МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
имени Гумарбека Даукеева

Кафедра «Телекоммуникационные сети и системы»
Специальность: 6М071900 «Радиотехника, электроника и телекоммуникации»

ДОПУЩЕН К ЗАЩИТЕ
Зав. кафедрой
PhD, доцент Темырканова Э.К.
(ученая степень, звание, ФИО)

_____
(подпись)
«_____»_____2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: «Моделирование трафика IoT/M2M в системе MatLab»

Магистрант: Давлетов З.С. _____ группа МРЭТн 18-1
(Ф.И.О.) (подпись)
Руководитель: к.т.н., профессор _____ Туманбаева К.Х
(ученая степень, звание (подпись) (Ф.И.О.)

Рецензент_____ _____ _____
(ученая степень, звание) (подпись) (Ф.И.О.)

Консультант по ВТ к.т.н., профессор _____ Туманбаева К.Х
(ученая степень, звание) (подпись) (Ф.И.О.)

Нормоконтроль: _к.т.н., профессор _____ Туманбаева К.Х
(ученая степень, звание) (подпись) (Ф.И.О.)

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
имени Гумарбека Даукеева

Институт Космической Инженерии и Телекоммуникаций

Специальность: 6М071900 «Радиотехника, электроника и телекоммуникации»

Кафедра: «Телекоммуникационные сети и системы»

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистранту Давлетову Зинатдину Сырымовичу
(фамилия, имя, отчество)

Тема диссертации «Моделирование трафика IoT/M2M в системе MatLab»

Утверждена Ученым советом университета №122 от «25» откября 2018
Срок сдачи законченной диссертации «25» мая 2020г.
Цель исследования является моделирование и анализ трафика IoT/M2M

Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:

1. Анализ современного состояния сети IoT/M2M
2. Анализ и моделирование трафика ИВ
3. Моделирование трафика IoT/M2M в сети с протоколом MQTT

Перечень графического материала (с точным указанием обязательных чертежей)

Рисунок 3.1 - Структура модели издатель/подписчик
Рисунок 3.3 - Структура системы
Рисунок 3.7 - Имитационная модель для MQTT
Рисунок 3.11 - Время отклика системы: а)для приложений на основе событий (умная парковка) б)для приложений на основе участия (сигнал погоды)

Рекомендуемая основная литература

1. Тихвинский, Г.С. Бочечка, Б.И. Нургожин, А.З. Айтмагамбетов Сети IoT/M2M: технологии, приложения и регулирование. Алматы. «Ақ-Шағыл», 2016.

2. MatLab, "Discrete Event Simulation Software - SimEvents -Simulink," [Accessed 2019],http://www.mathworks.com/products/simevents/

Г Р А Ф И К
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1. Информационный обзор согласно теме	05.02.2020	
2. Анализ современного состояния сети IoT/M2M (теоретическая часть)	10.03.2020	
3. Исследование характеристик трафика приложений IoT	25.03.2020	
4. Анализ и моделирование трафика ИВ	05.04.2020	
5. Моделирование трафика IoT/M2M в сети с протоколом MQTT	20.05.2020	

Дата выдачи задания_30 сентября 2018г._____

Заведующий кафедрой _____ (Темырканова Э.К.)
(подпись) (Ф.И.О.)

Научный
руководитель диссертации _____ (Туманбаева К.Х.)
(подпись) (Ф.И.О.)

Задание принял к исполнению
магистрант _____ (Давлетов З.С.)
(подпись) (Ф.И.О.)

Аңдатпа

Бұл магистрлік диссертация Интернет заттарының және машина-машина өзара әрекеттесуінің (IoT / M2M) трафигін талдауға арналған. Жұмыста IoT / M2M трафиктің сипаттамалары мен қолданыста бар модельдеріне талдау берілген.

IoT / M2M трафиктің MQTT протоколына сәйкес желіде жұмыс істейтін ақырғы автоматтар трафигі ретінде аналитикалық модель әзірленген, және MATLAB ортасында имитациялық моделі жасалды. Ұсынылған модельдің тиімділігі бағаланады.

Аннотация

Данная магистерская диссертация посвящена анализу трафика Интернета вещей и межмашинного взаимодействия (IoT/M2M). В работе представлен анализ характеристик трафика и существующих моделей трафика IoT/M2M.

Разработана аналитическая модель трафика IoT/M2M как трафика конечных автоматов, работающих в сети по протоколу MQTT, и имитационная модель в среде MATLAB. Оценена эффективность предложенной модели.

Annotation

This master's work is devoted to analysis Internet of Thing’s traffic and machine interaction (IoT/M2M). The dissertation presents an analysis of traffic characteristics and existing IoT / M2M traffic models.

An analytical IoT / M2M traffic model, like traffic of state machines operating in the network under the MQTT protocol, and simulation model in the MATLAB environment are developed. The effectiveness of the proposed model is evaluated.

Содержание

Введение

В настоящее время взаимодействие между различными устройствами без вмешательства человека используется во многих отраслях, таких как энергетика, безопасность, транспорт и здравоохранение. Эти устройства передают данные в современные телекоммуникационные сети, создавая дополнительный трафик. Для обозначения таких соединений в телекоммуникационных сетях используется термин M2M (машина-машина). Поскольку сеть ИВ(IoT/M2M) продолжает набирать обороты в телекоммуникационных сетях, ожидается что в ближайшем будущем будет подключено и использовано очень большое количество устройств. Для надлежащего планирования и измерения сети используется модели трафика. Эти модели предназначены для точного сбора и прогнозирования свойств трафика IoT в сжатой форме.

MATLAB® и Simulink® могут помочь нам в разработке, создании прототипов и развертывании приложений IoT, таких как профилактическое обслуживание, оптимизация операций, диспетчерское управление и многое другое.

Сервисы управления для сетей межмашинной коммуникаций (M2M) и Интернета вещей (IoT), которые позволяют машинам обмениваться информацией друг с другом для реализации процедур и алгоритмов для автоматизированного управления производственными процессами, или передавать эту информацию без участия или с ограниченным участием человека, или с ограниченным вмешательство человека как конечного пользователя услуг M2M может предоставляться операторами сетей и услуг M2M / IoT.

Целью магистерской диссертации является моделирование и анализ трафика IoT/M2M.

Для достижения поставленной цели необходимо выполнить следующие задачи:

– провести анализ современного состояния сети межмашинного взаимодействия M2M;

– провести анализ особенностей трафика в сетях M2M;

– моделирование процесса обслуживания M2M трафика в мобильной сети с использованием системы имитационного моделирования MatLab;

– сравнительный анализ полученных результатов.

Практическая значимость работы заключается в том, что разработанные модели могут применяться при анализе обслуживания M2M трафика

1 Анализ современного состояния сети IoT/M2M

1.1 Технология Интернета вещей

При исследовании развития мобильных сетей пятого поколения неизменно возникает задача анализа технологии Интернета вещей (Internet of Things, IoT).

Современная сеть IoT не является строго стандартизированной. Для построения таких сетей используются несколько иная концепция чем стандартизированные телекоммуникационные сети. Чтобы анализировать трафик сети IoT предлагается несколько эталонных моделей этих систем [1].

Современная сеть IoT не стоит на одном месте, она всегда развивается и предлагаются более новые протоколы для требований этих интеллектуальных сетей. Ученые и инженеры по всему миру изучают реальные и компьютерные модели сети IoT для определения наилучших вариантов по ихпроизводительности. Оценка характеристик трафика моделей IoT дает представления о принципе работы каждого из IoT устройств и применения их в какой-то важной сфере из деятельности.

Устройства IoT оснащены встроенными датчиками, исполнительными механизмами, процессорами и трансиверами. IoT - это не единственная технология – скорее это агломерация различных технологий, которые работают вместе в тандеме. *Датчики* и *исполнительные механизмы* - это устройства, которые помогают во взаимодействии с физической средой. Данные, собранные *датчиками*, должны храниться и обрабатываться разумно, чтобы извлечь из них полезные выводы. Мы широко определяем термин «*датчик*», так как оно может быть - мобильным телефоном или светильником, если они предоставляют информацию о своем текущем состоянии (внутреннее состояние и окружающая среда). *Исполнительный механизм* - это устройство, которое используется для изменения окружающей среды, например, регулятор температуры кондиционера.

Хранение и обработка данных могут быть выполнены на границе самой сети или на удаленном сервере. Если возможна какая-либо предварительная обработка данных, то это обычно делается либо на датчике, либо на каком-либо другом ближайшем устройстве. Обработанные данные затем обычно отправляются на удаленный сервер. Возможности хранения и обработки объекта IoT также ограничены доступными ресурсами, которые часто очень ограничены из-за ограничений размера, энергии, мощности и вычислительных возможностей. В результате основная исследовательская задача состоит в том, чтобы обеспечить получение правильных данных с желаемым уровнем точности. Наряду с проблемами сбора и обработки данных существуют и проблемы в связи. Связь между устройствами IoT в основном беспроводная, поскольку они обычно устанавливаются в географически разнесенных местах. Беспроводные каналы часто имеют высокий уровень искажений и ненадежны. В этом сценарии надежная передача данных без слишком большого

количества повторных передач является важной проблемой, и поэтому технологии связи являются неотъемлемой частью изучения устройств IoT.

IoT – это некая сеть устройств-вещей, которые организуются сами между собой, без влияния человека. То есть это возможно только при хорошем программном обеспечении и при достаточным ресурсе сетевого трафика. Сети IoT могут иметь различные конфигурации и объемы в зависимости от его назначения.

Главное отличие сети Интернета вещей от обычных телекоммуникационных сетей заключается в следующем:

– очень большое количество подключаемых к сети устройств;

– требование низкого энергопотребления;

– ограниченные вычислительные ресурсы этих устройств, то есть они все должны соединяться по требованию к некоторому серверу и обеспечиваться непрерывной связью.

В сетях малого радиуса действия используются беспроводные технологии, которые обмениваются данными на расстоянии от нескольких сантиметров до сотен метров. К ним относятся технологии бесконтактной передачи данных с близкого расстояния, беспроводные персональные сети (WPAN), а также беспроводные локальные сети (WLAN). Это такие технологии как: RFID, NFC, BLE, Ant, EnOcean, Z-Wave, Insteon, ZigBee, MiWi, DigMesh, WirelessHart, 6LowPAN, WiFi [2].

В сетях большой дальности используется беспроводная технология, способная передавать сообщения на десятки километров, чтобы охватить большие площади. Маломощные глобальные сети (LPWAN) представляют собой специализированный тип сетевых технологий, предназначенных для соединения устройств в стесненных условиях, с акцентом на энергоэффективность и покрытие на большие расстояния. Различают нелицензированный и лицензированный LPWAN в соответствии с назначенными полосами частот. Среди них нелицензированные: LoRaWAN, Symphony Link, Weightless, SIGFOX, DASH7. Лицензированны: eMTC, NB-IoT, EC-GSM-IoT. Перечисленные технологий иллюстрируют нам что сети IoT это на одна отдельная вещь, а совокупность всех этих технологий в соответствии с рисунком 1.1 [3].

Уже в этом году на планете используются более 50 млрд устройств которые частично подключены к сетям, и беспроводным технологиям как Wi-Fi (стандарт IEEE 802.11), ZigBee (стандарт IEEE 802.15.4), Bluetooth (стандарт IEEE 802.15.1), 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), итд. Разработчики этих технологий дали возможность сетям использовать все его возможности. Например, стандарт IEEE 802.11ah расширения стандарта IEEE 802.11 с применением разработки энергоэффективного протокола[4] представлен в Приложении А.

Среди проводных технологий важную роль в проникновении «интернета вещей» играют решения PLC — технологии построения сетей передачи данных по линиям электропередачи, так как во многих приложениях

присутствует доступ к электросетям (например, торговые автоматы, банкоматы, интеллектуальные счётчики, контроллеры освещения изначально подключены к сети электроснабжения). Так и над PLC, будучи открытым протоколом, стандартизуемым IETF, отмечается как особо важный для развития «интернета вещей»

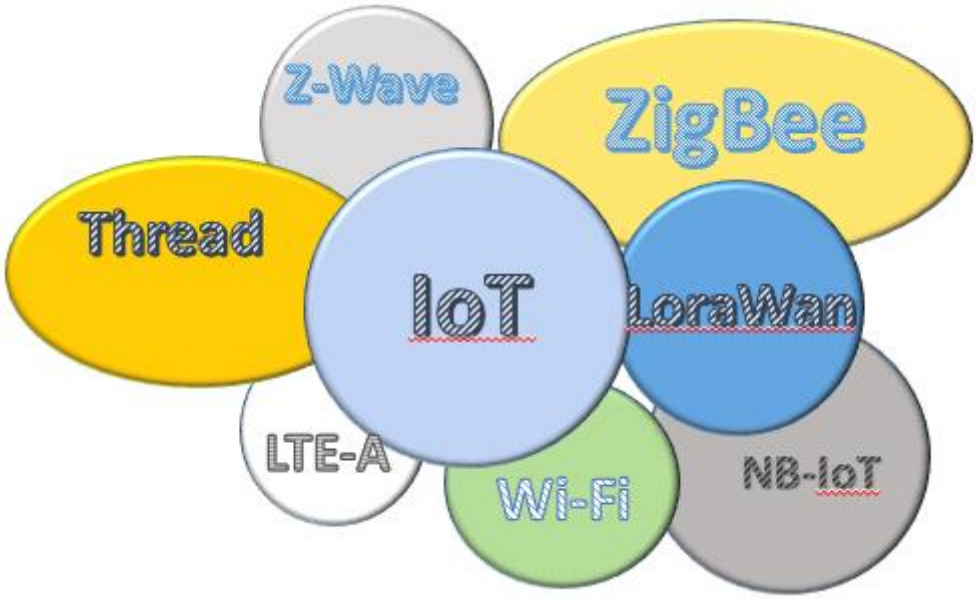


Рисунок 1.1 – Технологии IoT

Стандарт IEEE 802.15.4 (ZigBee) нацелен, основным образом, на применение в качестве средства связи среди самостоятельных устройств и оборудования. На производстве они могут быть использованы в складских организациях, при автоматизации технологических процессов устройствами Интернета вещей могут быть разнообразные измерители, детекторы, сервоприводы, электрические метки. В бытовых условиях устройствами Интернета вещей могут служить индивидуальные персональные компьютеры, игровые приставки, датчики безопасности, освещения, кондиционирования, радиофицированные игрушки[5].

Bluetooth Low Energy (BLE) (версия традиционного Bluetooth) нацелен на использование при сборе данных и мониторинга с автономным питанием. BLE, равно как обыкновенный Bluetooth, функционирует в не лицензируемом спектре 2.4 – 2.483 ГГц. Выходная мощь передатчиков BLE равна 0 дБ (1 мВт), в данном стандарте наибольшее расстояние взаимосвязи равно 50 м. при применении известных топологий «точка-точка» и «звезда»[6].

С целью решения задачи снижения энергопотребления, а также задачи конвергенции сетей доступа со сетями IP, был выработан и активно формируется эталон 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks). Концепция 6LoWPAN возникла из идеи, что «Интернет-протокол может и должен применяться даже к самым маленьким устройствам», и что

устройства с низким энергопотреблением с ограниченными возможностями обработки должны иметь возможность участвовать в Интернете вещей.

Реализовать IoT концепцию в практике возможно в рамках одного здания, квартала, компании, однако по причине недоступности стандартов существующих в настоящий период определенных технологий, создание массовых сетей нереально. Другими словами, в настоящее время Интернет вещей – это никак не стандартизованная теория, какой некогда была также глобальная паутина сетей.

Тем не менее, международными телекоммуникационными организациями и объединениями уже сейчас предлагаются различные варианты построения и взаимодействия концепций IoT. Например, МСЭ (Международный Союз Электросвязи) с целью решения задачи типизации концепций IoT МСЭ-Т создал IoT-GSI (Global Standards Initiative on Internet of Things) – глобальная инициатива по стандартизации сети Интернета вещей, что помимо остального дает иерархическую модель построения интеллектуальных систем.

По причине своеобразных условий для интеллектуальных сетей, были изобретены новейшие или же изменены ранее имеющиеся протоколы. Среди более популярных, протоколы HTTP/HTTPS (RESTful), MQTT, CoAP, QUIC [7].

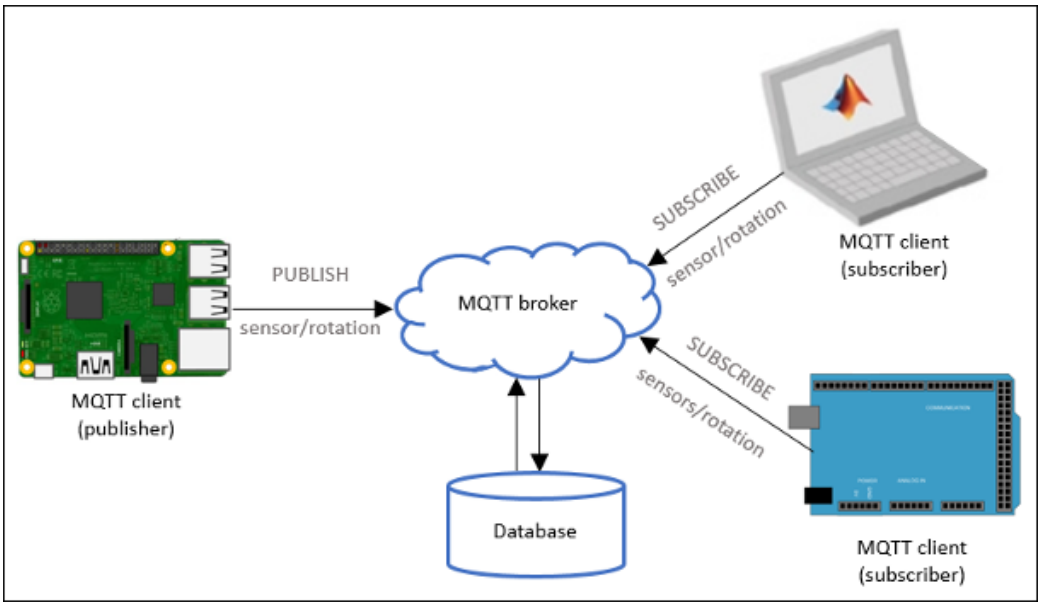


Рисунок 1.2 – Реализация протокола MQTT[11]

MQTT (Message Queue Telemetry Transport) – протокол обмена уведомлениями среди устройств согласно принципу публикатор-абонент, который работает сверху протокола TCP. Это соглашение было основано с целью применения в сетях с невысокой полосой пропускания, в сетях с значительной задержкой или низкой надежности. В рисунке 1.2 приведен реализация работы протокола MQTT посредством использования программы

Matlab с чипами ESP8266 [8, 9]. Этот микроконтроллер изначально не предназначалось для широкого использования, но посредством роста технологий Интернета вещей оно стало актуальном среди исследователей, так как у него есть возможность контролировать прибор подключенные к одной сети Wi-Fi. MQTT простой протокол работающий поверх TCP/IP. Существуют большие количества IoT приложений верхнего уровня для Android, iOS и других платформ, поддерживающих этот протокол [10].

CoAP (Constrained Application Protocol) – протокол прикладного уровня, который работает в базе REST (Representational State Transfer) стандартов. Протокол CoAP считается двоичным также функционирует сверху UDP, в отличие от HTTP. Этот протокол используется устройствами и сетями с ограниченными ресурсами. Для наглядности в рисунке 1.3 приведен различия между протоколами.

