации товаров и продуктов, особенно в логистике. Основные рабочие частоты: низкочастотный диапазон (125 или 134 кГц), среднечастотный диапазон (13,56 МГц) и высокочастотный диапазон (800 МГц... 2,45 ГГц). Характеристики этих стандартов приведены в таблице ниже.

Низкочастотный диапазон обычно используется в системах контроля доступа и для обнаружения животных и металлических предметов (например, пивных кегов).

В настоящее время наибольшей популярностью пользуется средняя полоса. Он используется в транспорте и подобных приложениях, требующих использования перезаписываемых карт. Основным стандартом является ISO 14443, и все смарт-карты производятся в соответствии с этим стандартом. Для меток среднего уровня применяются два стандарта: ISO 15693 и EPC. ISO 15693 в первую очередь выпускает перезаписываемые токены с довольно широкими функциональными возможностями. Электронный код товара (EPC) имеет простую структуру и является электронным эквивалентом штрих-кода.

Высокочастотный диапазон (800 МГц ... 2,45 ГГц) был разработан относительно недавно, но существующие стандарты на уровне излучения в этом диапазоне для пассивных идентификационных устройств составляют от 4 ... до 8 метров, что очень важно, например, для складов. В этой области доминируют два стандарта: ISO 18000 и EPC. Сегодня можно сказать, что стандарт EPC для средних и высоких частот является очень перспективным, особенно для логистических приложений.

Чтобы преодолеть технические трудности, связанные с разработкой международного стандарта RFID, основные производители систем RFID создали рабочую группу в рамках Международной организации по стандартизации (ISO) и Международного электротехнического комитета (IEC) для разработки международных стандартов на системы RFID для управления грузами. Подкомитет 31, в состав которого входит данная рабочая группа, занимается товарными штрих-кодами. Рабочая группа RFID разделена на четыре подгруппы: профили приложений, синтаксис данных, уникальная радиочастотная идентификация и радиointерфейс. Эти подгруппы занимаются разработкой международных стандартов по общим вопросам, связанным с использованием систем RFI, информационным содержанием радиометок и системой управления ими, общей системой уникальной идентификации радиометок и, наконец, правилами радиосвязи между радиометками и считывателем. Результатом работы этих подгрупп станет набор международных стандартов, которые будут комплексно решать все

вопросы, связанные с совместимостью компонентов системы RFI от различных производителей.

Преимущества технологии RFID:

- Технология RFID не требует подключения или прямой видимости;
- Метки RFID считываются быстро и точно (почти 100% идентификация);
- RFID можно использовать в агрессивных средах, метки RFID могут считываться грязью, краской, паром, водой, пластиком и деревом;
- Пассивные RFID-метки имеют практически неограниченный срок службы;
- Метки RFID несут большой объем информации и могут быть интеллектуальными;
- Метки RFID невозможно подделать;
- Метки RFID можно считывать и записывать.

Применение технологии RFID.

До недавнего времени системы RFID были более дорогими, чем бесконтактные системы идентификации по штрих-кодам. Однако технологические достижения в области маркировки позволили использовать их там, где раньше применялись штрих-коды. Сегодня системы маркировки могут успешно конкурировать по цене со штрихкодами. Технология RFID предлагает решения даже в оптически сложных условиях.

Чип RFID похож на штрихкод, который передает информацию на считывающее устройство или сканер. Печатные штрих-коды обычно считываются с помощью лазерного сканера, который требует прямого зрения для обнаружения и считывания информации. В случае RFID считывающее устройство может считывать закодированную информацию, даже если метка скрыта, например, когда она встроена в продукт или вшита в одежду. Маленькая метка RFID может содержать больше информации, чем штрихкод. Кроме того, в отличие от штрих-кодов, метки RFID могут передавать данные из различных упаковок, например, тележек или коробок с товарами.

Системы RFID в настоящее время используются в различных ситуациях, когда необходимо быстро и точно отслеживать, контролировать и регистрировать перемещение различных объектов. Типичные области применения включают:

- Электронный мониторинг входа и перемещения людей на объекте;
- Контроль за движением и продажей товаров и ценностей на производстве, складах (особенно универмагах), в магазинах, на складах;
- Автоматический сбор данных на железнодорожных линиях, платных дорогах, железнодорожных станциях и грузовых терминалах.
- Управление движением, планирование и маршрутизация, интенсивность расписания и оптимальный выбор маршрута;
- Общественный транспорт: управление движением, продажа билетов и оптимизация пассажирских перевозок;

- Электронные платежные системы для всех видов транспорта, включая управление платными дорогами, автоматический сбор платы за проезд, транзит и платные парковки.
- Охрана (вместе с другими техническими средствами аудиовизуального наблюдения);
- Системы безопасности и сигнализации транспортных средств.



Рисунок 2.7 - Области применения технологии RFID

Как уже упоминалось, RFID-метки-это пассивные устройства, состоящие из антенны, конденсатора и небольшого полупроводникового чипа. Новейшие технологии производства позволяют сегодня интегрировать эти компоненты в акриловую подложку, что снижает стоимость RFID-устройств и позволяет производителям прикреплять этикетки к таким изделиям, как обычные наклейки. Для использования RFID-тегов не требуются батарейки и, соответственно, не требуется техническое обслуживание. Они получают питание от сканера, используя индуктивную связь или технологии электромагнитной съемки.

2.3 Беспроводные сенсорные сети

С точки зрения инженера-электрика, датчик или преобразователь - это устройство, которое собирает информацию о физическом процессе или явлении и преобразует ее в электрические сигналы, которые можно обрабатывать, измерять и анализировать. Термин "физический процесс", используемый в данном определении "датчика", может представлять собой любую конкретную информацию, такую как температура, давление, свет, звук, движение, положение, поток, влажность, излучение и т.д.

Сенсорная сеть - это структура, состоящая из датчиков, вычислительных устройств и элементов связи, которая предназначена для обнаружения, наблюдения и реагирования на событие или явление. События могут быть связаны с физическим миром, промышленной средой, биологическими системами или вычислительной инфраструктурой (информационными технологиями), а контролирующая или наблюдающая организация может быть потребителем, правительством, гражданской, военной или промышленной компанией. Такие сенсорные сети могут использоваться для дистанционного зондирования, медицинской телеметрии, наблюдения, сбора данных и т.д.

Что такое беспроводная сенсорная сеть? Как уже упоминалось, обычная сенсорная сеть состоит из датчиков, контроллера и системы связи. Когда система связи реализована в сенсорной сети с использованием беспроводного протокола, такие сети называются беспроводными сенсорными сетями (Wireless Sensor Networks, WSN).

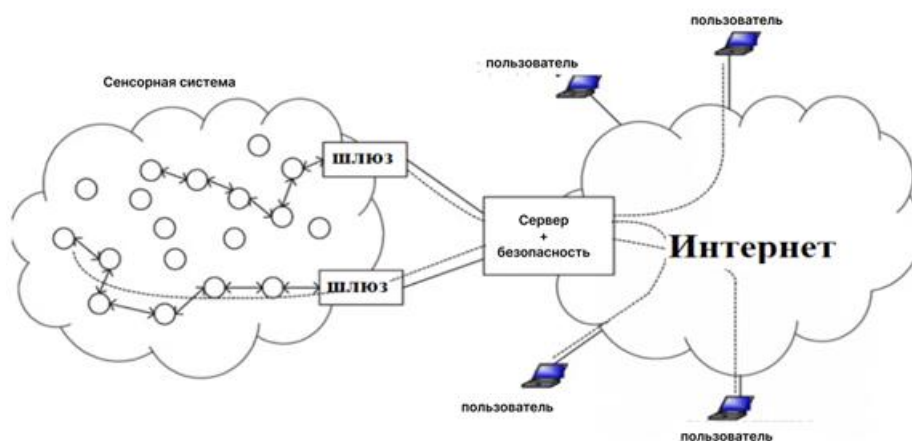


Рисунок 2.8 - Архитектура беспроводной сенсорной сети

Беспроводная сенсорная сеть очень плотная и часто состоит из множества сенсорных узлов, развернутых в большом количестве для поддержки зондирования, вычислений, встроенных вычислений и связи.

Последние достижения в области технологий, коммуникаций и сетей привели к появлению новых конструкций датчиков, информационных технологий и беспроводных систем. Эти современные датчики можно использовать в качестве моста между физическим и цифровым миром. Датчики используются во многих устройствах, отраслях промышленности, машинах и в окружающей среде для предотвращения повреждений и аварий в инфраструктуре, например, при защите природных ресурсов, сохранении дикой природы, повышении производительности, безопасности и т.д.

Структура беспроводной сенсорной сети. Типичную беспроводную сенсорную сеть можно разделить на две части: сенсорный узел и архитектура сети.

Беспроводная сенсорная сеть. Сенсорный узел WSN состоит из четырех основных компонентов: источника питания, датчика, вычислительного устройства и системы связи.

Датчик собирает аналоговые данные из физического мира, а АЦП преобразует эти данные в цифровые. Главный процессор, который обычно представляет собой микропроцессор или микроконтроллер, берет на себя интеллектуальную обработку данных и управление.

Система связи состоит из радиосистемы для передачи и приема данных, обычно это радиосистема малого радиуса действия. Поскольку все компоненты являются маломощными устройствами, для питания всей системы используется небольшая батарейка, например, CR-2032.

Вопреки своему названию, сенсорный узел состоит не только из сенсорного компонента, но и из других важных функций, таких как обработка данных, связь и устройства хранения. С помощью всех этих функций, компонентов и принадлежностей сенсорный узел отвечает за сбор данных из физического мира, анализ сети, корреляцию данных и интеграцию данных от другого датчика с собственными данными.

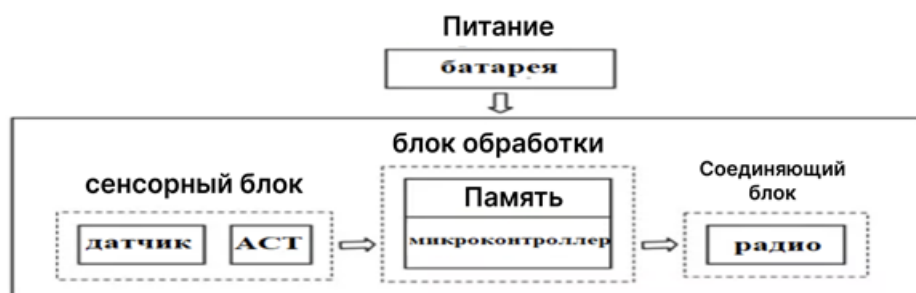


Рисунок 2.10 - Беспроводной узел сенсорной сети

Даже если большое количество сенсорных узлов развернуто на большой территории для совместного мониторинга физической среды, связь между сенсорными узлами не менее важна. В WSN сенсорный узел связан не только с другими сенсорными узлами, но и с базовой станцией посредством беспроводной связи.

Базовая станция посылает команды сенсорным узлам, а сенсорные узлы выполняют задачи посредством взаимной связи. Как только сенсорные узлы собирают необходимые данные, они отправляют их на базовую станцию.

Базовая станция также действует как шлюз к другим сетям через Интернет. После получения данных от сенсорных узлов базовая станция выполняет простую обработку данных и отправляет обновленную информацию пользователю через Интернет.

Когда все сенсорные узлы подключены к базовой станции, создается так называемая архитектура одноточечной сети. Хотя транспортировка на большие расстояния возможна, расход энергии на связь гораздо выше, чем на сбор данных и вычисления.

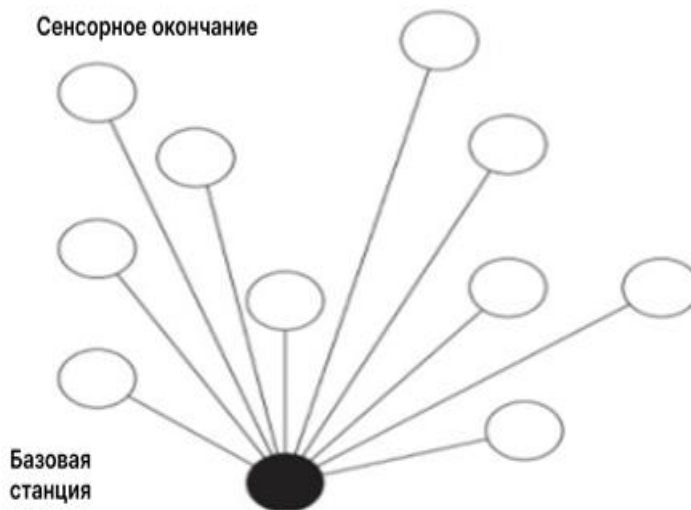


Рисунок 2.11 - Однослойная сетевая архитектура

Поэтому многослойная сетевая архитектура обычно используется в важных приложениях. Вместо одной линии связи между узлом датчика и базовой станцией данные передаются через один или несколько промежуточных узлов.

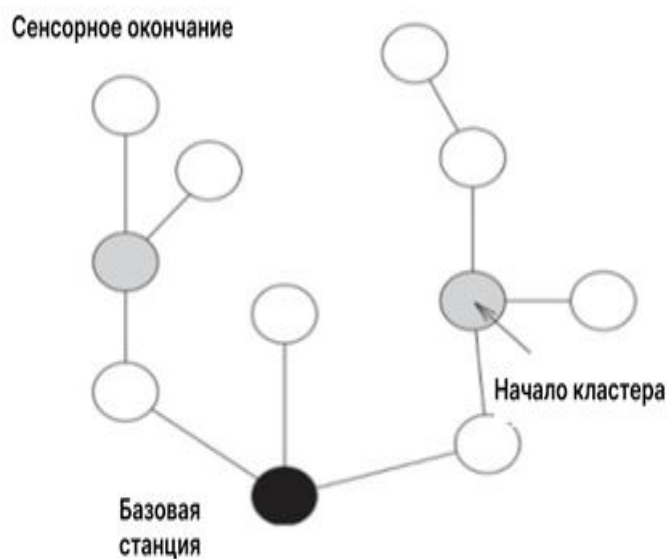


Рисунок 2.11 - Многослойная сетевая архитектура

Это можно осуществить двумя способами. Плоская сетевая архитектура и иерархическая сетевая архитектура. В плоской архитектуре базовая станция отправляет команды всем сенсорным узлам, но сенсорный узел с соответствующим запросом реагирует, используя свои равные узлы через многослойную строку.