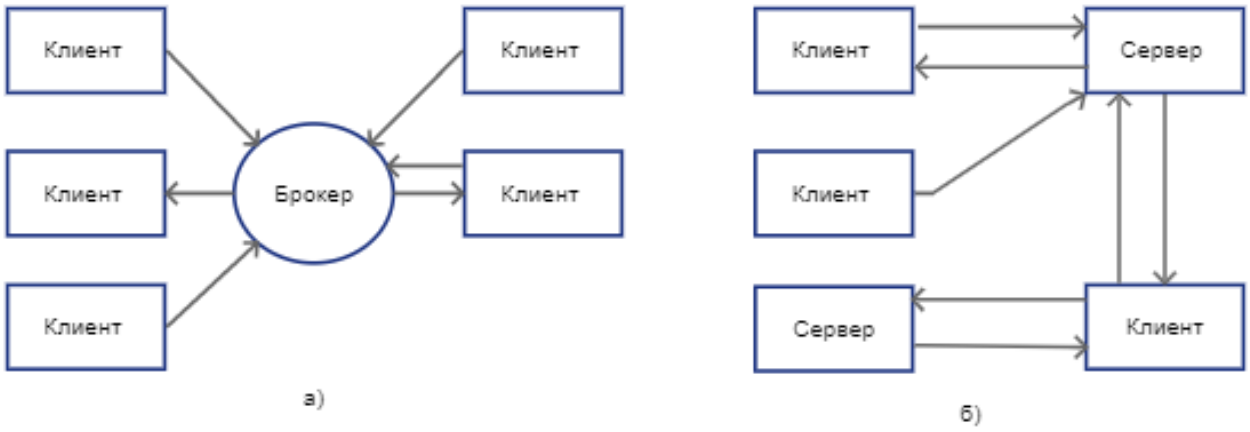


Рисунок 1.3 – Общее представления моделей MQTT(а) и CoAP(б)

Расширенный протокол очереди сообщений (AMQP) - это протокол открытого прикладного уровня для промежуточного программного обеспечения, ориентированного на сообщения. AMQP - это двоичный протокол прикладного уровня, разработанный для эффективной поддержки широкого спектра приложений обмена сообщениями и шаблонов связи. Он обеспечивает управляемую потоком коммуникацию, ориентированную на сообщения, с гарантиями доставки сообщений, такими как, самое большее, один раз (когда каждое сообщение доставляется один или никогда), по крайней мере, один раз (где каждое сообщение обязательно будет доставлено, но может делать это несколько раз) и ровно один раз (когда сообщение всегда будет приходить и делать это только один раз), и аутентификацию TLS . Он предполагает базовый надежный протокол транспортного уровня, такой как протокол управления передачей (TCP).

Телекоммуникационная сеть обязана совершенствоваться таким образом, чтобы обеспечить все без исключения нужные требования с целью практического использования концепции «Интернета вещей». Одним из таких

условий следует рассматривать обслуживание мультисервисного трафика с установленными качественными показателями. Данный трафик возможно анализировать как результат сложения двух компонентов, представляющих потоки IP-пакетов различной натуры. Первый компонент иногда именуют трафиком людей (пользователем, как правило, становится индивид), второй – трафик вещей, создаваемый при осуществлении концепции IoT. Свойства первого компонента стремительно исследуются экспертами согласно теории телетрафика на основе теоретических моделей и результатов измерений в эксплуатируемых мультисервисных сетях. Исследование второго компонента усложняется тем, что до сих сложно давать прогноз характеру увеличения трафика IoT с необходимой достоверностью. Это объясняется недостаточным объемом статистических данных, но эту задачу можно решить используя имитационное моделирование. Подобным методом можно исследовать мультисервисный трафик, в состав которого входят данные, формируемые оконечными устройствами IoT[12].

Основным значительным трендом IoT в последние годы является взрывной рост числа устройств, подключенных и контролируемых Интернетом. Широкий спектр приложений для технологии IoT означает, что специфика может сильно отличаться от одного устройства к другому, но есть основные характеристики, присущие большинству из них.

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

Группу технологий, основанных на подключении приложений Интернета вещей к узкополосной сети связи, имеющую низкую мощность излучения и зону действия с радиусом до нескольких километров, обозначают LPWAN.

К этой группе относится технология LoRa WAN (Long Range Wide Area Networks), представленная в 2015 году компанией Semtech и исследовательским центром IBM Research. Для поддержки, развития и стандартизации данной технологии был создан альянс LoRa (LoRa Alliance), который в настоящее время стремительно развивается, о чём говорит постоянное увеличение количества зарегистрированных членов. В состав альянса входят как известные производители электроники: Cisco, IBM, Kerlink, IMST, Semtech, Microchip Technology, - так и ведущие телекоммуникационные операторы (Bouygues Telecom, KPN, SingTel, Proximus, Swisscom)[13].

Технология LoRa основывается на двух главных элементах[14]:

– радиоинтерфейсе физического уровня, который определяет все характеристики передачи радиосигналов между шлюзами сети и оконечными устройствами;

– сетевой архитектуре (рисунок 1.4), в которую входят IoT/M2M устройства, шлюзы, сетевые серверы, подключенные к Интернет, и серверы приложений.

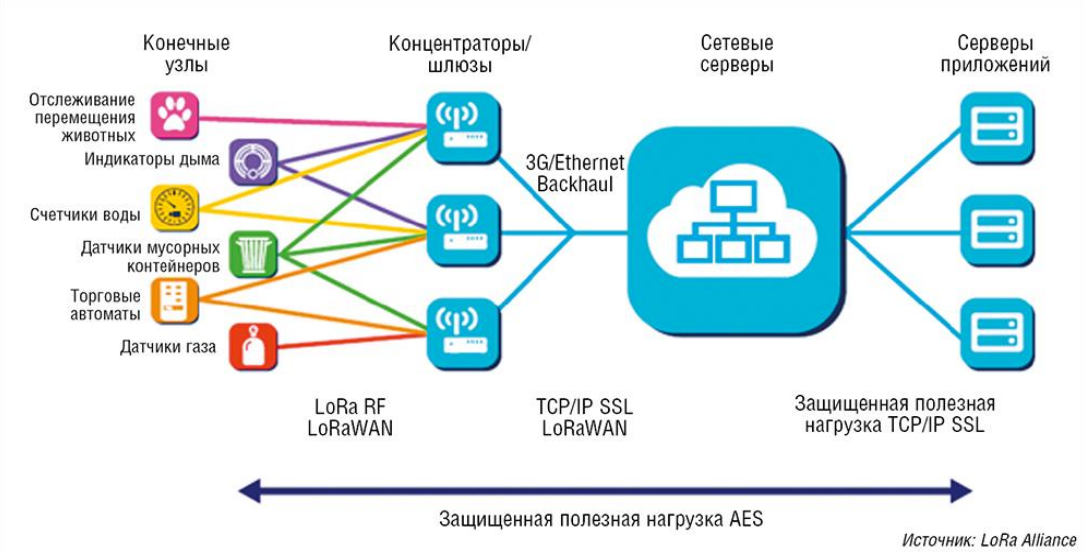


Рисунок 1.4 – Архитектура сети LoRa

Первое, что нужно понять, это то, что LPWAN (маломощная глобальная сеть) не является стандартом. Это широкий термин, охватывающий различные реализации и протоколы, как собственные, так и с открытым исходным кодом, которые имеют общие характеристики, как следует из названия:

– низкое энергопотребление: работает на небольших недорогих батареях в течение многих лет;

– широкая область: имеет рабочий диапазон, обычно более 2 км в городских условиях.

Физическим ограничением для достижения низкой мощности и широкого диапазона является небольшой размер данных. Большинство технологий LPWAN могут отправлять только менее 1000 байтов данных в день или менее 5000 бит в секунду.

В таблице 1.1 приведены все технологии по диапозону их работоспособности в сравнении с LPWAN.

Как видно из таблицы 1.1 характеристики LPWAN делают его отличным выбором для следующих классов приложений IoT:

– для интеллектуального освещения, интеллектуальных сетей при плотном расположении (города или большие здания);

– для долгосрочного мониторинга датчиков и счетчиков, которые будут устанавливаться и контролироваться в течение длительного периода времени (например, счетчики воды, детекторы газа, интеллектуальное сельское хозяйство и удаленные дверные замки).

Проще говоря, технология LPWAN хорошо работает в ситуациях, когда устройствам необходимо отправлять небольшие данные по широкой области,

сохраняя при этом срок службы батареи в течение многих лет. Это отличает LPWAN от других протоколов беспроводной сети, таких как Bluetooth, RFID.

Таблица-1.1 – Виды технологий IoT

Дальность применения	Технология	Описание
Беспроводная связь малого радиуса действия	Bluetooth mesh networking	Спецификация, обеспечивающая вариант ячеистой сети для Bluetooth с низким энергопотреблением (BLE) с увеличенным числом узлов и стандартизированным прикладным уровнем (Модели).
	Light-Fidelity (Li-Fi)	технология беспроводной связи, аналогичная стандарту Wi-Fi, но использующая связь в видимом свете для увеличения пропускной способности
	NFC	протоколы связи, позволяющие двум электронным устройствам обмениваться данными в диапазоне 4 см.
	RFID	технология, использующая электромагнитные поля для считывания данных, хранящихся в тегах, встроенных в другие элементы.
	Wi-Fi	технология для локальных сетей, основанная на стандарте IEEE 802.11 , где устройства могут обмениваться данными через общую точку доступа или напрямую между отдельными устройствами.
	ZigBee	протоколы связи для персональных сетей на основе стандарта IEEE 802.15.4, обеспечивающие низкое энергопотребление, низкую скорость передачи данных, низкую стоимость и высокую пропускную способность.
	Z-Wave	протокол беспроводной связи, используемый в основном для домашней автоматизации и безопасности[15].
Беспроводная связь средней дальности	LTE-Advanced	спецификация высокоскоростной связи для мобильных сетей. Обеспечивает усовершенствования стандарта LTE с расширенным покрытием, более высокой пропускной способностью и меньшей задержкой[16].

Продолжение таблицы 1.1

Дальность применения	Технология	Описание
Беспроводная связь средней дальности	5G	5G можно использовать для достижения высоких требований к IoT для связи и подключения большого количества устройств IoT, даже когда они находятся в движении[17].
Беспроводная связь на большие расстояния	LPWAN	беспроводные сети, предназначенные для обеспечения связи на большие расстояния с низкой скоростью передачи данных, снижения мощности и стоимости передачи.
	VSAT	технология спутниковой связи, использующая небольшие антенны для узкополосных и широкополосных данных.
	NB-IoT	стандарт сотовой связи для устройств телеметрии с низкими объёмами обмена данными. Разработан консорциумом 3GPP в рамках работ над стандартами сотовых сетей нового поколения.
	RPMA	Эта технология предлагает такие функции, как низкое энергопотребление, отдельный широковещательный канал для быстрых обновлений встроенного ПО, превосходный встроенный диапазон и 128-разрядное шифрование AES для различных приложений IoT.
Проводная связь	Ethernet	сетевой стандарт общего назначения, использующий витую пару и оптоволоконные каналы в сочетании с концентраторами или коммутаторами .
	PLC	технология связи, использующая электропроводку для передачи энергии и данных. Такие спецификации, как HomePlug или G.hn, используют ПЛК для сетевых устройств IoT.

Сотовые сети страдают в основном от плохого времени автономной работы и могут иметь пробелы в покрытии. Еще одна трудность связана с технологическим закатом (когда технология преднамеренно прекращается): в США 30 миллионов конечных точек 2G остались без связи. Многие из устройств IoT должны оставаться в сети в течение 10 лет[8].

В настоящее время ведутся исследования технологий LTE-M, NB-IoT, EC-GSM и 5G IoT, но ни одна из них не является кросс-совместимой, и пока

не решено, подойдут ли они для долгосрочных решений IoT. Первые версии LTE-M в настоящее время разрабатываются AT & T и Verizon.

Ячеистые сети, такие как ZigBee, используются в приложениях IoT. На самом деле, многие системы домашней автоматизации используют ZigBee, но ZigBee не идеально подходит для приложений LPWAN. Ячеистые сети полезны только на средних расстояниях и не обладают возможностями дальнего действия технологий LPWAN.

Что еще более важно, ячеистые сети не работают от батареи, поскольку каждый узел должен постоянно принимать и повторять соседние радиосигналы. Когда датчики масштабируются до тысяч, ZigBee или другие ячеистые сети не соответствуют потребностям приложений LPWA.

LTE-M и Narrowband-IoT (NB-IoT) являются многообещающими дополнениями к пространству LPWAN. LTE-M – это реакция Партнерского проекта третьего поколения (широко известная как « 3GPP») на интенсивный интерес к решениям LPWAN, поддерживающим стандартное подключение LTE при сохранении ресурсов. NB-IoT – это еще одна конструкция 3GPP, противодействующая нарушению работы Sigfox и LoRa Alliance (ниже), однако NB-IoT отличается от LTE-M тем, что работает вне конструкции LTE.

Одно большое преимущество NB-IoT связано с его более простой формой сигнала: технология потребляет минимальную мощность. Еще одним большим преимуществом является стоимость. Благодаря выбору наборов микросхем, специально разработанных для протоколов NB-IoT, которые имеют более простую конструкцию, общая стоимость компонентов снижается. Наконец, NB-IoT имеет потенциальные преимущества для приложений умного города. LinkLabs предсказывает, что NB-IoT может иметь лучшее проникновение в здания по сравнению с LTE-M. С другой стороны, развертывание в США будет затруднено из-за повсеместного распространения LTE, и поскольку микросхемы, которые также включают LTE-M, зачастую непомерно дороги, вам придется выбирать. Но часто это зависит от вашего конкретного случая использования; NB-IoT, вероятно, лучше всего подходит для статических активов, таких как интеллектуальные счетчики, тогда как LTE-M имеет преимущества в роуминговых приложениях, таких как транспортные средства или дроны[18].

LTE-M имеет заметные преимущества. Во-первых, скорость передачи данных выше, что важно для сценариев с большим количеством данных. И в отличие от NB-IoT, интерфейс довольно прост. Однако, помимо того, что LTE является в первую очередь технологией США, необходимо учитывать и другие ограничения. С одной стороны, все еще ощущается эффективность энергопотребления с LTE-M[19].

1.2 Архитектура сети межмашинных коммуникаций

Архитектура системы IoT, в ее упрощенном виде, состоит из трех уровней:

– уровень 1: устройства;

– уровень 2: пограничный шлюз;
– уровень 3: облако.

К устройствам относятся сетевые устройства, такие как датчики и исполнительные механизмы, имеющиеся в оборудовании IoT, особенно те, которые используют протоколы, такие как Modbus , Bluetooth , Zigbee или собственные протоколы, для подключения к пограничному шлюзу. Мир вещей относится к микроэлектромеханическим системам, интеллектуальным датчикам, простым интерфейсам человек-машина (ЧМИ) и т. Д., Которые объединяются в сети (Сети вещей, NoT) для повсеместного взаимодействия с другими вещами, окружающей средой и / или людьми. NoT обычно представляют собой экосистемы с ограниченными ресурсами, как правило, со средним временем задержки доступа, высокой частотой ошибок, низкой пропускной способностью данных и ограниченным временем в сети, где потребление энергии должно быть оптимизировано до максимума. В упрощенной модели вещи выделяются основные блоки связи, вычислений и взаимодействия (датчики, исполнительные механизмы и ЧМИ). Мир Интернета обычно строится вокруг компьютеров, централизованной программной инфраструктуры или в облаке. Приложения и сервисы используют вещи для обеспечения понимания контекста, искусственного интеллекта, аффективных вычислений. В зависимости от их рассмотрения, планшеты и смартфоны могут быть включены в оба мира. Тем не менее, из-за их мощности (вычисления, связь, время автономной работы, пользовательские интерфейсы) Считается более целесообразным рассматривать их ближе к миру компьютеров и Интернета, чем к миру вещей. В настоящее время Интернет выступает в качестве базовой инфраструктуры для обмена информацией. Однако доступ к нему имеет ряд ограничений, таких как необходимость в уникальном идентификаторе, изменение технологии связи и принятие интернет-протоколов. В настоящее время эта «стена IP» обычно проходит через шлюз IoT. Интернет – это метод глобального присоединения, при котором множество сервисов и приложений используют извлеченную информацию IoT для предоставления услуг конечным пользователям. В каждом из них потребности являются виртуальным представлением вещей IoT для обеспечения взаимодействия. Как только «стена IP» сохранена и благодаря возможности подключения, предоставляемой Интернетом, службы могут получить доступ к информации, но для того, чтобы информация была полезной, ее необходимо понимать, и это представляет собой то, что называется «стеной понимания». Архитектура технологий IoT показывает нам полную информацию о том какая технология в каком уровне используется в соответствии с рисунком 1.5.

Пограничный шлюз состоит из систем агрегации данных датчиков, называемых edge gataways, которые предоставляют такие функции, как предварительная обработка данных, защита подключения к облаку, использование таких систем, как WebSockets, концентратор событий и, даже в некоторых случаях, граничная аналитика или туманные вычисления . Уровень

пограничного шлюза также необходим для предоставления общего представления об устройствах верхним уровням для облегчения управления.

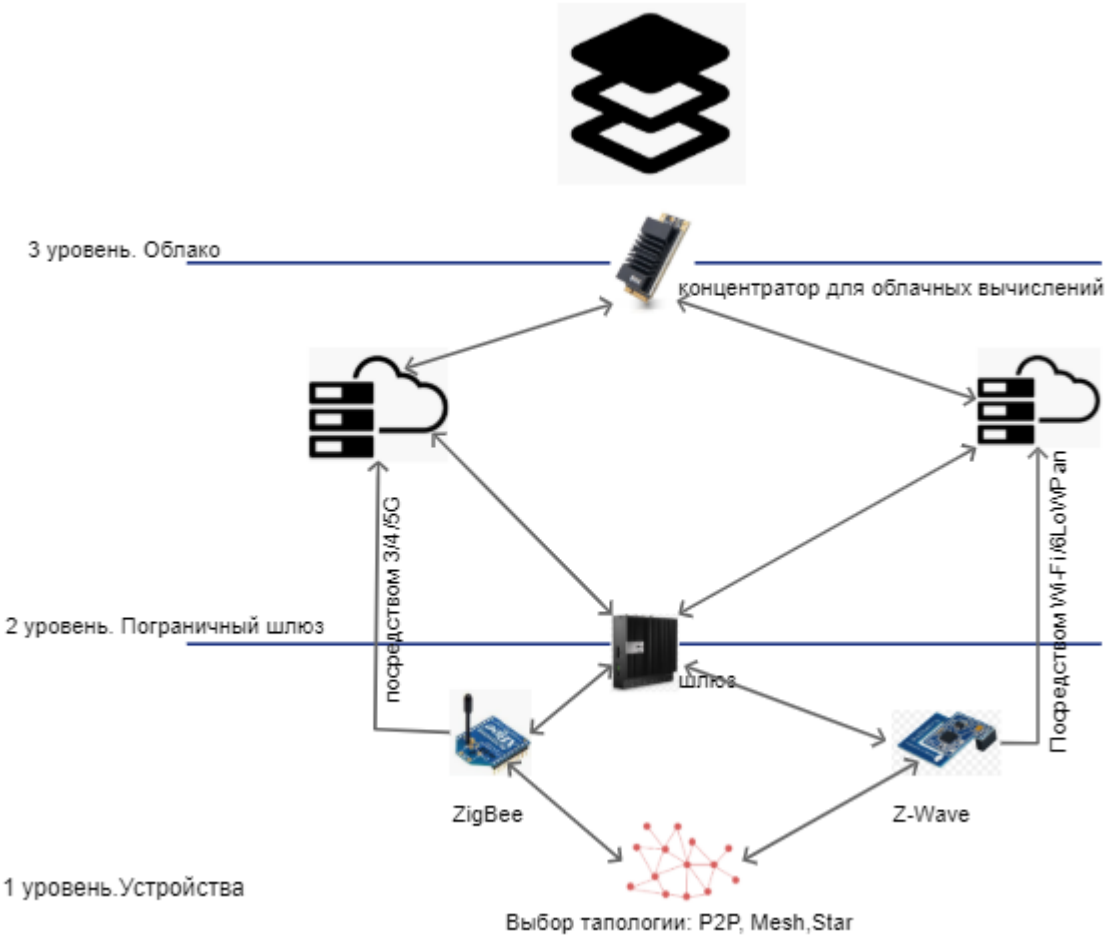


Рисунок 1.5 – Архитектура сетей интернета вещей

Последний уровень включает облачное приложение, созданное для IIoT с использованием архитектуры микро-сервисов, которые обычно являются полиглотами и по своей природе безопасны с использованием HTTPS / OAuth. Он включает в себя различные системы баз данных, в которых хранятся данные датчиков, такие как базы данных временных рядов или хранилища активов, использующие внутренние системы хранения данных (например, Cassandra, PostgreSQL). Уровень облачных вычислений в большинстве облачных IoT-систем включает систему *очередей событий* и обмена сообщениями, которая обеспечивает связь, которая происходит на всех уровнях. Некоторые эксперты классифицировали три уровня в системе IIoT как пограничные, платформенные и корпоративные, и они связаны между собой бесконтактной сетью, сетью доступа и сетью обслуживания, соответственно.

Вещи формируют потоки информации – байты подобранной со поддержкой датчиков такого рода простой информации, равно как

температура, влажность или положение. Зачастую данную информацию именуют Небольшими сведениями (Little Data), так как она небольшая по объемности.

Огромное скопление различных приборов представляет колоссальное число разных не больших сведений через сеть в облако, в каком месте они объединятся, с периодом данных становятся все более и больше. Также тогда их именуют ранее термином Крупные сведения (Big Data). Тут Сеть Интернет вещей становится по-настоящему интеллектуальным, Big Data дают возможность для вас отсылать требования ко тысячам также млн. сведений, для того чтобы исследовать также регулировать объектами наиболее результативно.

Использование аналитических данных, приобретенных с измерителей, предоставляет для вас возможность сопоставить события с результатами или действиями. К примеру, вы знаете, то что весной в улице темнеет позже, по этой причине вам сможете настроить прибор наружного осияние во уличных лампах подобным способом, для того чтобы некто подсоединялся во наиболее позже период, этим наиболее берегя электроэнергию. Либо, к примеру, измерители, нашедшие преобладание степени пульсации оснащения, дают возможность исключить неисправности также своевременно осуществить восстановление.

Опираясь на Интернет вещей, сеть вещей - это архитектура для прикладного уровня Интернета вещей, который рассматривает конвергенцию данных с устройств IoT в веб-приложения для создания инновационных вариантов использования. Чтобы программировать и контролировать поток информации в Интернете вещей, прогнозируемое архитектурное направление называется BPM Everywhere, которое представляет собой сочетание традиционного управления процессами с интеллектуальным анализом процессов и специальными возможностями для автоматизации управления большим количеством согласованных устройств.

1.3 Стандарты IoT/M2M

Стандартизация является одной из самых больших проблем, стоящих перед ростом IoT.

IoT - это передовая технология, которая состоит из множества поддерживающих технологий, например, различных типов технологий сетей связи, информационных технологий, технологий зондирования и управления, программных технологий, технологий устройств и аппаратных средств. Это основано на широко используемых технологиях поддержки, которые определены в стандартах нескольких организаций, таких как ISO, IEC, ITU, IETF, IEEE, ETSI, 3GPP, W3C и т.д.

Поскольку «вещи» связаны друг с другом, интерфейсы между «вещами» должны быть определены на техническом и прикладном уровнях, чтобы получить все преимущества IoT. Работа по стандартизации IoT продвигается по многим направлениям. Обширная литература и поиск в Интернете

позволили создать следующие организации, которые занимаются стандартизацией в области IoT. Результаты этого исследования собраны в таблице.

Результаты показывают, что существует множество организаций, работающих в области стандартизации различных аспектов Интернета вещей.. Стандартизация также позволяет оптимизировать функциональность, стоимость и качество различных приложений и решений IoT.

Таблица 1.2 – Стандарты Интернета Вещей

Короткое имя	Длинное имя	Стандарты в разработке
EPCglobal	Электронный код продукта Технология	Стандарты для принятия технологии EPC (электронный код продукта)
FDA	Управление по контролю за продуктами и лекарствами США	Система UDI (уникальная идентификация устройства) для различных идентификаторов медицинских устройств
GS1	Глобальные Стандарты Один	Стандарты для UID («уникальные» идентификаторы) и RFID быстро движущихся потребительских товаров (потребительских товаров), предметов медицинского назначения и других вещей.
IEEE	Институт инженеров по электротехнике и электронике	Базовые стандарты технологий связи, такие как IEEE 802.15.4 , IEEE P1451-99 (IoT Harmonization) и IEEE P1931.1 (ROOF Computing).
IETF	Интернет-инженерная группа	Стандарты, которые составляют TCP / IP (набор протоколов Интернета)
O-DF	Открытый формат данных	O-DF - это стандарт, опубликованный рабочей группой «Интернет вещей» The Open Group в 2014 году, в котором указана общая структура информационной модели, которая должна применяться для описания любых «вещей», а также для публикации, обновления и запросов. информация при использовании вместе с O-MI (открытый интерфейс обмена сообщениями).
O-MI	Открытый интерфейс обмена сообщениями	O-MI - это стандарт, опубликованный рабочей группой «Интернет вещей» The Open Group в 2014 году, который определяет ограниченный набор ключевых операций, необходимых в системах IoT

Продолжение таблицы 1.2

Короткое имя	Длинное имя	Стандарты в разработке
OCF	Open Connectivity Foundation	Стандарты для простых устройств, использующих CoAP (протокол ограниченных приложений)
OMA	Открытый Мобильный Альянс	OMA DM и OMA LWM2M для управления устройствами IoT, а также GotAPI, который обеспечивает безопасную среду для приложений IoT
XSF	Фонд Стандартов XMPP	Расширения протокола XMPP (Extensible Messaging and Presence Protocol), открытого стандарта обмена мгновенными сообщениями

На рисунке 1.6 предоставлена эталонная модель для систем IoT. Целью составления данной модели является предоставление четких определений и описаний, которые можно точно применять к элементам и функциям систем и приложений IoT. Данная эталонная модель:

– упрощает: помогает сломать сложные системы, чтобы каждая часть была более понятной;

– разъясняет: предоставляет дополнительную информацию для точного определения уровней IoT и определения общей терминологии;

– идентифицирует: указывает, где определенные типы обработки оптимизированы в разных частях системы;

– стандартизирует: это первый шаг, позволяющий поставщикам создавать продукты IoT, которые работают друг с другом;

– организует: делает IoT реальным и доступным, а не просто концептуальным.

В сети IoT данные генерируются множеством видов устройств, обрабатываются по-разному, передаются в разные места и обрабатываются приложениями. Предлагаемая эталонная модель IoT состоит из трех уровней. Каждый уровень определяется терминологией, которая может быть стандартизирована для создания общепринятой системы отсчета. Эталонная модель IoT не ограничивает область действия или месторасположение ее компонентов. Например, с физической точки зрения каждый элемент может находиться в одной стойке оборудования или распространяться по всему миру. Эталонная модель IoT также позволяет выполнять обработку, происходящую на каждом уровне, от тривиального до сложного, в зависимости от ситуации. Модель описывает, как задачи на каждом уровне должны обрабатываться для поддержания простоты, обеспечения высокой масштабируемости и обеспечения поддержки. Наконец, модель определяет функции, необходимые для полной системы IoT. Важно отметить, что в IoT

данные передаются в обоих направлениях. В шаблоне управления управляющая информация течет от вершины модели к основанию. В схеме мониторинга поток информации является обратным. В большинстве систем поток будет двунаправленным.

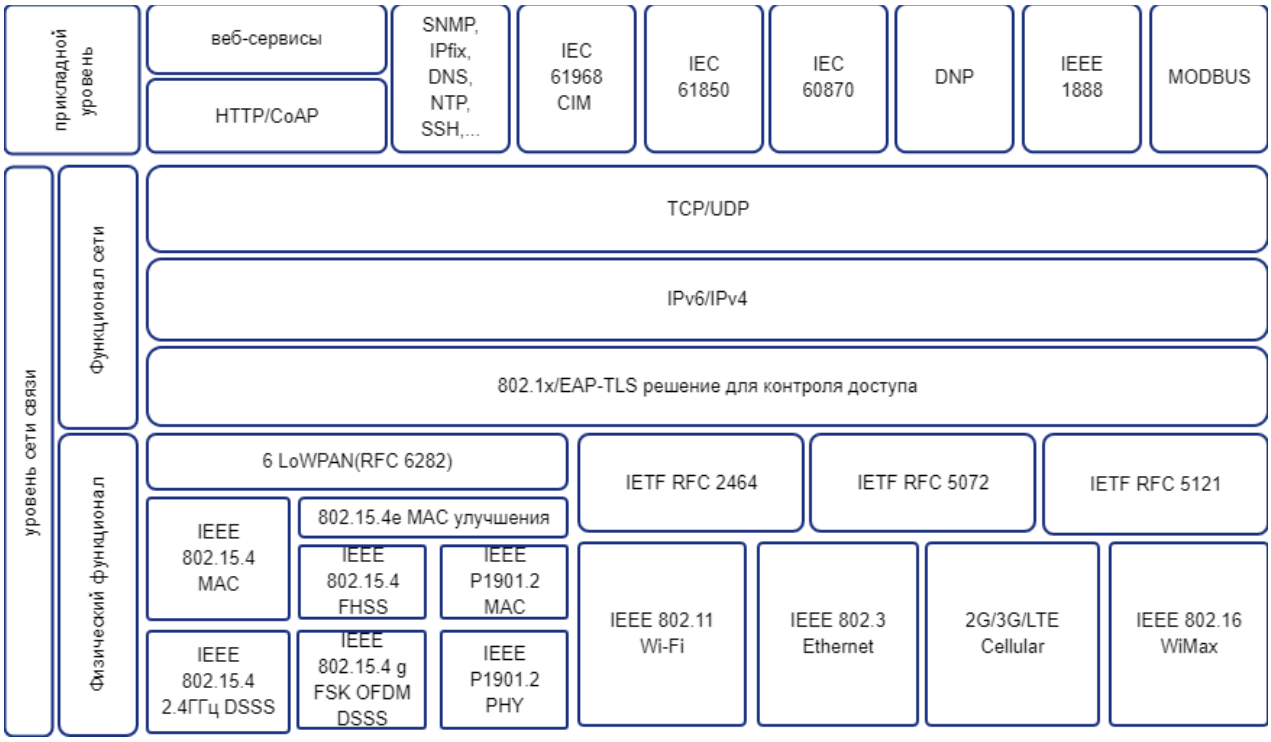


Рисунок 1.6 – Эталонная модель открытых стандартов

1.4 Адресуемость в сетях M2M/IoT

Оригинальная идея центра Auto-ID основана на RFID-метках и четкой идентификации с помощью электронного кода продукта. Это превратилось в объекты, имеющие IP-адрес или URI . Альтернативное представление из мира семантической сети направлено на то, чтобы сделать все вещи (не только электронные, интеллектуальные или с поддержкой RFID) адресуемыми существующими протоколами именования, такими как URI . Сами объекты не взаимодействуют, но на них теперь могут ссылаться другие агенты, такие как мощные централизованные серверы, действующие для своих владельцев. Интеграция с Интернетом подразумевает, что устройства будут использовать IP - адреса качестве отдельного идентификатора. Из - за ограниченного адресного пространства в IPv4 (что позволяет 4,3 млрд различных адресов), объекты в IoT придется использовать следующее поколение Интернет - протокола (IPv6) в масштабе с чрезвычайно большого адресного пространства. Устройства Интернета вещей дополнительно выиграют от автоматической конфигурации адреса без сохранения состояния, присутствующей в IPv6, поскольку это уменьшает накладные расходы на конфигурацию на хостах, и IETF 6LoWPAN сжатие заголовка. В значительной степени будущее Интернета вещей не будет возможно без поддержки IPv6; и,

следовательно, глобальное внедрение IPv6 в ближайшие годы будет иметь решающее значение для успешного развития IoT в будущем.

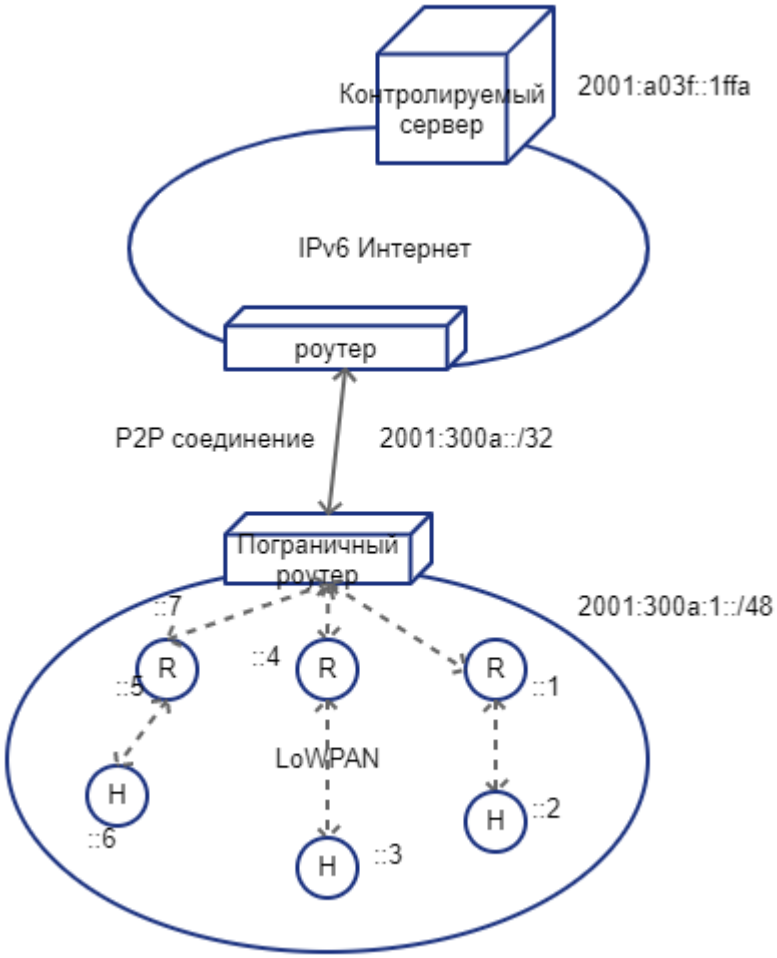


Рисунок 1.7 – Адресация в 6LoWPAN

6LoWPAN-адресация отличается от обычной IPv6-адресации. По сути, адреса IPv6 сжимаются для целей 6LoWPAN. Таким образом, LoWPAN работает по принципу плоского адресного пространства, что означает, что внутри этой беспроводной сети есть только одна подсеть IPv6, в которой она имеет уникальные адреса управления доступом к среде. И эти адреса имеют длину 64 или 16 бит. Таким образом, сжатие адресов IPv6 выполняется путем исключения префикса IPv, сжатия IID (идентификатора интерфейса) и сжатия адресов многоадресной рассылки. По существу, глобальный префикс известен всем узлам сети, а префикс канального уровня указывается форматом сжатия заголовка. Пример адресации показан на рисунке 1.7. Он имеет основную интернет-сеть IPv6, подключенную через маршрутизатор и граничный маршрутизатор, который поддерживает 6LoWPAN. С этого момента речь идет о сетевой адресации, специфичной для сети 6LoWPAN. Если посмотреть на

этот адрес граничного маршрутизатора, он является общим для всей сети 6LoWPAN[20].

1.5 Характеристики трафика приложений IoT

Связь M2M является фундаментальной частью парадигмы IoT. Количество устройств, подключенных к Интернету, растет в геометрической прогрессии, равно как и сетевой трафик. В большинстве случаев трафик имеет дело с маломощными устройствами с батарейным питанием, которые отправляют и получают сообщения по ограниченным сетям, в отличие от традиционных коммуникаций, ориентированных на человека. Понимание характеристик трафика, генерируемого пользователями сети, является важнейшим первым шагом в проектировании сети. Чем точнее технология соответствует требованиям приложения, тем лучше она использует ограниченные ресурсы. Более того, знание характеристик трафика способствует формированию новых бизнес-возможностей. Конечные пользователи могут оценить приблизительные затраты, связанные с сетевым взаимодействием, и сравнить их со стоимостью полученной информации, в то время как сетевые операторы могут найти новые рынки для предоставления своих услуг. Наконец, что не менее важно, характеристики трафика показывают возможность использования IoT и основные препятствия для распространения IoT по всему миру. Правильное понимание этих проблем может не только улучшить текущие решения, но и ускорить весь процесс развертывания.

Чтобы облегчить обсуждение и сравнение, все три области применения будут иметь одинаковую структуру, а именно. краткое введение, типичные приложения, характеристики трафика, предпочтительные сетевые технологии, а также выполнимость и основные проблемы. Кроме того, характеристики трафика IoT-услуг всегда суммируются в ссылочных таблицах. Эта иерархия уменьшает отвлекающие факторы и фокусируется на главной цели - определении характеристик трафика доменов приложений IoT.

1.5.1 Умные здания

Умные здания и жилые домены направлены на повышение энергоэффективности зданий и улучшение качества нашей жизни. В последние несколько лет, безусловно, существует значительный спрос на автоматизацию в этой области, и в результате было предложено много решений. Тем не менее, преимущества IoT расширяют возможности еще больше, и благодаря простым системам со статически определенным поведением теперь можно разрабатывать высокодинамичные архитектуры, которые собирают шаблоны действий пользователей и адаптируются к ним соответствующим образом[21].

1) Типичные области применения: для интеллектуальных зданий и жилых помещений включают автоматизированное управление освещением и отоплением, мониторинг использования энергии и воды для экономии

расходов, дистанционное управление интеллектуальными приборами и персональные настройки на основе предпочтений пользователя , но также обнаружение аномалий для повышения безопасности объекта.

2) Характеристики трафика: с точки зрения трафика данных, интеллектуальные здания и жилые помещения относительно нетребовательны, но требуют масштабируемой инфраструктуры, поскольку каждое свойство отличается. Скорость движения нечаста и часто нерегулярна, учитывая тот факт, что люди перемещаются внутри здания в течение дня. Тем не менее, требования к QoS могут быть высокими, так как пользователю требуется быстрое время отклика, и он не хочет ждать полминуты, пока не загорится свет или устройство не выполнит нужную команду. Что касается источника энергии, то в зависимости от услуги устройства могут питаться от сети или от батареи, с возможностью или без возможности перезарядки, но они также могут быть автономными, например, в случае потока воды в случае приборы контроля воды. В таблице 1.3 приведены характеристики трафика наиболее распространенных услуг в интеллектуальных зданиях и жилых помещениях.

3) Предпочтительные сетевые технологии: на основе определенного трафика данных интеллектуальных зданий и живых приложений, сетевые технологии ближнего действия могут быть предпочтительнее. Например, Wi-Fi очень широко распространен, и, как было показано, во многих случаях энергетические ресурсы не являются самой большой проблемой. Для устройств с более ограниченными возможностями может быть хорошим выбором несколько WPAN, специально разработанных для IoT (например, Bluetooth, ZigBee, Z-Wave, Thread и т. Д.).