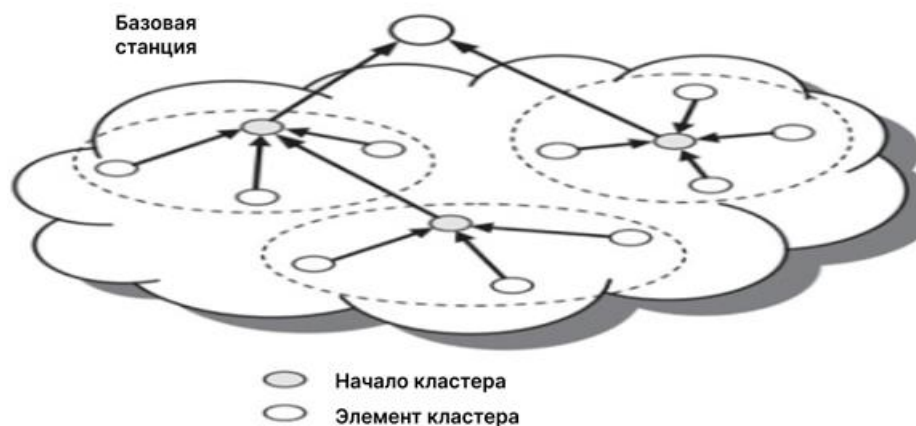


Рисунок 2.12 – Главы кластеров могут отправить данные на базовую станцию

В иерархической архитектуре группа сенсорных узлов создается как кластер, и сенсорные узлы отправляют данные своим соответствующим главам кластера. Затем главы кластеров могут отправить данные на базовую станцию.

Классификация беспроводных сенсорных сетей.

Беспроводные сенсорные сети сильно зависят от приложений и конфигурируются в соответствии с требованиями каждого приложения. Поэтому характеристики одной WSN будут отличаться от характеристик другой WSN.

Беспроводные сенсорные сети можно разделить на следующие категории независимо от сферы применения.

- Статические и мобильные WSN
- Детерминированные и недетерминированные сети WSN
- Одна базовая станция и несколько базовых станций
- со стационарными базовыми станциями и мобильными базовыми станциями
- Простые и многоугольные WSN
- Самоадаптивные и неадаптивные сети WSN
- Однородные и неоднородные сети WSN

Топология беспроводной сенсорной сети.

WSN может представлять собой сеть с одним или несколькими узлами. Ниже приведены некоторые из различных сетевых топологий, используемых в WSNs.

В топологии "звезда" имеется центральный узел, называемый концентратором или коммутатором, к которому подключены все узлы сети. Топология "звезда" очень проста в реализации, проектировании и расширении. Поскольку все данные передаются через концентратор, он играет жизненно важную роль в сети, и его отказ может привести к отказу всей сети.

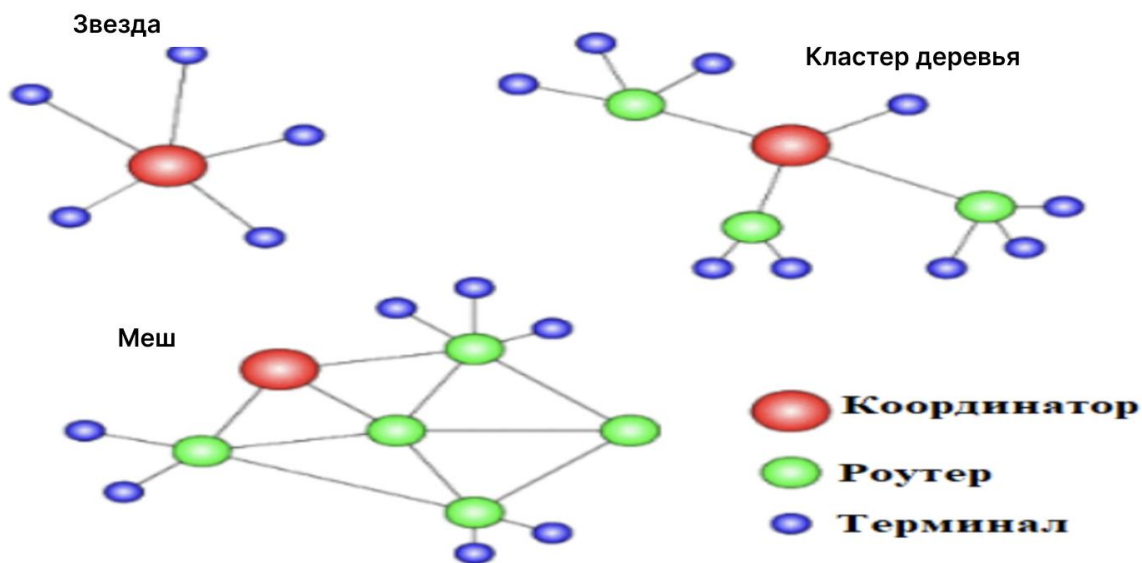


Рисунок 2.13 - Топология беспроводной сенсорной сети

Топология дерева - это иерархическая сеть с главным узлом на вершине, который связан со многими узлами на других уровнях и т.д. Вычислительная мощность и потребление энергии максимальны в корневом узле и снижаются по мере уменьшения иерархии.

В Mesh (топология сетки), каждый узел не только передает свои собственные данные, но и действует как ретранслятор, отправляя данные другим подключенным узлам. Топология Сетка далее делится на полные и частичные сетки. В топологии полной сетки каждый узел соединен со всеми другими узлами, а в топологии частичной сетки узел соединен с одним или несколькими соседними узлами.

2.4 Межмашинная связь M2M

Машины становятся умнее с каждым годом. Благодаря M2M машины научились обмениваться информацией, что значительно облегчило жизнь людей.

M2M (machine to machine) - это технология, которая позволяет машинам обмениваться информацией друг с другом или передавать информацию в одностороннем порядке. Сюда входят проводные и беспроводные системы для мониторинга датчиков и различных параметров оборудования, таких как температура, местоположение, уровень топлива и запасов и т.д.

Эти технологии активно используются в системах охраны и безопасности, здравоохранении, промышленных телеметрических системах, системах слежения и т.д.

Разница между M2M и IoT. M2M является частью концепции Интернета вещей (IoT). Однако IoT и M2M - это не одно и то же, но их часто обобщают. "IoT" - более широкое понятие (с точки зрения того, что подключается), а M2M - неотъемлемая часть IoT (как подключается, с помощью каких инструментов).

Обе технологии способствуют повышению эффективности и точности производственных процессов и могут оказать положительное влияние на общее качество жизни людей. M2M в какой-то степени стал основой IoT, но если в M2M информация может передаваться как беспроводным, так и проводным способом, то подключение к IoT всегда беспроводное.

Интернет вещей (IoT) - это система подключения интеллектуальных устройств к сетям для сбора данных, анализа и принятия решений. В отличие от этого, M2M - это система прямой связи между двумя устройствами.