Таблица 1.3 – Характеристики трафика умных домов

Сервис	Размер сети	Скорость трафика	Требования к QoS
мониторинг состояния здания	с 10 до 100 устройств	1 сообщение/час	низкое, допустимое задержка 1 мин
обнаружения аномалий		нечастый	высокое, допустимое зарежка 3 секунд
контроль света		нечастый	высокое, допустимое зарежка 3 секунд
контроль дверей		1 сообщение/15 мин	высокое, допустимое зарежка 5 секунд
климат контроль		1 сообщение/15 мин	высокое, допустимое зарежка 5 секунд
умные приборы		нечастый	высокое, допустимое зарежка 3 секунд
использование энергии и воды	меньше 10 устройств	нечастый	высокое, допустимое зарежка 3 секунд

4) Осуществимость и основные проблемы. Умные здания и жилые домены уже имеют множество прикладных решений, и, поскольку трафик не так требователен, сама технология не является серьезной проблемой. Более серьезная проблема - плохая совместимость устройств разных производителей и, следовательно, отсутствие единой общей платформы, с которой можно было бы управлять устройствами. В настоящее время существует два подхода к решению этой проблемы. Первый подход направлен на то, чтобы предложить общепринятые сетевые технологии (такие как ZigBee, Z-Wave, Thread и т. Д.), Тогда как второй основан на сокрытии базовой сетевой технологии, предлагая интеграционную среду.

Это лишь маленькая часть всей структуры систем IoT трафика.

1.5.2 Умный город

В условиях быстрого роста городского населения во всем мире обеспечение устойчивости государственных услуг требует поиска новых способов улучшения использования государственных ресурсов, снижения эксплуатационных расходов и оптимизации основных компонентов инфраструктуры города. Тема создания города более разумным, безусловно, не нова, однако IoT может предложить вычислительные и сенсорные возможности, которые могут повысить скорость общего прогресса[22].

1) Типичные приложения: Приложения для «умного города» нацелены на широкий спектр задач, от сокращения расходов на повседневные услуги, такие как молния или управление отходами, до мониторинга городских условий, таких как шум или загрязнение воздуха, вплоть до расширения имеющейся информации о текущей загруженности дорог или ситуации с парковкой.

2) Характеристики трафика: из-за количества и разнообразия услуг характеристики трафика в области умного города весьма разнообразны. Размер сети обычно средний или большой, соединяющий от сотен до тысяч устройств. Кроме того, городская территория типична своей высокой плотностью и количеством препятствий, которые необходимо учитывать. С другой стороны, скорость трафика и QoS менее требовательны, поскольку городские услуги IoT обычно не так критичны. В большинстве случаев частота передачи данных ниже или даже нерегулярна с допустимой задержкой до 1 минуты. Что касается источника энергии, то большинство услуг полагаются на датчики с батарейным питанием, которые должны иметь очень хороший срок службы, и поэтому некоторые решения по сбору энергии будут полезны. Таблица V описывает характеристики трафика различных служб в отдельности.

3) Предпочтительные сетевые технологии. В городских районах обычно имеется хороший охват всех видов сетей, поэтому подходят как сетевые технологии ближнего, так и дальнего радиуса действия. Однако, учитывая характеристики трафика, LPWAN могут удовлетворить все требования, предлагая более простую реализацию.

4) Осуществимость и основные проблемы. С технической точки зрения создание умного города не является проблемой. Все описанные сервисы могут быть легко разработаны и развернуты с использованием современных технологий. Но вопрос в том, какой ценой. Кроме того, важно отметить, что город не является зеленым полем, и многие системы уже внедрены. Большинство этих систем являются проприетарными и взаимно несовместимыми, но должны быть интегрированы в одну сложную платформу умного города. Экономическая эффективность и близость существующих решений представляют собой сложные проблемы, которые постепенно преодолеваются, но все еще необходимы дальнейшие исследования.

Таблица 1.4 – Характеристики трафика умного города

Служба	Размер сети	Скорость движения	Требования по QoS
Городской мониторинг потребления энергии и воды	от среднего до большого, от 100 до 1000 устройств	обычная, 1 сбщ каждые 10 мин на устройство	низкая, терпимая задержка 1 мин
Контроль освещения	большой, тысячи устройств	нерегулярный, нечастый	средняя, допустимая задержка 15 сек
Отслеживание парковки	большой, тысячи устройств	нерегулярный, нечастый	средняя, допустимая задержка 10 сек
Управление пробками	большой, тысячи устройств	обычная, 1 сбщ каждые 10 мин на устройство; нерегулярный для тревоги	средняя, допустимая задержка 15 сек; высоко для тревоги
Управление отходами	большой, тысячи устройств	нерегулярный, нечастый	средняя, допустимая задержка 30 сек
Мониторинг городской среды	от среднего до большого, от 100 до 1000 устройств	обычная, 1 сбщ каждые 15 мин на устройство; нерегулярный для тревоги	средняя, допустимая задержка 30 сек; высоко для тревоги
Структура мониторинга здоровья			

1.5.3 Умный транспорт и мобильность

Быстрая урбанизация, связанная с растущими заторами на дорогах и глобализацией рынков, создала спрос на более разумное управление транспортом и мобильностью. Цель состоит в том, чтобы сделать транспортировку более быстрой, дешевой и безопасной, чего можно достичь, собирая все виды данных и анализируя их, чтобы найти оптимальные решения[19].

1) Типичные приложения. Среди наиболее обсуждаемых приложений интеллектуальной сети и области мобильности, несомненно, являются автоматизированные и автономные транспортные средства, поскольку они относятся к каждой группе пользователей - отдельным лицам, обществу, а также промышленности. Тем не менее, другие типичные приложения включают локализацию и отслеживание транспортных средств, контроль качества отгрузки, динамическое управление светофорами на основе текущей дорожной ситуации и мониторинг состояния дорог.

2) Характеристики трафика. Интеллектуальная область транспорта и мобильности может быть требовательной с точки зрения характеристик трафика. Количество датчиков в транспортных средствах быстро растет, так что сеть, способная обрабатывать тысячи мобильных устройств с хорошим покрытием, немыслима. Скорость трафика зависит от услуги. Может возникнуть необходимость отправлять сообщение каждые несколько секунд, например, в случае прогнозирования прибытия общественного транспорта, но частота может быть увеличена до 1 сообщения каждые 24 часа в таких сценариях, как получение данных для аналитических целей. Требования к QoS обычно высоки, с допустимой задержкой, близкой к реальному времени при обмене данными между транспортными средствами, хотя большинство услуг не требуют немедленного времени доставки, и задержка в несколько секунд является допустимой. Устройства для интеллектуального транспорта и мобильности в основном питаются от аккумуляторов транспортных средств или питаются от придорожных устройств / датчиков, поэтому точность и точность предпочтительнее экономии энергии. Однако даже в этой области можно найти устройства, для которых критически важна энергоэффективность, такие как дорожные датчики или датчики для контроля качества условий перевозки. Более подробная информация о характеристиках трафика интеллектуальной транспортной и мобильной области показана в таблице VII.

3) Предпочтительные сетевые технологии. Нельзя сказать, какие типы сетевых технологий предпочтительнее в интеллектуальном транспорте и мобильности, поскольку требования к характеристикам трафика очень разнообразны. Связь между транспортными средствами, безусловно, должна строиться на технологиях ближнего действия, тогда как для локализации и мониторинга транспортных средств требуются сетевые технологии большого

радиуса действия. Поэтому на каждую услугу нужно смотреть индивидуально.

4) Осуществимость и основные проблемы: интеллектуальные приложения для транспорта и мобильности, такие как автоматизация транспортных средств, представляют собой начало современных возможностей. Несмотря на то, что в настоящее время ведутся активные исследования автономных транспортных средств во всем мире, реализация полностью автоматизированных перевозок все еще находится на некотором расстоянии из-за основных проблем, таких как сложность области, чрезвычайно динамичные условия и требуемая надежность.

Таблица 1.5 –Характеристики трафика умного транспорта и мобильности

Обслуживание	Размер сети	Скорость движения	Требования по QoS
Автоматизация автомобиля	большой, тысячи автомобилей	регулярный, 1 сбщ каждые 24 часа на транспортное средство, нерегулярный и частый в общении между транспортными средствами (V2V)	низкая, терпимая задержка 1 мин; высокая для V2V, переносимая задержка вблизи реального времени
Локализация и мониторинг транспортных средств	большой, тысячи автомобилей	регулярный, 1 сбщ каждые 30 сек на транспортное средство	средняя, допустимая задержка 10 сек
Мониторинг качества условий отгрузки	средний, 100 устройств	обычная, 1 сбщ каждые 15 мин на устройство	средняя, допустимая задержка 15 сек
Динамическое управление светофорами	большой, тысячи устройств	обычная, 1 сбщ каждые 1 мин на устройство	высокая, терпимая задержка 5 сек
Мониторинг состояния дороги	большой, тысячи устройств	нерегулярный, нечастый	средняя, допустимая задержка 30 сек

2 Анализ и моделирование трафика Интернета вещей

2.1 Прогнозирование объема трафика IoT/M2M

Трафик, создаваемый IoT/M2M устройствами, в настоящее время является недостаточно изученным и трудно прогнозируемым, что объясняется растущим числом приложений и большим разнообразием устройств в сети. Трафики, создаваемые отдельными устройствами, могут быть как регулярными, так и чисто случайными.

M2M трафик появился в сетях связи с появлением первых телеметрических устройств. До недавнего времени в сетях связи с коммутацией каналов широко применялись технологии сигнализации (пожарная, аварийная, сигнализация контроль доступа) и телеметрические технологии. Эти системы выполняли функции мониторинга окружающей среды и управления технологическими процессами. Часть сетевых ресурсов и трафика используемых для обслуживания, была не настолько существенной, чтобы оказывать заметное влияние на QoS для других типов трафика. Пример того что, для сигнализации квартир почти исключительно использовались ресурсы сети абонентского доступа (абонентские линии). В управлении технологическими процессами, например, сетей передачи электроэнергии, железных дорог трафик телеметрии обслуживается выделенными ресурсами ведомственных сетей связи. Аналогичных форм реализации межмашинных сетей почти не было, поэтому не было существенных проблем с QoS или проблем с их влиянием на QoS трафика других услуг.

Современная ступень развития коммуникационных технологий и компьютерных сетей приводит к внедрению информационных систем в сферу деятельности, которая ранее не была задействована в информационно-коммуникационных сетях. Необычайно широкое применение информационных технологий практически во всех сферах человеческой деятельности объясняются тем что развиваются сенсорные сети. Разработка VANET (Vehicular Ad Hoc Networks Автомобильные специальные сети) и других телекоммуникационных систем, разработанных во многих случаях для реализации передачи данных между машинами (автоматами), существенно влияет на часть M2M-трафика в сетях связи и увеличивает ее влияние на качество услуг связи [22,23,24,25,26,27].

Один из вариантов реализации межмашинных M2M-сетей это – сенсорные сети. Реализация последнего осуществляется очень быстро и уже сейчас актуальна задача изучения влияния M2M-трафика на существующие сети связи.

Рост трафика M2M объясняется тем что сегодня развертываются инфокоммуникационные сети ЖКХ [28,29]. Результат этого процесса может быть в будущем это объединение различных типов датчиков в одну систему. Как минимум, количество таких датчиков определяется количеством счетчиков на объем потребляемых услуг (электричество, вода и др.).). Это

говорит нам что, количество совмещенных датчиков только в этом процессе потенциально может превышать количество жителей. Развитие систем экологического мониторинга, а также систем общественного порядка и безопасности является еще одним приоритетом развития сетей M2M.

Эти системы могут использовать как проводные, так и беспроводные сети связи для передачи данных. Количество оконечных точек сети M2M вскоре может превысить численность населения, что означает фактическое количество абонентов сети. Все эти технологии в объединении определяется как Интернет вещей (IoT).

Межмашинный трафик оказывает значительное влияние на QoS в беспроводных сетях и на их работу [30, 31, 32]. Пример того что, незначительные трафики M2M в сетях усложняют или исключают возможность управления качеством канала связи методом оценки длительности занятости (разговора), который традиционно используется операторами связи. Специфика применения таких систем управления может быть выражена в специфических особенностях производимого трафика. Поведение ряда приборов может быть зависимым, что может привести к крупной активности, которая выражается в неконтролируемом увеличении трафика.

Из-за таких вот случаев в сегодняшние дни необходимо оценивать межмашинный трафик и его взаимодействие с услугами традиционной связи, связи с этим определять методы организации IoT-систем, которые обеспечивали бы хорошую синхронизацию с сетями связи.

На основе метода ассоциативного прогнозирования, был получен прогноз общего прироста трафика межмашинных сетей в фиксированных и мобильных сетях, показанный на рисунке 2.1.

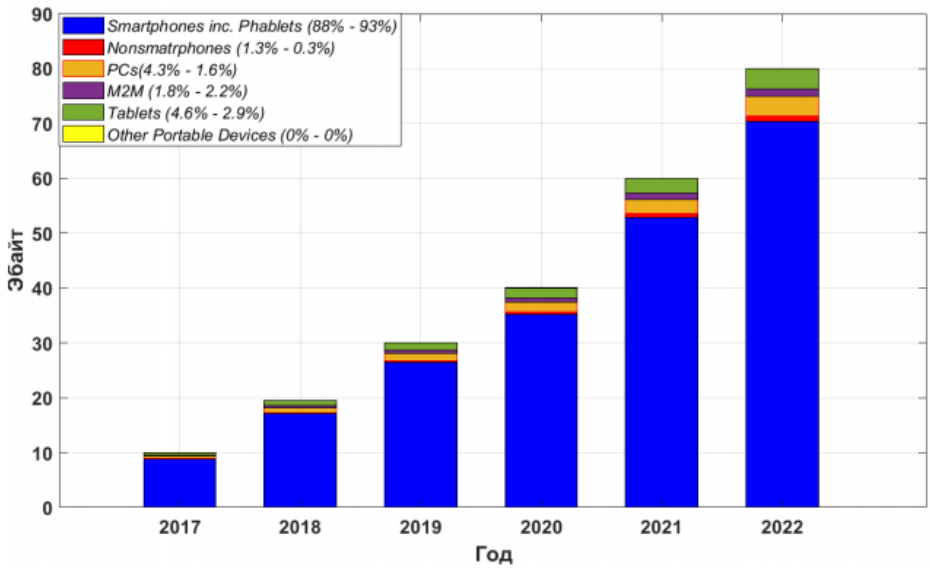


Рисунок 2.1 – Прогноз увеличения сетевого трафика IoT в сетях фиксированной и мобильной связи и беспроводного доступа

Отсюда видно, что прогнозы по трафику M2M в сетях фиксированной связи, а также в сетях мобильного и беспроводного доступа близки по значению, что объясняется приближенными значениями суммарного трафика в этих сетях. Необходимо отметить, что в прогнозе было учтено, что согласно 33% трафика в сетях мобильной связи передается в сети стационарной связи, что увеличивает его суммарный трафик.

Можно заметить, что общий объем трафика M2M на 2016 год преобладает 300 Пбайт, поэтому необходимо глубокое исследование характеристик этого трафика. Следует отметить, что часть трафика M2M составит порядка 5% от общего объема трафика сетей связи мира. Помимо этого, следует предположить, что трафик M2M может отличаться по своим характеристикам от трафика традиционных сетей связи.

Для описания трафика в существующих сетях связи применяются различные аналитические модели, обычно основанные на теории очередей. Целью построения модели является исследование характеристик трафика (потока) и методов его поддержания сетью связи.

Потоковый M2M-трафик - это информационный трафик (пакеты в сети передачи данных или сеансы в сети с коммутацией каналов). Его основное отличие от абонентского трафика H2H (от человека к человеку) заключается в том, что инициатором обмена информацией является автоматизированное устройство. В связи с этим, в зависимости от реализации технологии обмена данными (протокол связи), передача данных возможно при соблюдении следующих условий:

– влияние внешних факторов, которые приводят к передаче данных (смена) физических параметров, контролируемых датчиком;

– через определённый промежуток времени;

– технические причины, то есть передача сервисных данных не связана с вышеперечисленными условиями.

Из рисунка 2.2 видно, что количество Интернета вещей (согласно количеству устройств M2M) достигает значения в соответствии с количеством всех других устройств, подключенных к сетям связи. Этот прогноз, вероятно, будет оценкой количества «снизу», поскольку он учитывает только устройства M2M. Следовательно, количественные характеристики сети IoT таковы, что даже при оценке «снизу» показывается чрезвычайно большое количество IoT в краткосрочной перспективе. В связи с этим очевидно, что требуются методы, которые позволяют как эффективно проектировать, так и эффективно администрировать сети с таким количеством устройств. Также должна быть возможность контролировать трафик в таких сетях, который, ввиду значительного числа потенциальных источников, может создавать реальные угрозы для сети из-за перегрузки и низкого качества обслуживания для других типов трафика.

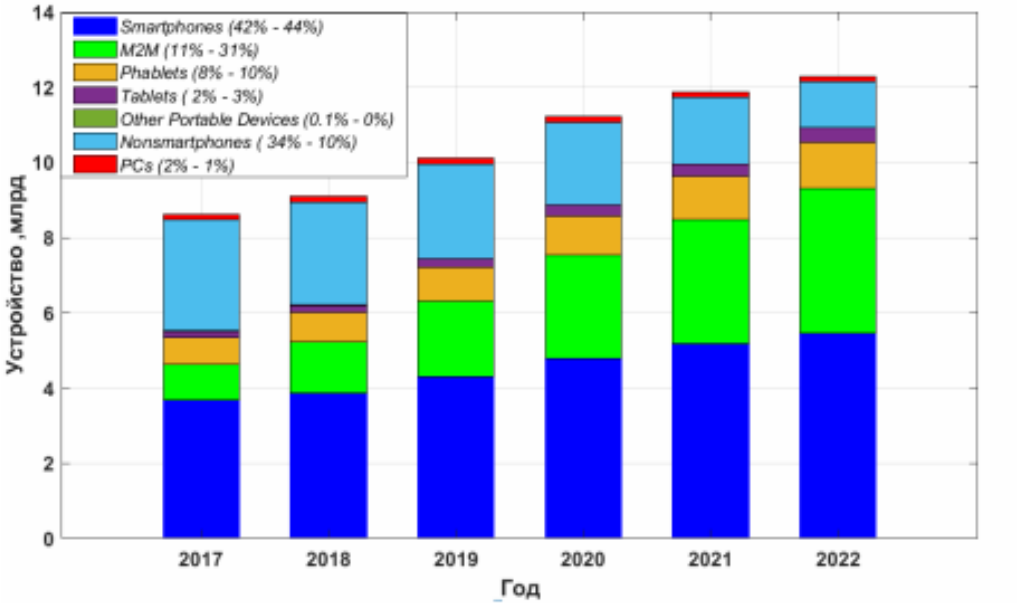


Рисунок 2.2 – Прогноз подключения к сети

Рост количества IoT, так и рост количества абонентов рассмотренных технологий, есть возможность описать логистической кривой:

$$f(t) = \frac{A}{1 + e^{-\frac{t - t_0}{B}}} \tag{2.1}$$

Для построения прогноза следует оценить быстроту роста B IoT (наклон кривой) и уровень насыщения A (максимально достижимое число Интернет вещей) как показано на рисунке 2.3.

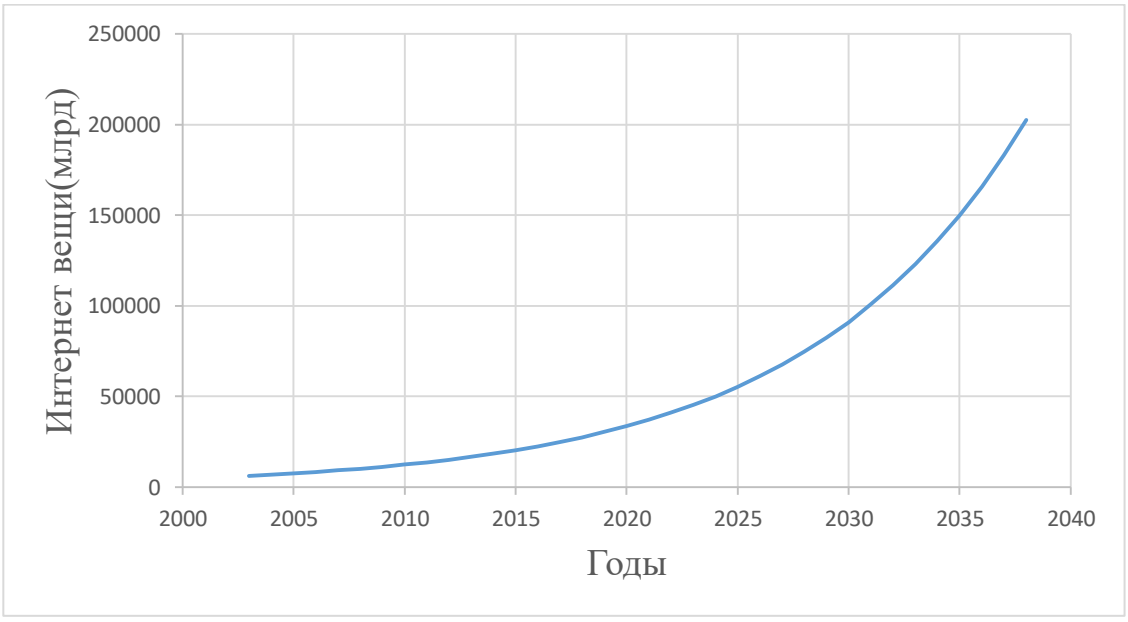


Рисунок 2.3 – Прогноз роста числа IoT

2.2 Анализ характеристик и параметров трафика IoT/M2M

Интернет-трафик является наименее изученным процессом и возможность предсказания является минимальным. Трафик, создаваемый системами мониторинга, может быть регулярным потоком, а трафик от систем сигнализации, которые реагируют на внешние факторы, является непредсказуемым случайным процессом. В обоих случаях свойства трафика IoT могут существенно влиять на качество трафика обслуживания других услуг связи, что также имеет место в сети связи. Влияние трафика IoT на качество сети связи создает ее потенциальные уязвимости. Особенности трафика интернета вещей, такие как неограниченная устойчивость автоматических устройств, зависимость от внешних раздражителей, детерминированный (регулярный) или квази-детерминированный трафик, могут привести к снижению качества обслуживания как трафика межмашинных коммуникаций, и еще трафика различных услуг сети.

Характеристики трафика M2M отличаются от существующих сетевых трафиков, основанных на модели взаимодействия человека с человеком в цепочке конечного пользователя E2E ("end-to-end"). Соединение на основе модели взаимодействия "человек-человек" (H2H) подвержено определенным закономерностям генерируемого трафика по длине сессии, объему данных и частоте взаимодействия. Модели трафика M2M, построенные по сценариям взаимодействия "человек-человек", будут иметь свои особенности.

Основные характеристи трафика M2M можно перечислить как :

– массивность числа устройств в M2M;

– маленький объем трафика генерирующиеся M2M-устройствами;

– ассеметричный объем трафика;

– нерегулярный и концентрированный трафик на отдельных временных участках;

– гибкость требований по времени доставки данных;

– групповой доступ;

– разнооразие уровней QoS для данных M2M.

По свойствам M2M можно выделить три основных видов трафика.

Опосредованный трафик – производится автоматическими системами использующих активные устройства. Этот трафик нужно рассматривать как отклик на различных случайных событий. В этом трафике интенсивность наблюдаемых событий может быть сравнима с частотой отказов самого контрольного устройства или даже меньше. Для того чтобы обеспечить необходимую надежность обнаружения наблюдаемых событий, необходимо следить за техническим состоянием сенсоров. Это требует передачи сервисных данных, объем которых может значительно превышать объем необходимой информации, а характеристики трафика обусловливаются характеристиками диагностического процесса состояния датчиков.

Псевдо-детерминированный трафик - производится автоматическими системами с использованием пассивных датчиков. В сегодняшний день

широкое распространение имеют системы диспетчерского управления и сбора данных (SCADA - Supervisory Control And Data Acquisition), построенные по принципу "мастер-ведомый". В этих системах датчики подчинены (пассивные устройства) и передают данные по запросу ведущего устройства. В данном конкретном случае характеристики трафика определяются с помощью алгоритма выбора промежутка времени между мгновениями, когда передаются запросы данных. Обычно в существующих системах промежутки времени между моментами опроса не являются случайными. Измерение датчиков производится по определенному расписанию или просто с заданным фиксированным интервалом времени. Этот вид трафика включает в себя также трафик, генерируемый разнообразными автоматическими комплексами в детерминированные моменты времени (обновление данных, программное обеспечение по расписанию и т.д.).

Служебный трафик – типичный трафик для систем с активными сенсорами. Он генерируется, когда возникают некоторые внешние события (обычно случайных), которые заставляют задействовать сервисных операций для поддерживания возможности использования системы, а также для анализа работоспособности датчиков. Это сервисный трафик, генерируемый в результате различных видов аппаратных или программных сбоев, с целью устранения которых выполняются необходимые процедуры для установления соединения, передачи параметров для настройки датчиков и т.д. Как правило, служебный трафик приводит к формированию сигнального трафика, который достаточно хорошо изучен для сенсорных сетях, поэтому его характеристики в данной работе далее не анализируются.

Тема моделирования трафика очень широка. Он варьируется от моделей голоса с коммутацией каналов на основе формул Эрланга, моделей очередей с коммутацией пакетов до анализа тяжелых хвостов в потоках TCP и их источника в структуре приложения. В общем случае M2M не ограничивается каким-либо видом услуг по транспортировке своей полезной нагрузки, например, он может использовать дейтаграммы голоса, SMS и IP. Однако с введением LTE, которое само по себе больше не поддерживает передачу голоса с коммутацией каналов, все приложения могут быть сопоставлены с IP-датаграммами. Далее сосредоточимся на моделях трафика с коммутацией пакетов (но для полноты картины будет также упомянута модель коммутации каналов). Для этого обсудим различные модели трафика для разных сценариев в сети.

Любая коммуникационная сеть выполняет определенный объем работы по доставке (сервису) трафика, при этом расходуя определенное количество ресурсов. Трафик - это процесс приема приложений от пользователей или других устройств, способных генерировать такие приложения. Этот процесс обычно описывается случайным процессом. Однако в сети IoT это также может быть детерминированным процессом. Приложение приходит в случайное или определенное время. При обслуживании каждого приложения сеть потребляет определенное количество ресурсов. Если сеть не имеет

свободных ресурсов при получении приложения, приложение отказывает в обслуживании или помещает его в очередь, в зависимости от используемой спецификации услуги. Применяются две основные служебные дисциплины: с отказом и с ожиданием.

В сетях с коммутацией каналов будут применяться дисциплина обслуживания с отказом, в то время как в сетях с коммутацией пакетов (сообщения) будут приниматься комбинированные дисциплины обслуживания, что допускает как потерю, так и ожидание.

Когда разные приложения могут иметь разные приоритеты, приоритетные услуги могут предоставляться субъектам. В этом случае приложение с более высоким приоритетом будет помещено в очередь перед приложением с более низким приоритетом.

Сеть связи или ее фрагменты могут быть представлены в виде системы массового обслуживания. Функция СМО определяется атрибутами и параметрами трафика и пропускной способности и может быть описана параметрами качества обслуживания (задержка и вероятность потери в буфере) [33]. Обозначения характеристик потока:

– M, марковский поток, поток без последействия;

– MX , ординарный поток, при котором случайные заявки X поступают в один момент веремени;

– MAP, обобщенный поток;

– BMAP, обобщенный поток, в котором несколько заявок поступают в один момент времени;

– MMPP, Пуассоновский поток при котором заявки образуют кластеры;

– D, детерминированный поток;

– Ek, поток Эрланга к – го порядка;

– G, произвольное распределение;

Обозначения характеристик обслуживания:

– M, экспоненсиальное распределение времени обслуживания;

– D, постоянное время;

– Ek, распределение Эрланга к – го порядка;

– G, произвольное распределение.

Обозначения очереди:

– FIFO/FCFS, упорядоченная очередь, первый пришел, первый обслужен;

– LIFO/LCFS, стековая очередь, последний пришел, первый обслужен;

– SIRO, случайный выбор из очереди;

– PNPN, выбор с приоритетом

В течение некоторого времени M2M находится в центре внимания мобильной индустрии, и наряду с текущей деятельностью в исследовательском сообществе предпринимаются усилия по пониманию влияния M2M на архитектуру мобильной сети и спецификации соответствующих стандартов (например, ETSI M2M). , 3GPP и IEEE).

Стандартизация IEEE вызвала рабочую группу по M2M в рамках CDMA. Рабочая группа IEEE Machine-to-Machine (M2M) была создана в 2010 году для работы над проектами 802.16p и 802.16.1b. Оба стандарта были одобрены IEEE в 2012 году. Целевая группа IEEE 802.16 Machine-to-Machine (M2M) является важным ресурсом с точки зрения характеристик трафика и моделей трафика для интеллектуальных сетей и приложений M2M. Стандарт содержит две таблицы, обеспечивающие хороший обзор моделей трафика M2M. Таблица 2.1 ссылается на стандарт IEEE802.16p. Таблица отображают средний размер сообщения, скорость транзакции и скорость передачи данных в сочетании с распределением процесса прибытия в потоке трафика.

Таблица 2.1 – Параметры трафика городских M2M устройств

Техника / Приборы	Средняя скорость передачи сообщений/ с	Средний размер сообщения (в байтах)	Скорость передачи данных (б / с)	Распределение и прибытие
машина в продуктовом магазине	0.0083	24	0.2667	Пуассоновский
машина в магазине	5.5556e-4	24	0.0178	Пуассоновский
Дорожные знаки	0.0333	1	0.2664	Равномерный
Светофор	0.0167	1	1.3360	Равномерный
Датчики движения	0.0167	1	1.3360	Пуассоновский
Прокат машин	1.1574e-5	152	1.4814e-3	Пуассоновский

2.3 Анализ существующих моделей трафика IoT/M2M

Поскольку IoT продолжает набирать обороты в телекоммуникационных сетях, ожидается, что в ближайшем будущем будет подключено и использовано очень большое количество устройств. Для надлежащего планирования и измерения сети, а также внутренних облачных систем и результирующей нагрузки сигнализации используются модели трафика. Эти модели предназначены для точного сбора и прогнозирования свойств трафика IoT в сжатой форме.

Характеристики обмена данными между устройствами (M2M) значительно отличаются от обычных связей между людьми (H2H, human to human). Основными отличиями являются:

– обычные приложения M2M генерируют короткие пакеты периодических пакетов данных;

– большую часть времени связь M2M устанавливается по каналам восходящей линии связи;

– трафик M2M генерируется машиной и обычно не зависит от вмешательства человека;

– требования к качеству услуг (QoS) для связи M2M значительно отличаются от приложений H2H, таких как мобильность, задержка задержки, объем данных, приоритеты, энергопотребление, требования безопасности.
Поэтому обслуживание устройств M2M (M2MD) традиционными сетями, построенных для связи H2H, усложняется и ставит несколько задач .

Точная модель трафика связи M2M имеет решающее значение при планировании и реализации сети M2MD, то есть Интернета вещей (IoT). В частности, он играет важную роль в следующих аспектах:

– оценка эффективности использования энергии алгоритма распределения радиоресурсов (RRA) и производительности пропускной способности;

– обеспечение лучшего понимания связи и трафика M2M, чтобы позволить разработчикам сетей оснастить сеть эффективными ресурсами для обработки прогнозируемого огромного количества устройств;

– можно избежать нескольких угроз безопасности, если бы люди могли определить разницу между обычным трафиком, передаваемым устройствами M2M, и вредоносным трафиком, генерируемым, например, в результате нарушения безопасности, такого как трафик, генерируемый атакой распределенного отказа в обслуживании.

В модели трафика [34] подразделяются на два основных класса, а именно:

– модели исходного трафика;

– модели агрегированного трафика.

Модель исходного трафика учитывает трафик отдельного M2MD, а модель агрегированного трафика учитывает результирующие характеристики трафика в широкополосной сети. Модели трафика Source, обычно используемые в литературе, являются расширениями моделей трафика H2H. Следовательно, они не могут использоваться непосредственно для моделирования трафика M2M из-за различий между двумя типами связи, обсуждавшимися ранее. В частности, модели в литературе обычно учитывают очень конкретные сценарии. Следовательно, они не могут быть обобщены для трафика M2M. Поэтому трафик, полученный из предложенной модели связи M2M, может охватывать более широкий диапазон настроек.

В частности, предполагается, что на генерируемый трафик из предложенной модели связи влияют несколько факторов (как показано на рисунке 2.1).

Первый фактор - это информационная емкость канала. Это играет важную роль во времени передачи данных. Большинство моделей трафика, доступных в литературе, не учитывают информационную емкость, поскольку они в основном основаны на моделях Эрланга и Энгеста. Модели Эрланга и Энгсета были предложены для телефонных сетей (т.е. сетей с коммутацией

каналов) и, вероятно, не подходят для трафика M2M. Вторым фактором, не учитываемым в существующих моделях трафика M2M, является инцидент блокирования, при котором пользователям требуется доступ к совместно используемым каналам, но каналы уже полностью заняты. Кроме того, механизм множественного доступа отсутствует в существующих моделях трафика M2M. Для совместно используемого канала существует два основных подхода множественного доступа, классифицированных в статье [35], а именно:

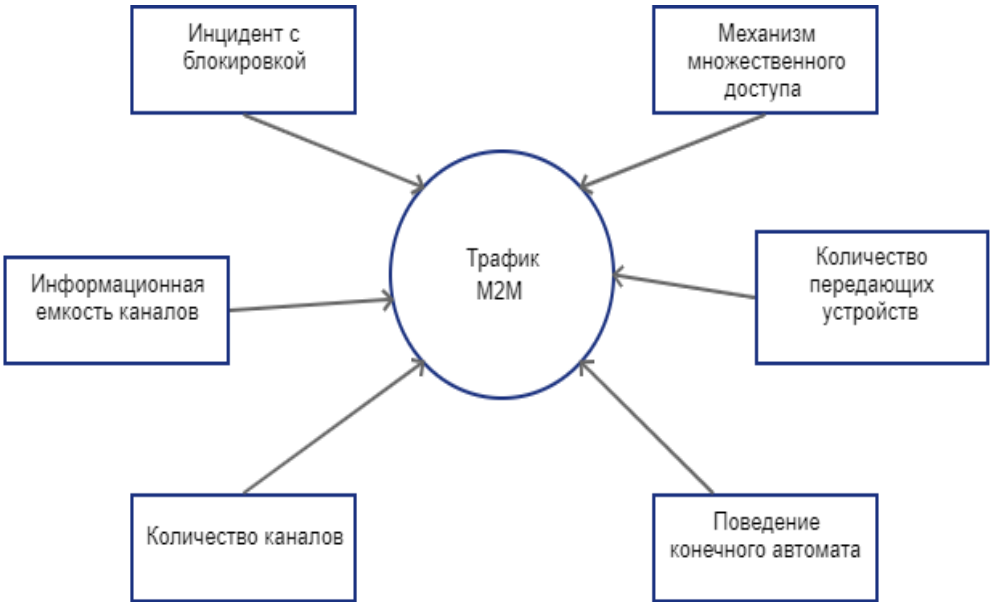


Рисунок 2.4 – Факторы, влияющие на трафик связи M2M

– централизованный запланированный доступ, в котором централизованное устройство определяет, какая часть канала выделена для каждого пользователя, например, алгоритмы планирования сотовой связи;

– распределенный доступ, при котором каждый пользователь локально выбирает канал для доступа, например, механизм ALOHA. Использование предложенной модели связи на основе полученного трафика обеспечивает значительное улучшение (по сравнению с моделями трафика, предложенными в литературе).

2.3.1 Управляемая событиями модель трафика M2MD

Авторы в [36] предложили классифицировать трафик M2MD в двух различных моделях в соответствии с периодичностью передач. Первая модель изучала трафик периодического обновления, называемый узлами фиксированного планирования (FS), например регулярные отчеты об измерениях датчиков. Предполагается, что трафик, генерируемый узлом FS, следует детерминированному процессу, представляющему периодические передачи. Вторая модель ориентирована на непериодический трафик данных, называемый узлами Events Driven (ED), например, отчет о событии

экстренной тревоги. Пакеты трафика, сгенерированные примечаниями ED, были смоделированы как процесс Пуассона.

Хотя авторы в [36] предложили модель трафика, которая выделяет отличительные характеристики трафика M2M, они сделали некоторые упрощающие предположения, которые не отражают поведение в обобщенном смысле. Первым предположением было то, что M2MD могут быть либо узлами FS, либо узлами ED. Это предположение делает модель применимой только для некоторых конкретных устройств M2M. Эти устройства могут выполнять только определенную работу, например, периодически сообщать о температуре, но не могут сообщать об инциденте, в котором температура выше определенного порогового значения. В настоящее время в большинстве практических систем большинство M2MD могут быть как узлом FS, так и узлом ED. Предположение о том, что все узлы ФС синхронизированы, может рассматриваться как чрезмерно упрощенное предположение. Авторы в [37] исследовали синхронизацию генерируемого машиной трафика, такого как сообщения об обновлении состояния маршрутизаторов, которые сообщают о текущем состоянии канала. Они продемонстрировали (аналитически и эмпирически), что переход поведения от асинхронизированного к синхронизированному происходит внезапно, даже если на него влиял внешний влияющий фактор (например, их одновременное включение). Синхронизация в случае M2MD является более сложной задачей, поскольку M2MD обычно подключаются к сети через беспроводное соединение, следовательно, неравенство задержек распространения и битовых ошибок играют существенную роль в сдерживании успешной синхронизации.

2.3.2 Марковски- модулированный пуассоновский процесс (MMPP)

Марковский процесс с двумя состояниями (как показано на рисунке 2.5) обычно используется в литературе для моделирования прибытия в очередь. Модель MMPP также использовалась для моделирования прибытия трафика M2M. Первое состояние, т.е. «Передача» или «Вкл», представляет M2MD, передающий данные. Второе состояние, то есть «Ожидание» или «Отключить», представляет собой M2MD, не передающий данные, также известный как спящий режим. PI,T представляет вероятность перехода из состояния ожидания в состояние передачи, а PT,I из состояния передачи в состояние ожидания.

Передача данных в модели MMPP получается из вероятности устойчивого состояния (то есть вероятности существования в конкретном состоянии, когда время приближается к бесконечности) состояния передачи. Следовательно, вероятность передачи PT может быть выражена [38] как:

$$P_T = \lim_{t\to\infty}(P_{I,T})^t = \lim_{t\to\infty}(1-P_{T,I})^t = \frac{P_{I,T}}{P_{I,T}+P_{T,I}} \qquad (2.2)$$

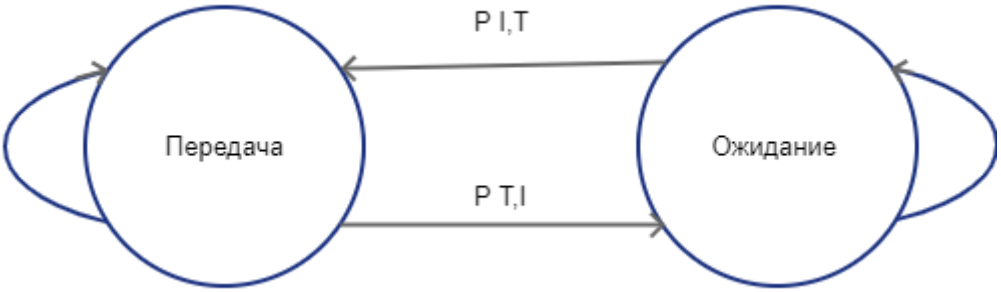


Рисунок 2.5 Марковский процесс с двумя состояниями

Хотя в литературе широко используется модель цепочки Маркова с двумя состояниями, она не является оптимальной моделью для трафика M2M через общий канал. Это связано с тем, что это зависит от процесса прибытия Пуассона, и здесь не так, как объяснялось ранее. Кроме того, пакеты данных M2MD обычно являются неоднородными и не могут рассматриваться как идентичные или представленные как состояние в цепочке Маркова с двумя состояниями. Например, периодическое обновление, сообщающее о состоянии батареи M2MD и изображение нарушителя, проходящего проверку безопасности, не может рассматриваться как идентичные передачи данных из-за размера и характера передаваемых данных. Кроме того, эта модель не учитывает инциденты блокирования, которые часто происходят в сетях с высокой плотностью пользователей, таких как IoT. Инцидент блокировки происходит, когда передатчик (то есть M2MD) имеет данные для передачи, но все каналы, предназначенные для данных в сети, полностью заняты.