Система M2M. Для обмена информацией между машинами используются проводные и беспроводные системы. Часто используются беспроводные технологии связи M2M. Его внедрение требует меньше ресурсов, денег и времени. Это быстрее, дешевле и удобнее. Однако, если беспроводные системы не могут быть использованы, необходимо использовать проводные системы. На производственном предприятии, заполненном сталью и бетоном, очень трудно получить сигнал беспроводной связи.

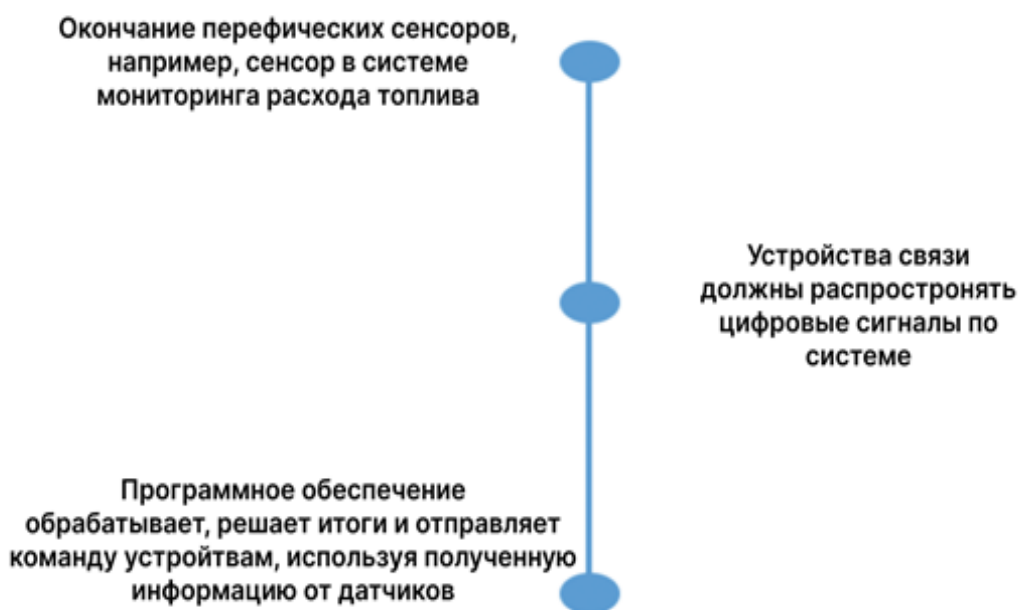


Рисунок 2.14 - Состав беспроводной системы M2M

В системах M2M информация передается через GSM, GPRS/EDGE, CSD, а также через спутник (ГЛОНАСС/GPS) - отслеживание транспорта и т.д.

Понятно, как работает M2M-связь, но каково ее значение в повседневной жизни? Пример использования умных технологий в жизни: если новый счетчик электроэнергии автоматически отправляет информацию о сожженных киловаттах поставщику услуг и вам не нужно звонить в регулирующий орган

или пить "чай", чтобы сравнить данные, значит, используется технология M2M системы IoT. Она работает практически без вмешательства человека, делая жизнь проще, удобнее, комфортнее и безопаснее. Конечно, передача данных со счетчиков - не единственное преимущество межмашинной связи.

Технологии M2M, IoT, сегодня широко используются - от беспроводного интернета и управления водителями до измерения температуры тела, давления и позиционирования пациентов, чтобы они не потерялись или не разлили топливо.

Возможности систем M2M облегчают жизнь во всех областях. И не только в жизни, но и в бизнесе: я говорю о сканировании товаров и выяснении количества остатков на складе - недостающих или потерянных, или об установке GPS-датчика в автомобиль и выяснении местонахождения водителя на карте города.

Системы M2M даже используются для создания "умных городов", делая жизнь в мегаполисах удобной и безопасной. Технология уже активно используется в Сингапуре, самом умном городе мира, а также в Копенгагене, Лондоне, Стокгольме, Цюрихе, Барселоне, Амстердаме, Женеве, Сан-Франциско, Чикаго, Нью-Йорке, Мельбурне, Токио, Сеуле и Берлине.

По предварительной информации, "умный город" принесет 10% дополнительных доходов в региональные бюджеты и сократит расходы на 15%.



Рисунок 2.15 - Разница между M2M и IoT

3 Расчет параметров сети LTE для IoT

3.1 Расчет бюджета потерь и зоны покрытия сетей GSM и LTE

Тип передаваемых данных – VoIP, скорость передачи: от 39,7 кбит/с. Δf системы: 10 МГц.

Высоты подъёма антенны абонентских станций 1.5 м, а базовых станций

30 и 50 м в городской и пригородной зоне соответственно.

Производится оценка зоны покрытия сети по моделям распространения Okumura–Hata и COST 231 – Hata.

Для LTE 1800 (город)

$$L = 45,5 - 13,82 \times \lg H_{\text{БС}} + 35,4 \times \lg F - (1,1 \times \lg F - 0,7) \times H_{\text{МС}} + (44,9 - 6,55 \lg H_{\text{БС}}) \times \lg R \quad (3.1)$$

$$R = 10^{\frac{L - 45,5 + 13,821 \lg H_{\text{БС}} - 35,41 \lg F + (1,11 \times \lg F - 0,7) H_{\text{МС}}}{(44,9 - 6,55 \times \lg H_{\text{БС}})}} \quad (3.2)$$

Для GSM 1800 и LTE 1800 (пригород):

$$L = 45,5 - 13,821 \times \lg H_{\text{БС}} + 35,4 \times \lg F - (1,1 \times \lg F - 0,7) \times H_{\text{МС}} + (44,9 - 6,55 \lg H_{\text{БС}}) \times \lg R$$

$$R = 10^{\frac{L - 45,5 + 12,921 \lg H_{\text{БС}} - 25,41 \lg F + (1,11 \times \lg F - 0,7) H_{\text{МС}}}{(44,9 - 6,55 \times \lg H_{\text{БС}})}}$$

Для GSM 900 и LTE 900 (город):

$$L = 74,52 - 13,82 \times \lg H_{\text{БС}} + 26,16 \times \lg F - 3,2[\lg(11,75 \times H_{\text{МС}})] + (44,9 - 6,55 \lg H_{\text{БС}}) \times \lg R \quad (3.3)$$

$$R = 10^{\frac{L - 74,52 + 13,821 \lg H_{\text{БС}} - 26,16 \lg F + 3,2(\lg 11,75 \times H_{\text{МС}})^2}{(44,9 - 6,551 \times \lg H_{\text{БС}})}} \quad (3.4)$$

Для GSM 900 и LTE 900 (пригород):

$$L = 63,35 - 13,82 \times \lg H_{\text{БС}} + 27,72 \times \lg F - 2 \left[\frac{\lg F}{28} \right]^2 + (44,9 - 6,55 \lg H_{\text{БС}}) \times \lg R - (1,1 \times \lg F - 0,7) \times H_{\text{МС}} \quad (3.5)$$

$$R = 10^{\frac{L - 63,35 + 13,82 \lg H_{\text{БС}} - 27,72 \lg F + 2 \left(\frac{\lg F}{28} \right)^2 + (1,1 \times \lg F - 0,7) \times H_{\text{МС}}}{(44,9 - 6,55 \times \lg H_{\text{БС}})}} \quad (3.6)$$

Допустимые потери составляют 149,2 дБ (GSM) и 155,1 дБ (LTE). Рассчитаем потери для LTE если известны радиус зоны покрытия R , км, высота подвеса антенны базовой $H_{\text{БС}}$, м и абонентской станций $H_{\text{МС}} = 1,5$ м.