2.3.3 Эмпирическая модель

Эмпирические модели опираются на эксперименты и тесты для их оценки. Как правило, модели, предлагаемые с использованием этой методологии, начинают с запуска эксперимента, а затем пытаются вписать собранные данные в соответствующее статистическое распределение. В последнее время исследователи использовали эмпирический подход и измерили трафик M2M в сотовой сети. Они пришли к выводу, что связь M2MDs окажет значительное влияние на связь смартфонов. В частности, M2MD будет конкурировать со смартфонами за доступные каналы, и, как следствие, вероятность блокировки возрастет. Хотя эмпирические модели иллюстрируют точный трафик, измеренный в сообщениях M2M, у них есть свои недостатки. Например, они представляют собой реактивный подход, который может описать только точный сценарий, для которого были собраны данные. Они не могут предложить обобщенную модель. Кроме того, подход, использованный в, может только моделировать агрегированный трафик, наблюдаемый через сеть.

2.3.4 Модель 3GPP

В сетях 3GPP при предоставлении услуг IoT, можно характеризировать трафик создаваемый ими следующими особенностями[39]:

– короткая продолжительность взаимодействия сеансов оконечных устройств;

– незначительный объем передаваемых трафиков;

– низкая мобильность оконечных M2M-устройств;

– массивность оконечных M2M-устройств;

– низкая потребление энергии;

– низкая потребность к вычислительной мощности;

– высокие требования к QoS

На рисунке 2.6 представлена архитектура сети 3GPP. Там показано варианты моделей взаимодействия сетей 3GPP с сетью M2M.

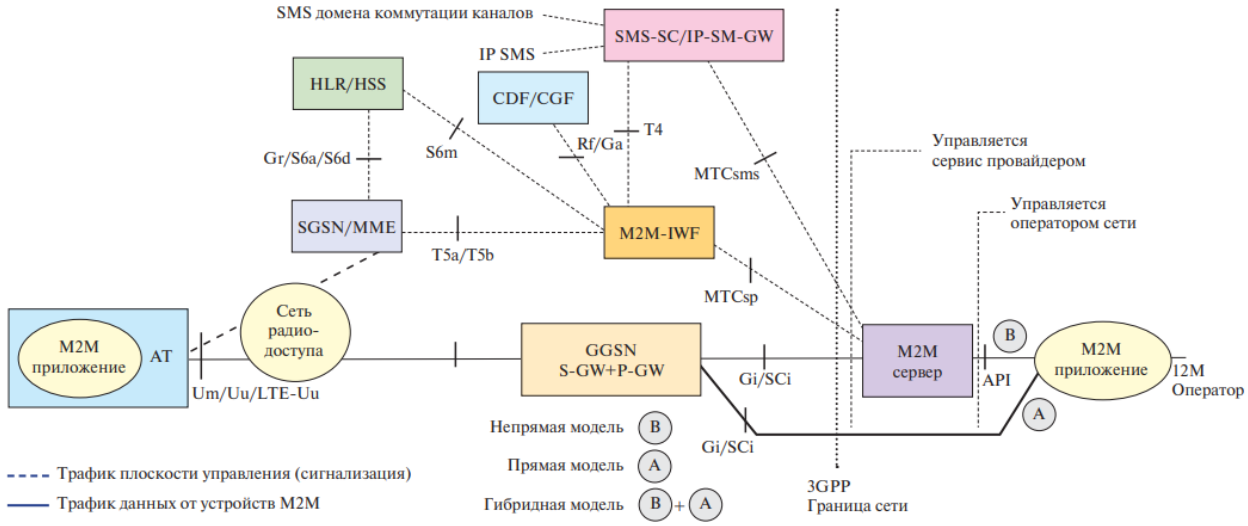


Рисунок 2.6 – Архитектура сети доступа M2M с использованием сети доступа LTE/3GPP[39]

2.3.5 Моделирование CMMPP

Синтетическая генерация трафика данных в соответствии с моделью CMMPP описана на блок-схеме на [40]. Требуются два вложенных цикла, как для устройств n, так и для временного индекса k соответственно. Матрица перехода P_n $[k]$ вычисляется заново для любой итерации в соответствии с уравнением:

$$P_n[k] = \Theta_n[k] * P_c + (1 - \Theta_n[k]) * P_U \qquad (2.3)$$

С точки зрения сложности это выполнимо, поскольку число состояний обычно мало, а требуемую выпуклую комбинацию можно эффективно вычислить. Случайное обновление состояния с $s_n[k\text{-}1]$ до $s_n[k]$ выполняется

впоследствии. Наконец, количество поступлений и размеров пакетов генерируется в соответствии с текущим состоянием $s_n[k]$. Подробное описание этой модели представление в [40]

2.4 Разработка модели трафика IoT/M2M как трафика конечных автоматов

M2M устройства, как правило, представляют собой конечные автоматы с низкой вычислительной сложностью, которые в основном состоят из датчика (ов), микропроцессора/контроллера и блока связи. Основной функцией M2M устройства является мониторинг среды и отправка отчета в централизованный узел для анализа данных. На рисунке 2.7 показана общая схема последовательности операций передачи данных M2M устройств.

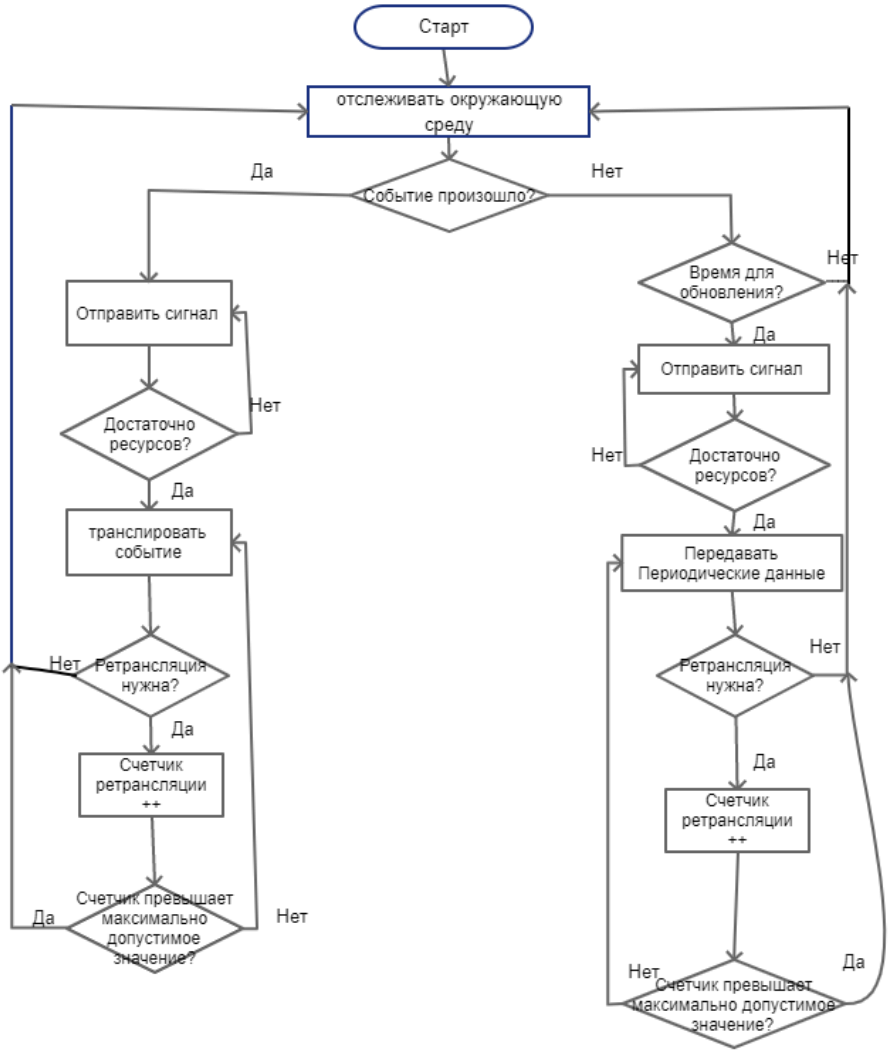


Рисунок 2.7 – Общая схема передачи данных M2M устройств.

Блок-схема показывает два типа данных, сгенерированных M2M узлах, то есть периодические обновления и данные отчетов об апериодических событиях.

Первоначально M2M устройство при запуске отслеживает окружающую среду (например, обнаруживает движение в комнате). После предварительно определенного периода M2M автомат отправляет периодическое обновление (то есть обновление состояний циклического перебора) на базовую станцию или централизованный узел. В случае инициированного прерывания (происходит событие, например, обнаруживается движение), M2M блок также передает исключительные, то есть непериодические, данные, чтобы сообщить о нем.

Предложенная модель связи M2M модуля показана на рисунке 2.8. Эта модель - это дискретный случайный процесс, состоящий из четырех состояний: Состояние покоя (S), По круговой (R), Прерывание (I) и Буфер (B). В любой момент M2M прибор считается находящимся в одном из этих четырех состояний и может перейти в другое состояние с определенной вероятностью, называемой переходной вероятностью. Переходная вероятность, показанные на рис. 4, представляют начальное состояние и конечное состояние. За основу этой модели было взято с материалов [41].

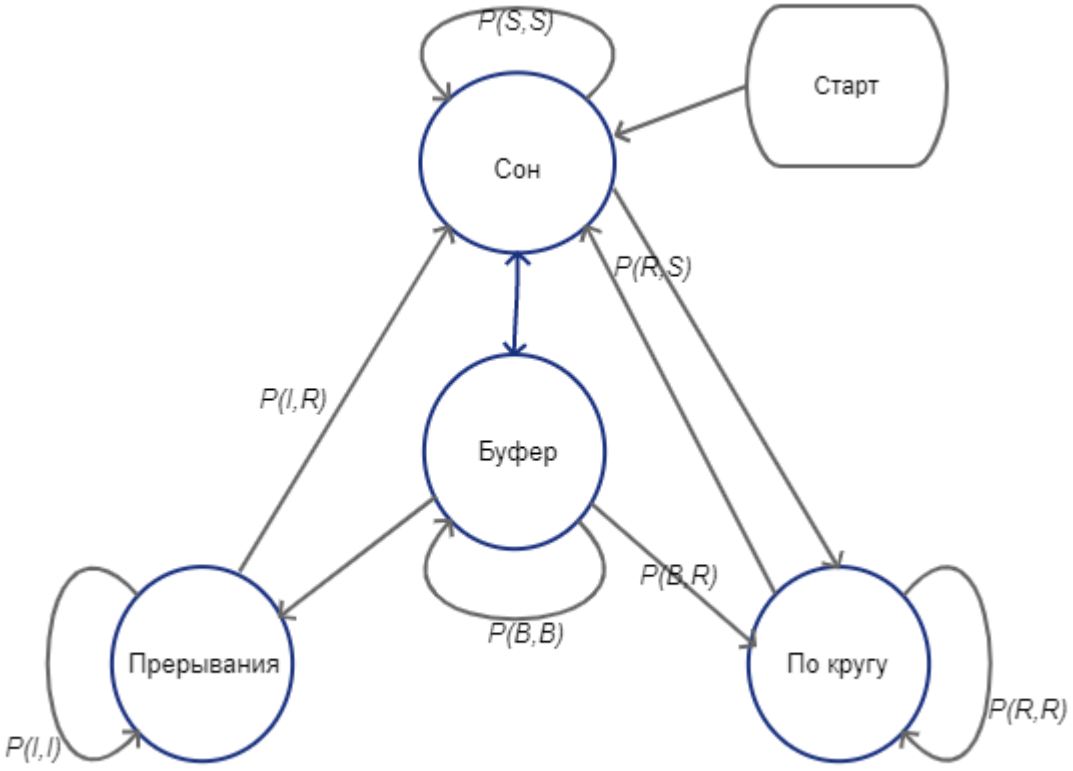


Рис 2.8 – Предлагаемая модель связи M2M устройств.

Состояние сна представляет собой начальное состояние конечного автомата, в котором M2M стенд не передает никаких данных. Состояние По Кругу представляет состояние, в которую M2M устройство передает данные регулярных периодических обновлений, например, периодический отчет о комнатной температуре. Во время состояния буфера M2M устройство имеет данные для отправки, но все еще ожидает доступа к совместно используемым каналам для их передачи. Кроме того, в случае полностью занятых каналов M2M блоки буферизует пакеты данных, пока не сможет получить доступ к каналу. Состояние прерывания представляет событие, происходящее в M2M узлах, в котором оно отправляет данные, представляющие событие, например, активируется сигнализация о взломе.

Модель моделируется как дискретный случайный процесс, в котором в каждой единице времени происходит переход состояния. Переход может быть в любое возможное состояние (включая само начальное состояние). Вероятности перехода определяют, в какое состояние наиболее вероятно переместиться в следующем временном интервале. Суммирование вероятностей перехода, выходящих из любого состояния, должно равняться единице следующим образом:

$$\begin{aligned} P_{S,S} + P_{S,R} + P_{S,B} &= 1 \\ P_{B,B} + P_{B,I} + P_{B,R} &= 1 \\ P_{R,R} + P_{R,S} &= 1 \\ P_{I,I} + P_{I,S} &= 1 \end{aligned} \tag{2.4}$$

Вероятности перехода, когда система находится в одном и том же состоянии, зависят от нескольких факторов. В частности P(S,S), который представляет вероятность оставаться в состоянии сна, зависит от частоты как периодических обновлений, так и происходящего события. Наличие ресурсов канала напрямую влияет на значение P(B,B). В частности, значение P(B,B) равно мгновенной вероятности блокировки канала. Длина пакета данных M2M датчиков и качество канала, например, отношение сигнал / шум (SNR), определяют значение как P(R,R) так и P(I,I). В настоящее время мы только считаем, что SNR влияет на скорость передачи данных. Следовательно, максимально достижимая скорость передачи информации может быть получен по формуле пропускной способности Шеннона и может быть получен как:

$$R_{k,j} = BW \log_2(1 + SNR_{k,j}) \tag{2.5}$$

$$P_{(R,R)/(I,I)} = 1/\gamma(t)_{(R,R)/(I,I)}$$

$$\gamma(t)_{(R,R)/(I,I)} = DR_{(R)/(I)} / R_{k,j}(t) \tag{2.6}$$

где BW - ширина полосы канала;

γ - количество единиц времени, которое необходимо для передачи данных;

[.] - предельное значение функции;

t – момент времени;

DR - состояние.

В сети с общими каналами существует два основных метода множественного доступа. Первым методом является централизованное планирование, в котором M2M аппарат должен отправить запрос планирования (SR) на централизованное устройство (скажем, базовую станцию) для доступа к каналу. Базовая станция управляет расписанием множественного доступа канала M2M узлам. Второй метод - это распределенное планирование, в котором каждый M2M модуль принимает локальное решение о том, должен ли он получать доступ к какому-либо конкретному каналу на основе методов определения канала.

В сети с централизованным планированием центральное устройство (например, базовая станция) планирует доступ к совместно используемому каналу M2M устройств. Следовательно, M2M датчику требуется отправить запрос планирования (SR) перед началом передачи данных. После того как базовая станция получает SR, она планирует указанный ресурс (такой как время и пара полосы пропускания) для M2M узлов. Таким образом, когда происходит прерывание (т.е. требуется асинхронная передача данных), M2M устройство должно хранить данные в своем буфере (то есть состоянии буфера). Продолжительность времени, которое пакеты данных проводят в буфере, представляет время отправки SR на базовую станцию и для планирования ресурса. С другой стороны, в состоянии по кругу пакеты данных передаются в заранее определенную эпоху (то есть в явно определенное время). Соответственно, M2MD отправляет SR на базовую станцию заранее, и периодические обновления M2M устройств не требуют буферизации данных.

Однако в сети с распределенным планированием вся передача данных (то есть передача данных выполняется состояниями прерывания и циклического перебора) должна буферизироваться до тех пор, пока M2M узлы не обнаружит канал и не определит незанятый канал перед передачей данных.

Вероятности перехода в коммуникационной модели M2M можно представить в виде матрицы перехода:

$$\delta = \begin{bmatrix} P(S,S) & P(S,R) & P(S,B) & P(S,I) \\ P(R,S) & P(R,R) & 0 & 0 \\ P(B,S) & P(B,R) & P(B,B) & P(B,I) \\ P(I,S) & 0 & 0 & P(I,I) \end{bmatrix} \quad (2.7)$$

где вероятности в каждой строке имеют одинаковое начальное состояние, а вероятности в каждом столбце имеют одинаковое состояние завершения.

Стационарные вероятности всех состояний обозначаются как *P(S), P(R), P(B) , P(I)* соответственно. Соответственно, стационарные вероятности могут быть выражены как стационарный вектор (Q):

$$Q = \left[P(S)P(R)P(B)P(I)\right], \quad где\ P(S)+P(R)+P(B)+P(I)=1 \tag{2.8}$$

Стационарные вероятности для M2M устройств для предложенной модели коммуникации могут быть получены с использованием уравнения статического равновесия:

$$\delta \times Q = Q или Q(\delta - 1) = 0 \tag{2.9}$$

M2M устройства передают данные только в двух состояниях, то есть По кругу и Прерывания. Следовательно, количество переданных пакетов может быть получено из MCM с использованием вероятности передачи данных устройством и количества устройств в интересующей области (n):

$$NP = P_T \times n \tag{2.10}$$

$$P_T = P_r \bigcup P_i \tag{2.11}$$

Для моделирования M2M устройства использовался имитатор дискретных событий [42] для оценки поведения сети. В работе было показано, что подход распределенного планирования может превзойти подход централизованного планирования, когда существует задержанная информация о состоянии канала (CSI). В сети с высокой плотностью пользователей (такой как сеть, обрабатывающая много M2M узлов), вероятность задержки CSI высока, поэтому в этой модели мы изучили передачу пакетов в сети с распределенным планированием. Предполагается, что вероятность доступа к каналам является равновероятным доступом через M2M девайсов, то есть считается, что все M2M устройства имеют одинаковый приоритет. Для моделирования рассматриваются пять M2M девайсов (т.е. n = 5), совместно использующих три канала. Параметры и соответствующие значения, используемые для получения численных результатов и результатов моделирования, таковы: Продолжительность моделирования: $10*10^4$едениц вермени; Количество M2M устройтсв: 5; Количество каналов: 3; *SNR* 1: 1/10; *SNR* 2: 1/30; Обновления рассылки: детерминированный,в среднем 10с; Распределение прерываний: Пуассон со средним 50с; Требования к данным: 150 / 1500 Кбит/с; P для модели Пуассона: экспоненциальное распределение со средним 10с; P_{bx}:0.

Количество пакетов, передаваемых в M2M по отношению к единицам времени, показано на рисунке 2.9. Как показано на рисунке, MCM способен более точно моделировать моделируемый M2M устройствами трафик. В частности, в случае, когда *y(R,R)* и *y(I, I)* равны единице и десяти соответственно, то есть *SNR1*, MCM может прогнозировать количество передаваемых пакетов со значительно более высокой точностью. Например, в *SNR1* количество пакетов, полученных путем моделирования, составляет 3×10^4 для единицы времени 5×10^4 , а использование MCM составляет $3{,}041 \times 10^4$, что составляет ошибку менее 1,4%. С другой стороны, в сценарии *SNR2* не так точно. Однако, используя модель MMPP, которая не адаптируется по отношению к *SNR* (на рисунке 2.9 обозначается как Пуассон), прогнозируемое число составляет $2{,}5 \times 10^4$, что составляет ошибку около 16,7%.

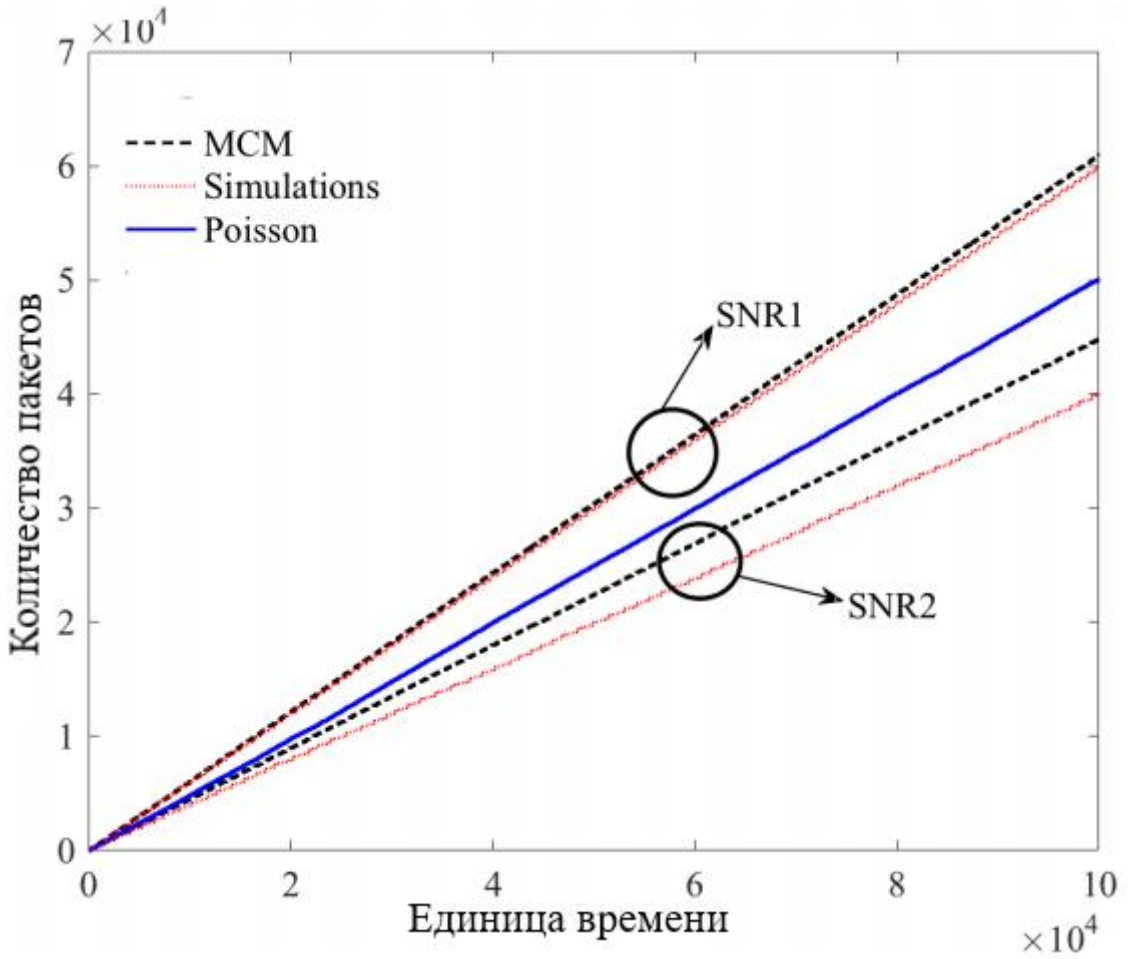


Рисунок 2.9 Количество переданных пакетов относительно единицы времени.

В этой модели предлагается связь M2M, более подробно изучив поведение M2M устройств. Затем мы использовали модель связи для оценки передаваемого трафика. Генерированный трафик имеет несколько других факторов, влияющих на него, таких как пропускная способность канала и используемая техника множественного доступа.

3 Моделирование трафика IoT/M2M в сети с протоколом MQTT

3.1 Протокол MQTT

Протокол MQTT (message queuing telemetry transport) – сетевой протокол, работающий поверх TCP/IP, предназначенный для обмена сообщениями между устройствами. Протокол MQTT обеспечивает стандартные основы связи для IoT, реализованные в виде архитектуры «издатель-подписчик» [43]. Протокол ориентируется на простоту в использовании, невысокую нагрузку на каналы связи, работу в условиях постоянной потери связи, лёгкую встраиваемость в любую систему. Основное предназначение — работа с телеметрией от различных датчиков, устройств, использование шаблона подписчика обеспечивает возможность устройствам выходить на связь и публиковать сообщения, которые не были заранее известны или предопределены, в частности, протокол не вводит ограничений на формат передаваемых данных. Данный протокол используется для межмашинной связи, когда пропускная способность сети ограничена и требуется небольшой объем кода. Издатель/подписчик - это хорошо зарекомендовавшая себя коммуникационная парадигма, которая позволяет издателю передавать свои сообщения любому количеству подписчиков через центральную точку связи, то есть MQTT-брокер. Каждое сообщение, отправляемое брокеру (посреднику), будет связано с определенной темой, при этом каждый клиент MQTT должен иметь уникальный ID идентификатор клиента. Брокер использует тему в качестве информации о маршрутизации, где каждый клиент, который хочет получать сообщения, подписывается на определенную тему, и посредник будет отвечать за распространение всех сообщений, относящихся к соответствующей теме. MQTT - это тематический протокол связи, в котором клиенты общаются по темам без каких-либо зависимостей между издателями данных и подписчиками. Модель издатель-подписчик показана на рисунке 3.1. Как правило, приложения IoT можно разделить на две группы: приложения на основе событий и на основе участия. Приложения на основе событий, где устройства IoT запускаются для сбора информации по конкретным событиям, таким как мониторинг аварийных ситуаций, безопасность наблюдения, управление трафиком, система интеллектуальной парковки и супермаркеты / розничные магазины. Для приложений, которые основаны на участии и периодическом восприятии относятся мониторинг здравоохранения, интеллектуальные сети, погодный сигнал, качество воды и воздуха. Таким образом, в нашей работе мы принимаем эти два вида приложений IoT и связанные с ними шаблоны трафика. Стоит отметить, что для каждого типа трафика требуется разное время обработки.

Брокер выступает в качестве почтового отделения, MQTT и не использует адрес предполагаемого получателя, а использует строку темы под названием «Тема», и любой, кто хочет получить копию этого сообщения,

подпишется на эту тему. Несколько клиентов могут получить сообщение от одного брокера (возможность «один ко многим»). Аналогично, несколько издателей могут публиковать темы для одного подписчика (от многих к одному).

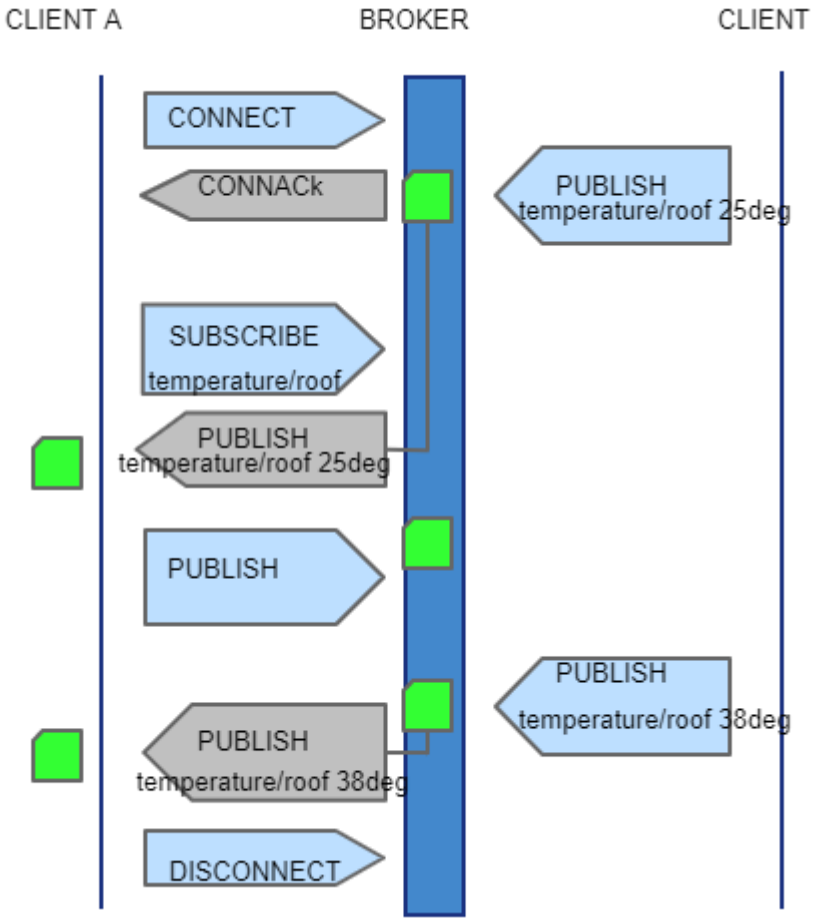


Рисунок 3.1 – Структура модели издатель/подписчик .

Каждый клиент может производить и получать данные как путем публикации, так и подписки, то есть устройства могут публиковать данные датчиков и при этом иметь возможность принимать информацию о конфигурации или команды управления (MQTT - это протокол двунаправленной связи). Это помогает как для обмена данными, управления и контроля устройств.

Благодаря архитектуре брокера MQTT устройства и приложения становятся более изолированными и более безопасными. MQTT использует шифрование Transport Layer Security (TLS) с именем пользователя, защищенными паролем соединениями и дополнительными сертификатами, которые требуют, чтобы клиенты предоставили файл сертификата, который совпадает с файлом сервера. Клиенты не знают IP-адреса друг друга.

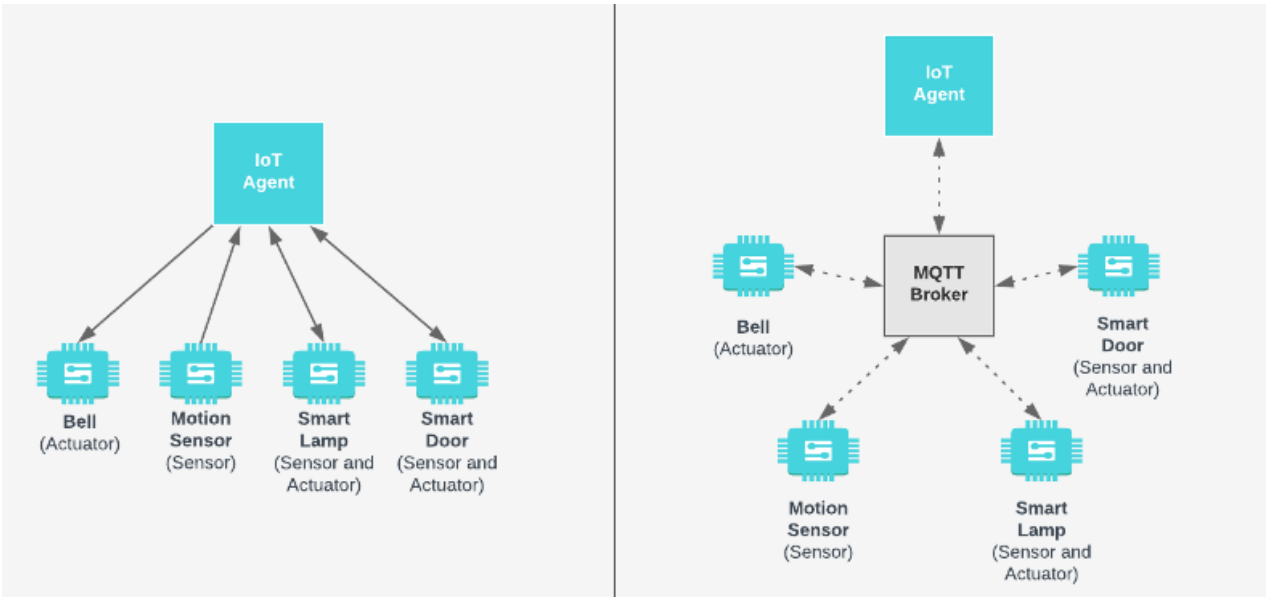
В случае одного источника сбоя, программное обеспечение брокера и клиенты имеют автоматическую передачу в резервный / автоматический

резервный брокер. Брокер резервного копирования также может быть настроен для распределения нагрузки клиентов между несколькими серверами на месте, облаком или комбинацией обоих.

Брокер может поддерживать как стандартные MQTT, так и MQTT для совместимых спецификаций, таких как Sparkplug [44] , может выполняться на одном сервере, в одно и то же время и с одинаковыми уровнями безопасности.

Таблица 3.1 – Сравнения протоколов [45]

HTTP	MQTT
Агент IoT напрямую связывается с устройствами IoT	Агент IoT связывается с устройствами IoT косвенно через брокера MQTT
Парадигма запрос-ответ	Парадигма публикации-подписки
IoT-устройства всегда должны быть готовы к приему сообщений	IoT-устройства выбирают, когда принимать сообщения
Более высокие требования к мощности	Требование к низкой мощности
Высокие требования к трафику	Низкие требования к трафику
Высокая надежность поддерживаемая уровнями QoS	Низкая надежность



a) b)

Рисунок 3.2 – Различия между транспортными протоколами a) HTTP b) MQTT

Посредник может хранить данные в виде сохраненных сообщений (необходимо подписаться с клиентом базы данных), чтобы новые подписчики на тему могли сразу получить последнее значение.

Посредник также отслеживает всю информацию о сеансе, поскольку устройства включаются и выключаются, что называется «постоянными сеансами».

Основные преимущества брокера MQTT:

– Устраняет уязвимые и незащищенные клиентские подключения;

– Может легко масштабироваться от одного устройства до тысяч;

– Управляет и отслеживает все состояния подключения клиента, включая учетные данные и сертификаты безопасности;

– Снижение нагрузки на сеть без ущерба для безопасности (сотовая или спутниковая сеть)

До разработки этого протокола использовался HTTP, в качестве транспортного механизма между устройствами и IoT агентом. HTTP использует парадигму запрос / ответ, где каждое устройство подключается напрямую к агенту IoT. MQTT отличается тем, что публикация-подписка основана на событиях и отправляет сообщения клиентам, смотрите рисунок 3.2 и таблицу 3.1. Для этого требуется дополнительная центральная точка связи (известная как брокер MQTT), которая отвечает за рассылку всех сообщений между отправителями и законными получателями. Каждый клиент, который публикует сообщение для брокера, включает в сообщение тему. Тема является маршрутной информацией для брокера. Каждый клиент, который хочет получать сообщения, подписывается на определенную тему, и брокер доставляет все сообщения с соответствующими темами для клиента. Поэтому клиенты не должны знать друг друга, они общаются только по теме. Эта архитектура позволяет масштабируемые решения без зависимостей между производителями данных и потребителями данных.

3.2 Модель системы

Наша система рассматривает сценарий применения MQTT, показанный на рисунке 3.3, в котором датчики на основе IoT собирают определенную информацию, а затем передают ее на соседние коммутаторы вплоть до брокера [46]. Мы предполагаем, что сетевые коммутаторы достаточно умны, чтобы программировать их удаленно и действовать в соответствии с изменениями трафика. Это предположение может соответствовать новым появляющимся технологиям, таким как программно-определяемые сети (Software-Defined Networking (SDN)). Посредник распространит данные о заинтересованности в приложениях подписки (Ai, i = 1, 2, ..., M) и информацию об управлении трафиком для коммутаторов на пути, чтобы заблокировать или позволить клиентам MQTT снизить нагрузку на сеть. Два типа приложений IoT развертываются с приходом пакетов с детерминированными (приложениями на основе участия) и случайными (приложениями на основе событий). Таким образом, воспринимающая информация, то есть поступление пакета данных IoT, моделируется как фиксированным, так и экспоненциальным временем между приходами со скоростями γm, m = 1, 2 .., n, n + 1 .., M

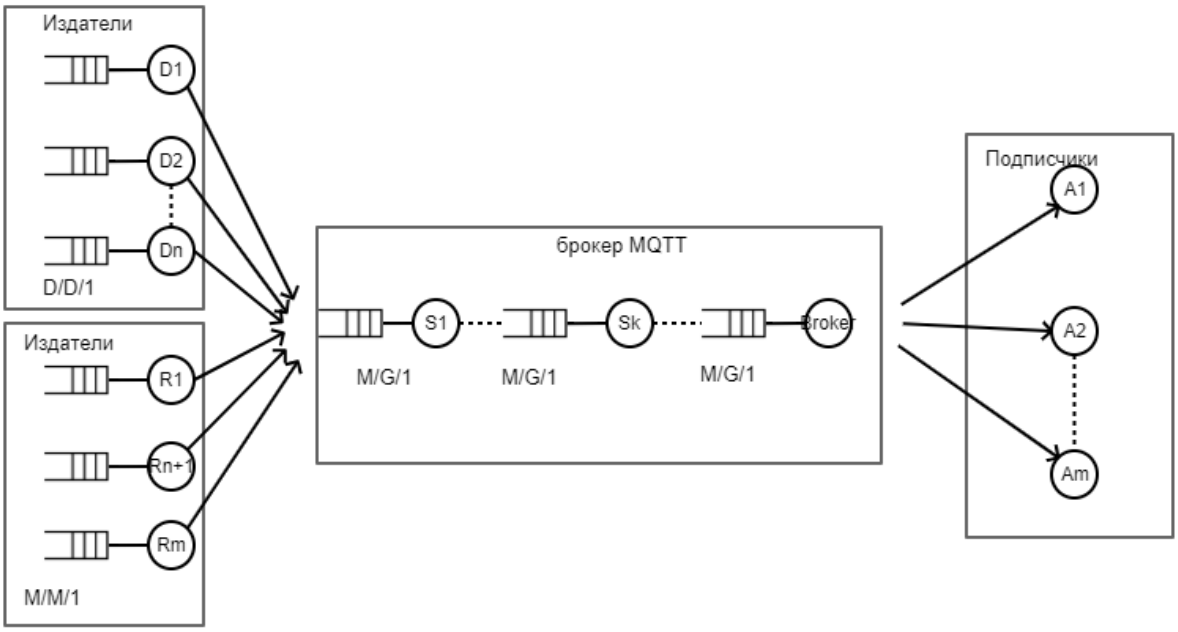


Рисунок 3.3 – Структура системы

Детерминированное приложение на стороне издателя имеет скорость поступления

$$\lambda_D = \sum_{i=1}^{n} \gamma \tag{3.1}$$

в то время как случайные поступления пакетов от основанных на событиях издателей предполагаются распределенными по закону Пуассону со скоростью

$$\lambda_R = \sum_{J=n+1}^{M} \gamma_j \tag{3.2}$$

Мы используем две приоритетные очереди с экспоненциально распределенной скоростью поступления пакетов и произвольным распределением для скорости обслуживания. Следовательно, промежуточный узел и коммутаторы ретрансляции моделируются как одиночные серверные средства с очередью M/G/1, которые отвечают за пересылку данных IoT подписанным клиентам. Из-за распределенной природы устройств IoT брокер является узким местом в нашей сети. Мы стремимся ограничить количество пакетов, поступающих в центральный брокер, чтобы предотвратить перегрузку сети. Посредник работает в очередях без приоритетов M/G/1 с экспоненциально распределенным временем между поступлениями λ и

средним временем обслуживания X. Считается, что случайные пакеты (то есть трафик IoT на основе событий) имеют более высокий приоритет.