$R = 3,2$ км; $H_{\text{БС}} = 50$ м; $H_{\text{МС}} = 1,5$ м; тип зоны покрытия – пригород.

$$L = 45,5 - 13,82 \lg 50 + 35,4 \lg F - (1,1 \times \lg 1800 - 0,7) \times 1,5 + (44,9 - 6,55 \lg 50) \times \lg 3,2 = 150 \text{ дБ}$$

Допустимые потери для LTE 155,5 дБ > 150 дБ, значит связь будет устойчивой.

3.2 Расчет восходящей линии (UL) LTE

Расчет восходящей линии (UL) состоит из нескольких этапов:

- расчет минимально допустимой мощности сигнала на входе приемника базовой станции;
- определение требуемой мощности принимаемого сигнала;
- расчет эффективно излучаемой мощности мобильной станции;
- определение максимально допустимых потерь.

3.2.1 Расчет минимально допустимой мощности сигнала на входе приемника базовой станции

Минимально допустимая мощность сигнала на входе приемника БС определяется из формулы (3.1):

$$P_{прбс}(\text{дБмВт}) = P_{ш}(\text{дБмВт}) + (E_b/N_0)_{\text{треб}}(\text{дБ}) - G_{обр}(\text{дБ}),$$

где $(E_b/N_0)_{\text{треб}}$ – требуемое значение E_b/N_0 ,

$G_{обр}$ – выигрыш от обработки,

$P_{ш}$ – мощность собственных шумов приемника.

Для анализа выбран тип оборудования БС Nokia Flexi WCDMA BTS. Коэффициент шума приемника данной базовой станции менее 3 дБ. Для расчета примем $K_{ш}=3$ дБ.

Мощность шумов приемника БС из (3.2):

$$P_{ш} = N + K_{ш} \quad (\text{дБмВт}). \quad (3.7)$$

Минимально допустимое значение E_b/N_0 на входе приемника для данного типа сервиса составляет 1.7 дБ при скорости абонента 3 км/ч.

Выигрыш от обработки составляет:

$$G_{обр} = 10 \log(R_{\text{чип}}/R_{\text{польз}}), \quad (3.8)$$

где $R_{\text{чип}}$ - чиповая скорость стандарта UMTS, чип/с,

$R_{\text{польз}}$ - скорость передачи данных пользователя, кбит/с.

Также необходимо учесть выигрыш за счет мягкого хендвера и запас на внутрисистемные помехи. Величину выигрыша примем равной $G_{хо}=2$ дБ. Величину запаса на внутрисистемные помехи определим из выражения (3.9). Величину относительной загрузки соты для начального расчета примем равной 50%. Допустимым значением величины относительной загрузки соты считается 50% [11].

Запас на внутрисистемные помехи равен:

$$M_{Int} = -10 \cdot \log_{10}(1-\eta) \quad (3.9)$$

С учетом вышеуказанных факторов, минимально допустимая мощность сигнала на входе приемника БС равна:

$$P_{прбс} = P_{ш} + (E_b/N_0)_{\text{треб}} - G_{обр} + L_n - G_{хо} \quad (\text{дБмВт}) \quad (3.10)$$

Рассчитаем минимально допустимую мощность сигнала на входе приемника базовой станции UMTS, если известны температура проводника, T° , тип линии (DL, UL), коэффициент шума приемника $K_{ш}$ (дБ), полоса согласованного фильтра приемника B (МГц), отношение средней энергии бита к спектральной плотности шума E_b/N_0 (дБ), чиповая скорость $R_{\text{чип}}$ (чип/с), скорость передачи данных пользователя $R_{\text{польз}}$ (кбит/с), загрузка соты - η .

$K_{ш}=3$ дБ, $E_b/N_0 = 1.7$ дБ, $R_{чип} = 3,84 \cdot 10^6$ чип/с, $R_{польз} = 384$ кбит/с, $\eta = 0,5$.

Мощность теплового шума в приемнике:

$$N = k \cdot T \cdot B = 1.38 \cdot 10^{-23} \cdot 293 \cdot 3.84 \cdot 10^6 = 1.55 \cdot 10^{-14} \text{ Вт},$$

$$N = 10 \cdot \lg(1.55 \cdot 10^{-14} / 0.001) = -108,2 \text{ дБмВт}.$$

Мощность шумов приемника БС из (3.2):

$$P_{ш} = N + K_{ш} = -108,2 + 3 = -105,2 \text{ дБмВт}.$$

Выигрыш от обработки составляет:

$$G_{обр} = 10 \log(R_{чип}/R_{польз}) = 10 \log(3,84 \cdot 10^6 / 384 \cdot 10^3) = 10 \text{ дБ}.$$

Запас на внутрисистемные помехи равен:

$$M_{Int} = -10 \cdot \log_{10}(1 - 0,5) = 3 \text{ дБ}.$$

Минимально допустимая мощность сигнала на входе приемника БС равна:

$$P_{прбс} = P_{ш} + (E_b/N_0)_{треб} - G_{обр} + L_n - G_{хо} = -105,2 + 1,7 - 10 + 3 - 2 = -112,5 \text{ дБмВт}.$$

3.2.2 Определение мощности принимаемого сигнала

Требуемая мощность принимаемого сигнала определяется выражением:

$$P_{пр} = P_{прбс} + L_{фидер} - G_{бс} + L_{фф} \text{ (дБмВт)}, \tag{3.11}$$

где $L_{фидер}$ - потери в фидере, дБ. Как правило, длина и тип фидера выбирается таким образом, чтобы значение затухания в нем составляла не более 3 дБ;

$G_{бс}$ – коэффициент усиления антенны базовой станции, дБ.;

$L_{фф}$ – запас на быстрые замирания, дБ.

Определяем требуемую мощности принимаемого сигнала, если известны потери в фидере $L_{фидер}$ (дБ), коэффициент усиления антенны базовой станции $G_{бс}$ (дБ), запас на быстрые замирания $L_{фф}$ (дБ). Значение мощности приемника

БС берется из предыдущей задачи.

$$L_{\text{фидер}} = 3 \text{ дБ}, G_{\text{бс}} = 18 \text{ дБ}, L_{\text{фф}} = 3 \text{ дБ. Тогда}$$

$$P_{\text{пр}} = P_{\text{прбс}} + L_{\text{фидер}} - G_{\text{бс}} + L_{\text{фф}} = -112,5 + 3 - 18 + 3 = -124,5 \text{ дБмВт.}$$

3.2.3 Расчет эффективно излучаемой мощности мобильной станции

Эффективно излучаемая мощность мобильной станции определяется выражением:

$$P_{\text{изМС}} = P_{\text{МС}} + G_{\text{БС}} - L_{\text{тело}} \text{ (дБмВт)}, \quad (3.12)$$

где $P_{\text{МС}}$ – мощность передатчика мобильной станции.

Для расчета взята минимальная мощность мобильной станции определенная стандартом (класс 4-21 дБмВт);

$G_{\text{БС}}$ – коэффициент усиления антенны базовой станции, принята равной 0 дБ;

$L_{\text{тело}}$ – потери на затухание в теле абонента. Для расчета $L_{\text{тело}}$ принимают равным 3 дБ.

Необходимо заметить, что потери на затухание в теле учитываются для голосовых типов услуг, и могут не учитываться для услуг по передаче данных.

Рассчитаем эффективно излучаемую мощность мобильной станции LTE, если известны мощность передатчика мобильной станции $P_{\text{мс}}$ (дБмВт).

Коэффициент усиления антенны базовой станции $G_{\text{мс}}$ (дБ), потери на затухание в теле абонента $L_{\text{тело}}$ (дБ) [12].

$$P_{\text{изМС}} = P_{\text{МС}} + G_{\text{БС}} - L_{\text{тело}} = 6 + 0 - 0 = 6 \text{ дБм Вт.}$$

3.2.4 Определение максимально допустимых потерь

Максимально допустимые потери на трассе равны:

$$L = P_{\text{изМС}} - P_{\text{пр}} \quad (3.13)$$

Определим максимально допустимые потери на трассе восходящей

линии LTE.

$$L = P_{изМС} - P_{пр.} = 6 + 146,46 = 152,46 \text{ дБмВт}$$

3.3 Расчет нисходящей радиолинии (DL) LTE

Данный расчет также осуществляется в несколько этапов:

- расчет минимально допустимой мощности сигнала на входе приемника МС;
- определение требуемой мощности принимаемого сигнала;
- расчет эффективно излучаемой мощности базовой станции;
- определение допустимых потерь на трассе.

3.3.1 Определение минимально допустимой мощности сигнала на входе приемника МС

Минимально допустимая мощность сигнала на входе приемника МС определяется аналогичным выражением (как и для БС):

$$P_{прмс}(\text{дБмВт}) = P_{ш}(\text{дБмВт}) + (E_b/N_0)_{\text{треб}}(\text{дБ}) - G_{обр}(\text{дБ}) \quad (3.14)$$

Приемник мобильной станции более простой, чем приемник БС, в нем используются более простые компоненты, следовательно, его коэффициент шума выше. Стандартом коэффициент шума приемника МС должен иметь значение < 9 дБ. Для расчета примем $K_{ш} = 8$ дБ.

Мощность собственных шумов приемника МС:

$$P_{ш} = N + K_{ш} \text{ (дБмВт)} \quad (3.15)$$

Минимально допустимая мощность сигнала на входе приемника МС с учетом запаса на внутрисистемные помехи и выигрыш от мягкого хэндовера равна:

$$P_{прМС} = P_{ш} + (E_b/N_0)_{\text{треб}} - G_{обр} - L_n - G_{хо} \text{ (дБмВт)}, \quad (3.16)$$

где $(E_b/N_0)_{\text{треб}}$ - минимально допустимое значение E_b/N_0 на входе приемника для данного типа сервиса составляет 4.8 дБ при скорости абонента 3 км/ч;

$$G_{обр} = 10 \log(R_{\text{чип}}/R_{\text{польз}});$$

$R_{\text{чип}}$ - чиповая скорость стандарта UMTS, чип/с;

$R_{польз}$ - скорость передачи данных пользователя. кбит/с;
 L_n – запас на внутрисистемные помехи. Примем что сота в нисходящей линии загружена также как и в восходящий. $L_n=3$ дБ;
 G_{xo} – выигрыш за счет мягкого хендовера, дБ.

Определяем минимально допустимую мощность сигнала на входе приемника МС, если известны температура проводника, T° , коэффициент шума приемника $K_{ш}$ (дБ), полоса согласованного фильтра приемника B (МГц), отношение средней энергии бита к спектральной плотности шума E_b/N_0 (дБ), чиповая скорость $R_{чип}$ (чип/с), скорость передачи данных пользователя $R_{польз}$ (кбит/с), загрузка соты - η .

$K_{ш}=8$ дБ ; $R_{чип}$ -чиповая скорость стандарта UMTS, $3,84 \cdot 10^6$ чип/с;

$R_{польз}$ - скорость передачи данных пользователя. 384000 бит/с;

L_n – запас на внутрисистемные помехи. Примем что сота в нисходящей линии загружена также как и в восходящий. $L_n=3$ дБ;

G_{xo} – выигрыш за счет мягкого хендовера, примем 2 дБ. Мощность собственных шумов приемника МС:

$$P_{ш} = N + K_{ш} = -108,2 + 8 = -100,2 \text{ дБмВт.}$$

Минимально допустимая мощность сигнала на входе приемника МС с учетом запаса на внутрисистемные помехи и выигрыш от мягкого хендовера равна:

$$P_{прМС} = P_{ш} + (E_b/N_0)_{треб} - G_{обр} - L_n - G_{xo} = -100,2 + 4,8 - 10 + 3 - 2 = -104,4 \text{ дБмВт,}$$

где $(E_b/N_0)_{треб}$ - минимально допустимое значение E_b/N_0 на входе приемника для данного типа сервиса составляет 4.8 дБ при скорости абонента 3 км/ч;

$$G_{обр} = 10 \log(R_{чип}/R_{польз}) = 10 \log(3,84 \cdot 10^6 / 384 \cdot 10^3) = 10 \text{ дБ.}$$

3.3.2 Определение требуемой мощности принимаемого сигнала

Требуемая мощность принимаемого сигнала определяется выражением:

$$P_{пр} = P_{прМС} + L_{тело} - G_{МС} + L_{ff} \text{ (дБмВт)}, \quad (3.17)$$

где $L_{тело}$ – потери на затухание в теле абонента.

Для услуг по передаче данных $L_{тело} = 0$;

G_{MC} – коэффициент усиления антенны мобильной станции, дБ. Значение G_{MC} принято равным 0 дБ;

L_{ff} – запас на быстрые замирания, дБ.

Расчитаем требуемую мощность принимаемого сигнала P_{np} для нисходящей радиолинии, если известны запас на быстрые замирания L_{ff} (дБ), коэффициент усиления антенны мобильной станции G_{MC} (дБ), потери на затухание в теле абонента $L_{тело}$ (дБ).

$$P_{np} = P_{npMC} + L_{тело} - G_{MC} + L_{ff} = -125,46 + 0 - 0 + 0 = -125,46 \text{ дБмВт}$$

3.3.3 Расчет эффективно излучаемой мощности базовой станции

Эффективно излучаемая мощность БС:

$$P_{изБС} = P_{БС} + G_{БС} - L_{фидер}, \text{ дБмВт},$$

где $P_{БС}$ – мощность передатчика базовой станции на кодový канал, дБ;

$G_{БС}$ – коэффициент усиления антенны базовой станции, дБ;

$L_{фидер}$ – потери обусловленные затуханием в фидере, дБ.

Определим эффективно излучаемую мощность базовой станции $P_{изБС}$ дБ, если известны мощность передатчика базовой станции на кодový канал $P_{БС}$ (дБ), коэффициент усиления антенны базовой станции $G_{БС}$ (дБ), потери обусловленные затуханием в фидере $L_{фидер}$ (дБ).

$$P_{изБС} = P_{БС} + G_{БС} - L_{фидер} = 50 + 17 - 2 = 55 \text{ дБмВт}$$

3.3.4 Расчет допустимых потерь на трассе

Допустимые потери на трассе

$$L = P_{изБС} - P_{np} - M_{Build}, \text{ дБ},$$

$$L = P_{изБС} - P_{np} - M_{Build} = 55 + 125,46 - 22 = 158,46 \text{ дБ}$$

где M_{Build} – запас на проникновение в помещение, дБ.

Типовые значения запаса на проникновение:

- 22 дБ в условиях плотной городской застройки;
- 17 дБ в условиях средней городской застройки;

- 12 дБ в условиях редкой застройки (в пригороде);
- 8 дБ в сельской местности (на открытой местности в автомобиле).

3.4 Расчет максимально допустимых потерь сети LTE

Максимально допустимые потери

$$LMARL = PEIRP - SRx + GRxA - LRxF - MBuild - MInt - MShade + GHO, \quad (3.18)$$

где P_{EIRP} – ЭИИМ передатчика, дБ;
 S_{Rx} – чувствительность приемника, дБ;
 G_{RxA} – коэффициент усиления антенны, дБи;
 L_{RxF} – потери в фидерном тракте, дБ;
 M_{Build} – запас на проникновение в помещение, дБ; M_{Int} – запас на внутрисистемные помехи, дБ; M_{Shade} – запас на затенение, дБ;
 G_{HO} – выигрыш от хендовера, дБ.

Запас на допустимые внутрисистемные помехи.

При расчете используется величина запаса на внутрисистемные помехи, которая характеризует возрастание мощности шума на входе приемника. Для расчета, принимают что запас на внутрисистемные помехи равен:

$$M_{Int} = -10 \cdot \log_{10}(1 - \eta), \quad (3.19)$$

где η – относительная нагрузка соты в восходящей или нисходящей линии.

Как видно, запас на внутрисистемные помехи это функция от загрузки соты, чем больше разрешенная нагрузка в соте, тем большую величину запаса необходимо учесть в расчете. При росте нагрузки до 100% запас на помехи стремится к бесконечности и зона обслуживания соты уменьшается до нуля. Зависимость значения данной величины от загрузки соты представлена на рисунке 3.1.

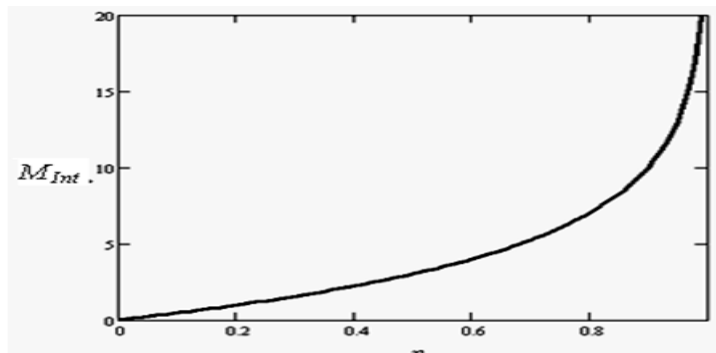


Рисунок 3.1 - Зависимость значения запаса на внутрисистемные помехи от значения относительной загрузки соты

Выигрыш за счет мягкого хэндовера.

Мягкий хэндовер имеет место в том случае, когда мобильная станция соединена как минимум с двумя сотами одновременно. В случае, если эти соты принадлежат двум разным базовым станциям(Node B), то объединение двух восходящих каналов осуществляется контроллером радиосети (RNC). В случае, если соты принадлежат одной базовой станции объединение сигналов осуществляется базовой станцией. В нисходящей линии объединение двух каналов осуществляется РАКЕ-приемником мобильной станции методом оптимального сложения. Можно рассматривать, как метод разнесенного приема, при использовании которого сигналы разных каналов складываются с учетом их весовых коэффициентов, а коэффициенты усиления в каждом канале прямо пропорциональны среднеквадратичному значению мощности сигнала и обратно пропорциональны среднеквадратичному значению мощности шума в этих каналах. При оптимальном сложении отношение сигнал/шум на выходе максимально. Выигрыш от мягкого хэндовера достигается за счет макро-разнесенного приема, следовательно уменьшает негативные эффекты от теневых зон и замираний. В реальной сети, зоны обслуживания большинства сот пересекаются. На границе соты мобильная станции может выбрать лучшую соту из доступных в данный момент, то есть мобильная станция не ограничена одним соединением. Это ведет к тому, что запас на замирания может быть снижен при расчете бюджета радиолинии, происходит уменьшение требуемого значения E_b/N_0 . Выигрыш от мягкого хэндовера зависит от условий распространения радиоволн. В городах, где замирания сигналов очень существенны, корреляция между сигналами, пришедшими от разных источников мала, как результат возрастает выигрыш от использования мягкого хэндовера. И наоборот в сельской местности, когда сигналы незначительно подвержены замираниям, корреляция между сигналами от разных источников возрастает, и выигрыш уменьшается. Величина выигрыша может меняться в пределах 2-5 дБ. Типичная величина выигрыша для расчета бюджета радиолинии составляет 2-3 дБ.

Ограничение управления мощностью или запас на быстрые замирания. Алгоритм быстрого управления мощностью введен в UMTS для того, чтобы поддерживать требуемое значение E_b/N_0 на входе приемника постоянным во время быстрых замираний, обусловленных многолучевостью. глубина замираний может доходить до 30 дБ. Быстрое управление мощностью особенно важно для абонентов имеющих малую скорость передвижения, так как они не могут быстро изменить свое положение для компенсации глубоких замираний. На границе соты, мощность передатчика мобильной станции максимальная, таким образом, не остается запаса на управление мощностью для компенсации быстрых замираний.

Для того, чтобы учесть этот процесс в расчете зададимся величиной запаса на быстрые замирания. Величина запаса на быстрые замирания зависит

от скорости абонента. Типичные значения величины запаса в зависимости от скорости абонента представлены в таблице 3.1.

Таблица 3.1 – Типичные значения величины запаса на быстрые замирания

| Тип абонента, скорость перемещения | Типичная величина запаса на быстрые замирания |
|------------------------------------|---|
| Небольшая скорость (3 км/ч) | 3-5 дБ |
| Средняя скорость (50 км/ч) | 1-2 дБ |
| Высокая скорость (120 км/ч) | 0.1 дБ |

Рассчитаем максимально допустимые потери L_{MARL} в сети LTE, если известны ЭИИМ передатчика:

- P_{EIRP} (дБ), чувствительность приемника - S_{Rx} , (дБ);
- коэффициент усиления антенны - G_{RxA} (дБи);
- потери в фидерном тракте - L_{RxF} , (дБ);
- запас на проникновение в помещение - M_{Build} , (дБ);
- запас на затенение - M_{Shade} , (дБ);
- выигрыш от хэндовера - G_{HO} (дБ);
- загрузка соты - η .

Типовые значения запаса на проникновение:

- 22 дБ в условиях плотной городской застройки;
- 17 дБ в условиях средней городской застройки;
- 12 дБ в условиях редкой застройки (в пригороде);
- 8 дБ в сельской местности (на открытой местности в автомобиле).

$$P_{EIRP} = 70 \text{ дБ}, S_{Rx} = -97,6 \text{ дБ}, G_{RxA} = 12 \text{ дБ}, L_{RxF} = 0,3 \text{ дБ}, \eta = 0,8, \\ M_{Build} = 17 \text{ дБ},$$

$$M_{Shade} = 9 \text{ дБ}, G_{HO} = 3 \text{ дБ}.$$

Определим запас на помехи M_{Int} , дБ

$$M_{Int} = -10 \cdot \log_{10}(1-\eta) = -10 \lg(1 - \eta) = -10 \lg 0,2 = 6,9 \text{ дБ}.$$

Максимально допустимые потери

$$L_{MARL} = 70 + 97,6 + 12 - 0,3 - 6,9 - 17 - 9 + 3 = 149,4 \text{ дБ}.$$

Допустимые потери для LTE 155,5 дБ > 149,4 дБ, значит связь будет устойчивой.

ЗАКЛЮЧЕНИЕ

В данном дипломном проекте были рассмотрены вопросы организации IoT технологий, их влияние на новые информационно-коммуникационные технологии и на корпоративные системы промышленного комплекса РК.

Произведен расчет параметров сети LTE для IoT, где рассчитан бюджет потерь и зоны покрытия беспроводных сетей связи, восходящая и нисходящая линия.

В целом цели и задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

- 1 Ashton K. Internet of things. RFID J.
- 2 Van Kranenburg R. The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID. The Netherlands, Amsterdam: Institute of Network Cultures, 2007.
- 3 Боронин, П. Н., & Кучерявый, А. Е. Интернет вещей как новая концепция развития сетей связи. Информационные технологии и телекоммуникации, 2(3),2014, 7.
- 4 Li Y., Hou M., Liu H., Liu Y. Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things // Inf. Technol. Manage. 2012. Vol. 13, No. 4.
- 5 Бекишева А.И., Салыкова М.С. Методические указания для выполнения экономической части выпускной работы. –Алматы: АУЭС, 2016. –24 с
- 6 Jia X., Feng O., Fan T., Lei Q. RFID technology and its applications in internet of things (IoT) // Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet). China, Yichang, 2012.
- 7 Sun C. Application of RFID technology for logistics on internet of things //AASRI Procedia. 2012. Vol. 1.
- 8 Ngai E. W. T., Moon K. K., Riggins F. J., Yi C. Y. RFID research: An academic literature review (1995–2005) and future research directions // Int. J. Prod. Econ. 2008. Vol. 112, No. 2.
- 10 Сайт об основных продуктах и оборудовании для IoT сети URL: <http://www.moog-crossbow.com/> (дата обращения 25.04.2017)
- 11 Сайт продажи профессионального IT оборудования URL: <http://www.appletech.kz/> (дата обращения 25.04.2018).
- 12 Сайт об основных продуктах и оборудовании мониторинга для IoT сети URL: <http://www.moog-crossbow.com/> (дата обращения 25.05.2018)

Отзыв руководителя

Дипломной работы

Алмуханова Жансая Кажмуханкызы

5B071900- Радиотехника, электроника және телекоммуникация

Тема Проектирование корпоративной сети на основе технологии IoT

В данном дипломном проекте были рассмотрены вопросы Интернет вещей, организации IoT технологий, их влияние на новые информационно-коммуникационные технологии и на корпоративные системы промышленного комплекса РК.

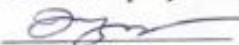
Приведены технологии Интернета вещей, технология LoRaWAN, радиочастотное обнаружение RFID.

Общие требования к составлению, изложению, оформлению и содержанию текстовых и графических материалов работы выполнены в соответствии с ГОСТ.

Дипломная работа выполнена на оценку 95/A/«отлично», а дипломант, Алмуханова Жансая достойна степени бакалавра специальности 5B071900- Радиотехника, электроника и телекоммуникации.

Научный руководитель

Ассоц.-профессор, к.т.н. каф.ЭТиКТ

 К.Х.Жунусов

«23» 05 2022 ж.

РЕЦЕНЗИЯ

на дипломную работу

Алмуханова Жансая Кажмуханқызы

5B071900- Радиотехника, электроника и телекоммуникации

Тема Проектирование корпоративной сети на основе технологии IoT

Интернет вещей - это совокупность физических объектов, подключенных к Интернету и взаимодействующих друг с другом и с внешней средой. Это понятие заимствовано из английского понятия Internet of Things (IoT).

Проведен анализ технологии IoT и показаны преимущества этой технологии.

В расчетном разделе были рассчитаны следующие параметры:

- сети LTE для IoT, где рассчитан бюджет потерь и зоны покрытия беспроводных сетей связи, восходящая и нисходящая линия.

Общие требования к составлению, изложению, оформлению и содержанию текстовых и графических материалов работы выполнены в соответствии с ГОСТ.

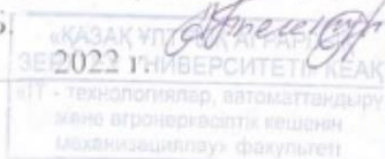
Дипломная работа выполнена на оценку 95/А/«отлично», а дипломант, Алмуханова Жансая достойна степени бакалавра специальности 5B071900- Радиотехника, электроника и телекоммуникации.

Рецензент

Кандидат технических наук, ассоциированный профессор КазНАИУ

Токмолдаев А. Б.

« 23 » мая



Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Алмуханова Жансая Кажмуханкызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Проектирование корпоративной сети на основе технологии IoT

Научный руководитель: Канат Жунусов

Коэффициент Подобия 1: 14.6

Коэффициент Подобия 2: 4.3

Микропробелы: 66

Знаки из других алфавитов: 151

Интервалы: 48

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

Обоснование:

Дата 23.05.2022

заведующий кафедрой



**Университеттің жүйе администраторы мен Академиялық мәселелер департаменті
директорының ұқсастық есебіне талдау хаттамасы**

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Алмуханова Жансая Кажмуханқызы

Тақырыбы: Проектирование корпоративной сети на основе технологии IoT

Жетекшісі: Канат Жунусов

1-ұқсастық коэффициенті (30): 14.6

2-ұқсастық коэффициенті (5): 4.3

Дәйексөз (35): 3.6

Әріптерді ауыстыру: 151

Аралықтар: 48

Шағын кеңістіктер: 66

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілісін.

Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

2022-05-20

Күні

Кафедра меңгерушісі



Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Алмуханова Жансая Кажмуханкызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Проектирование корпоративной сети на основе технологии IoT

Научный руководитель: Канат Жунусов

Коэффициент Подобия 1: 14.6

Коэффициент Подобия 2: 4.3

Микропробелы: 66

Знаки из других алфавитов: 151

Интервалы: 48

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

Обоснование:

2022-05-20

Дата



Сүңғат Марқсұлы

проверяющий эксперт