Частота поступления пакетов (скорость трафика) и общее количество издателей (объем трафика) являются двумя важными факторами, снижающими нагрузку на сеть. Наша модель экспериментально поддерживает и анализирует ряд предыдущих показателей скорости поступления пакетов в IoT-брокере, чтобы определить достоверность, при которой повышенная интенсивность поступления (λ) находится в определенном для приложения диапазоне или нет. В этом случае скорость пакетов не должна превышать максимальную скорость прихода λ_{max}. С другой стороны, максимально допустимые издатели M_{max} должны быть определены в соответствии с требованиями QoS. Таким образом, вероятность блокировки устройства IoT для предотвращения высокой сетевой нагрузки определяется выражением:

$$P_{бокировка} = \Pr\{\lambda > \lambda_{max} \square M > M_{max}\} \quad (3.3)$$

Конечная цель нашей работы - проанализировать метод предотвращения высокой нагрузки трафика в сети IoT, одновременно сводя к минимуму негативное влияние на пользователей системы. Наши основные задачи заключаются в следующем:

1) рассчитать максимальную частоту поступления пакетов, которая полностью отражает внутренние характеристики узла-издателя;

2) рассчитать максимальный интервал выборки для расчета текущей скорости пакетов, чтобы общая задержка в очереди должна соответствовать заранее заданному порогу QoS;

3) рассчитать максимальное количество издателей, которое может обслуживать система, не превышая некоторых ограничений по задержке.

Чтобы решить поставленные задачи в сети IoT, мы анализируем модель очередей (рисунок 3.1) для сети IoT-MQTT и оцениваем механизм обнаружения на основе скорости поступления собранного трафика и количества пользователей до того, как произойдет высокая нагрузка на сеть.

Рассмотрим аналитические выражения для основных измерений производительности QoS, которые могут зависеть от высокой сетевой нагрузки с точки зрения времени отклика системы, задержки в очереди и общего количества пакетов, поступивших в центральный брокер [7]. Обозначения применяемые в данной работе:

M – количество MQTT издателей (устройств ИВ);

M_{max} – максимальное количество MQTT издателей которые могут обслуживаться системой;

T_{QoS} – предопределенный порог задержки для QoS, с.;

Q – общая задержка в очереди, с.;

λ – скорость поступления пакетов, пакеты/с.;

λ_{max} – максимальная скорость поступления пакетов, пакеты/с;

X – средняя время обслуживания у брокера, с.;

X_2 - вторичное время обслуживания у брокера, с.;

R – среднее остаточное время, с.;

W – среднее время ожидания, с.;

T – среднее время ответа, с.;

N – среднее количество пакетов;

I – интервал выборки для расчета текущей максимальной скорости поступления пакета, с.

Проведем анализ двух типов пакетов данных: случайных (R - random) и детерминированных (D - deterministic) пакетов с различными классами приоритетов. Для каждого класса приоритета $p \in \{R, D\}$ пакеты поступают согласно пуассоновскому закону распределения с $\lambda = \lambda_D + \lambda_R$, время обслуживания имеет среднее значение X, а второй момент - X_2

Для достижения нашей цели сначала отметим, что среднее время ожидания пакетов с высоким приоритетом (то есть случайных пакетов), обозначенное как W_R, определяется как:

$$W_R = \frac{R}{(1-\rho_R)} \tag{3.4}$$

где $\rho_R = \lambda_R \cdot X_R$ - доля времени, в течение которого брокер обслуживает трафик с высоким приоритетом или простым языком коэффициент загрузки канала обслуживания, а R - остаточное время. Это остаточное время может быть записано как:

$$R = \frac{1}{2}\left(\left(\rho_R + \rho_D\right) * \frac{X_2}{X}\right) \tag{3.5}$$

Выражения среднего времени ожидания, обозначенные как W_D, для пакетов с более низким приоритетом (то есть детерминированных пакетов) могут быть выражены как:

$$W_D = \frac{R}{(1-\rho_R)(1-\rho_R-\rho_D)} \tag{3.6}$$

где нагрузка ρ_D определяется как $\rho_D = \lambda_D \cdot X_D$. Общее время пакетов в классе $p \in \{R, D\}$, проведенных в системе, составляет:

$$T = W + X. \tag{3.7}$$

Общее количество пакетов для каждого класса определяется как:

$$N = \lambda * W. \tag{3.8}$$

Собирая и экспериментально анализируя достаточно большое количество исторических значений прихода λ_{max} для каждого типа трафика у брокера MQTT, можно добиться чистого разделения между устройствами IoT. Предложенная модель повышает быстродействие брокера IoT при любых превышениях пакетов. При обнаружении каких-либо лишних запросов от одного или нескольких издателей MQTT брокер соответствующим образом реагирует на такой объемный трафик и останавливает ненадлежащее поведение устройств IoT.

Ожидается, что при большом количестве пакетов, вызванном допустимым пакетом, максимальное значение последовательного λ в коротком временном интервале будет близко к λmax, поскольку высокое использование сетевых ресурсов сохраняется только в течение короткого периода времени. Большее значение λ можно считать тем, что событие более вероятно из-за неправомерной нагрузки трафика. Для поддержки предварительно определенного QoS общая задержка, испытываемая способом обнаружения, не должна превышать предварительно определенный порог T_{QoS}. Следовательно, кумулятивная задержка может быть напрямую связана с интервалом выборки, обозначенным I, для сбора и вычисления текущего максимума λ. Таким образом, если мы допустим, чтобы Q была случайной величиной, которая обозначает общую задержку в очереди, то максимально допустимый интервал выборки, который учитывает ограничение задержки QoS, определяется как:

$$I = \arg\max\left\{Q \le T_{QoS}\right\} \tag{3.9}$$

$$Q = W_R + W_D \tag{3.10}$$

Кроме того, целевая система может быть заполнена запросами от большого количества распространенных издателей IoT. Таким образом, существует жесткое ограничение на количество издателей, которые может обслуживать каждая система. Этот предел может быть определен общими ограничениями задержки T_{QoS}, наложенными требованиями приложения. Затем максимально допустимое количество издателей, которых может обслуживать система как в формуле (3.11), где M_{max} - это максимальное количество издателей IoT для приложений обоих типов (на основе участия и на основе событий).

$$M_{max} = \frac{T_{QoS}}{Q} \tag{3.11}$$

Передавая информацию об управлении трафиком (λ_{max} *и* M_{max}) на границы сети, можно избежать высокой нагрузки на сеть и контролировать объемный трафик IoT.

3.3 Моделирование Matlab / Simulink

3.3.1 Моделирование систем M/M/1

Теория массового обслуживания, или очередей (англ. queueing theory), — раздел теории вероятностей, целью исследований которого является рациональный выбор структуры системы обслуживания и процесса обслуживания на основе изучения потоков требований на обслуживание, поступающих в систему и выходящих из неё, длительности ожидания и длины очередей [47]. Этот подход применяется к различным типам задач, в частности, для проектирования сетевой системы [48]. Существует некоторая модель массового обслуживания, которая может быть реализована в сетевой системе, которая обычно делится на детерминистическую и вероятностную модель.

M/M/1 - система массового обслуживания (СМО), в которой прибытия пакетов определяются законом Пуассона со скоростью λ, а время обслуживания пакетов имеет экспоненциальное распределение с интенсивностью μ. Один сервер обрабатывает содержимое пакетов по одному с дисциплиной «первым пришел - первым обслужен». Когда обслуживание завершено, пакет покидает очередь, и количество пакетов в системе уменьшается на единицу. Буфер имеет бесконечный размер, поэтому нет ограничений на количество пакетов, которые он может содержать.

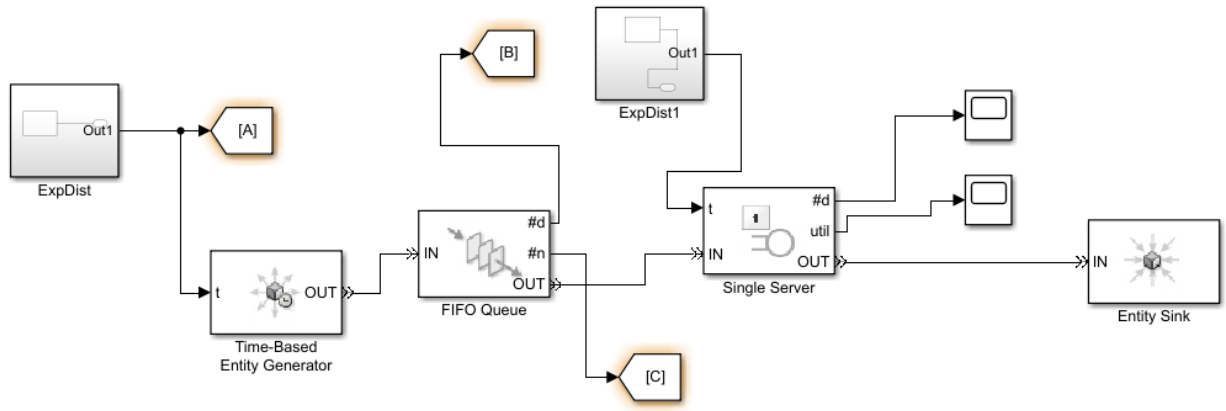


Рисунок 3.4 – Имитационная модель СМО вида M/M/1

В модели массового обслуживания M/M/1, рисунок 3.4, количество пакетов (N) в системе в стационарном состоянии формулируется следующим уравнением:

$$N = \frac{\rho}{1-\rho} \tag{3.12}$$

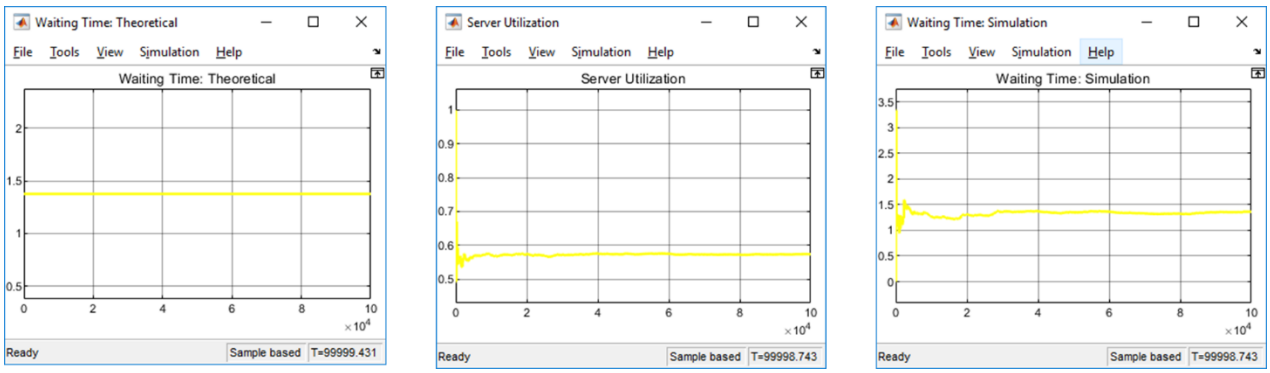
где $\rho = \lambda / \mu$ - коэффициент использование системы [49]. Более того, согласно теореме Литтла, среднее число пакетов в очереди (Nq) может быть сформулировано как $N_q = \lambda W$ [48]. В качестве альтернативы, N_q может быть определен следующим образом:

$$N_q = N - \rho = \frac{\rho}{1-\rho} - \frac{\rho*(1-\rho)}{1-\rho} = \frac{\rho^2}{(1-\rho)} \tag{3.13}$$

Следовательно, время ожидания пакета (W) может быть найдено на основе (2) следующим образом:

$$W = \frac{N_q}{\lambda} = \frac{\rho^2}{\lambda(1-\rho)} = \frac{\rho}{\mu-\lambda} \tag{3.14}$$

Моделирование модели M/M/1 изображено на рисунке 3.4. Интенсивность поступления пакетов по закону Пуассона представляет коэффициент усиления сигнала скорости с коэффициентом умножения «1». Выходной сигнал является входом для основанного на времени генератора пакетов. Экспоненциальное распределение скорости обслуживания представлено сигналом скорости с коэффициентом умножения «1». Результаты сравнения использования системы и очереди системы времени ожидания между теоретическим и имитационным моделированием изображены на рис. 3.5 с использованием λ = 0,5 и μ = 0,5.



a) b) c)

Рисунок 3.5 –. Результат сравнения M/M/1 от SimEvents. (a) Теоретический результат времени ожидания системной очереди; (b) результат моделирования использования системы; (c) Результат моделирования времени ожидания системной очереди.

3.3.2 Моделирование M/G/1

Система массового обслуживания M/G/1 представляет собой односерверную систему, куда клиенты приходят в соответствии с законом Пуассона со скоростью λ, а ее функция распределения составляет:

$$A(t) = 1 - e^{-\lambda t}, t \geq 0 \tag{3.15}$$

Время обслуживания является независимым и идентично распределяется с помощью общей функции распределения. Модель M/G/1 показана на рисунке 3.6.

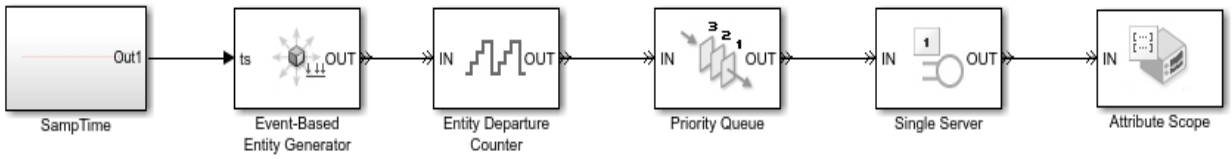


Рисунок 3.6 – Модель M/G/1

Средняя скорость обслуживания обозначается через μ, функция распределения времени обслуживания:

$$B(x) = P\{x < S\} \tag{3.16}$$

где S - случайная величина, описывающая время обслуживания, а ее функция плотности:

$$B(x)dx = P\{x < S \leq x + dx\} \tag{3.17}$$

Если B (x) является экспоненциальным распределением, мы имеем систему массового обслуживания M/M /1 или, если времена обслуживания постоянны, мы получаем систему массового обслуживания M/D/1. Это особые случаи систем массовых обслуживаний M/G/1.

Чтобы проверить предложенную нами модель, выполняется моделирование с использованием MATLAB / Simulink, где топология сети представлена на рисунке 3.7. Основной узел MQTT моделируется как одна очередь M / G / 1 с обычно распределенным временем обслуживания 2000 пакетов в секунду. Узлы издателя подключены к брокеру MQTT, и, как упоминалось выше, рассматриваются две категории опубликованных приложений с постоянным и пуассоновским трафиком данных.

Для моделирования выбран следующий пример сети Интернета вещей. В трех городах установлены устройства IoT, снимающие данные о погоде, где в каждом городе имеется 1000 устройств IoT, которые генерируют данные с

постоянной скоростью один пакет каждые 15 миллисекунд. Также было смоделировано четыре автомобильные стоянки с 1000 IoT-датчиками, которые генерируют пуассоновский трафик со средней скоростью поступления одного пакета каждые 64 миллисекунды. Как описано выше, два фактора сыграли главную роль в предотвращении высокой сетевой нагрузки: максимальная скорость поступления издателя λ_{max} и общее количество узлов издателя M_{max}.

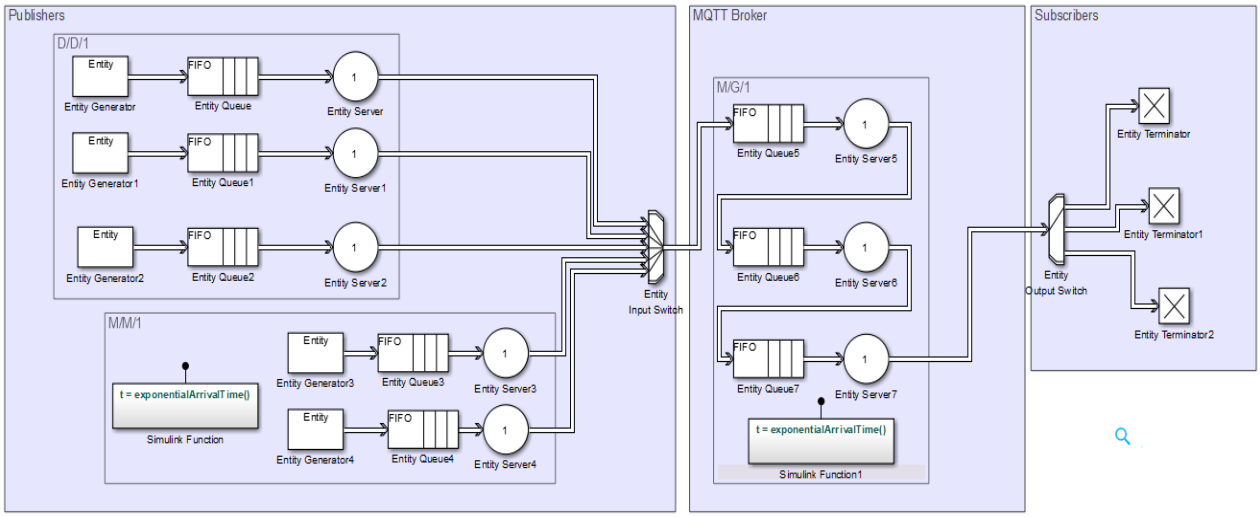


Рисунок 3.7 – Имитационная модель для MQTT

3.4 Оценка эффективности предложенной модели

Получены результаты моделирования, связанные с максимальной скоростью прибытия λ_{max}. По этой причине наше моделирование выполняется в течение относительно длительного периода времени, чтобы иметь возможность поддерживать ряд временных показателей прибытия. Из рисунка 3.8 можно заметить, что скорость трафика интеллектуальной парковки находится в диапазоне от 0 до 9 пакетов / миллисекунд, в то время как приложение для передачи метеорологического сигнала имеет максимум 8 пакетов / миллисекунду, смотрите на рисунок 3.8. MQTT-брокер ведет список максимально допустимой скорости поступления для каждого клиента и сообщает политику трафика (максимальную скорость поступления) программируемым коммутаторам точки входа. Коммутаторы постоянно собирают статистику и обновляют свои решения в зависимости от состояния сети и потребностей брокера. В этот момент, если частота поступления конкретного MQTT-клиента (устройства IoT) в интервале выборки 100 миллисекунд выше максимальной частоты поступления с вероятностью 98%, тогда этот клиент будет заблокирован для устранения нагрузки на сеть.

Реакция системы с и без нашего метода IDIoT была смоделирована. Мы запустили симуляцию в течение 100 секунд. На 50-й секунде один город и две автостоянки начинают отправлять с более высокой скоростью один пакет каждые 1,5 миллисекунды и один пакет каждые 6,4 миллисекунды,

соответственно. Такого рода изменения в скорости передачи данных могут быть сделаны преднамеренно или нет. Наша система определила переоцененные устройства и реагирует только на них, сохраняя поведение системы стабильным для других обычных пользователей. Как показано в рисунках 3.9 и 3.10, средняя загрузка сервера MQTT составляет 0,13 в нормальных условиях, но при загрузке сети она увеличивается до 0,39. Из этого можно сделать вывод, что в условиях высокой сетевой нагрузки сервер чрезвычайно обременен запросами большого объема, что приводит к увеличению использования. В какой-то момент сервер в конечном итоге достигает очень высокого уровня использования и не может принимать запросы от клиентов системы. В отличие от этого, когда рассматривается наш метод, MQTT-брокер может идентифицировать клиентов с ненормальным поведением точно по их идентификатору клиента и поддерживать систему в стабильном состоянии, чтобы отвечать другим клиентам. Это дает четкое представление о преимуществах использования мощности протокола MQTT-IoT и метода IDIoT.

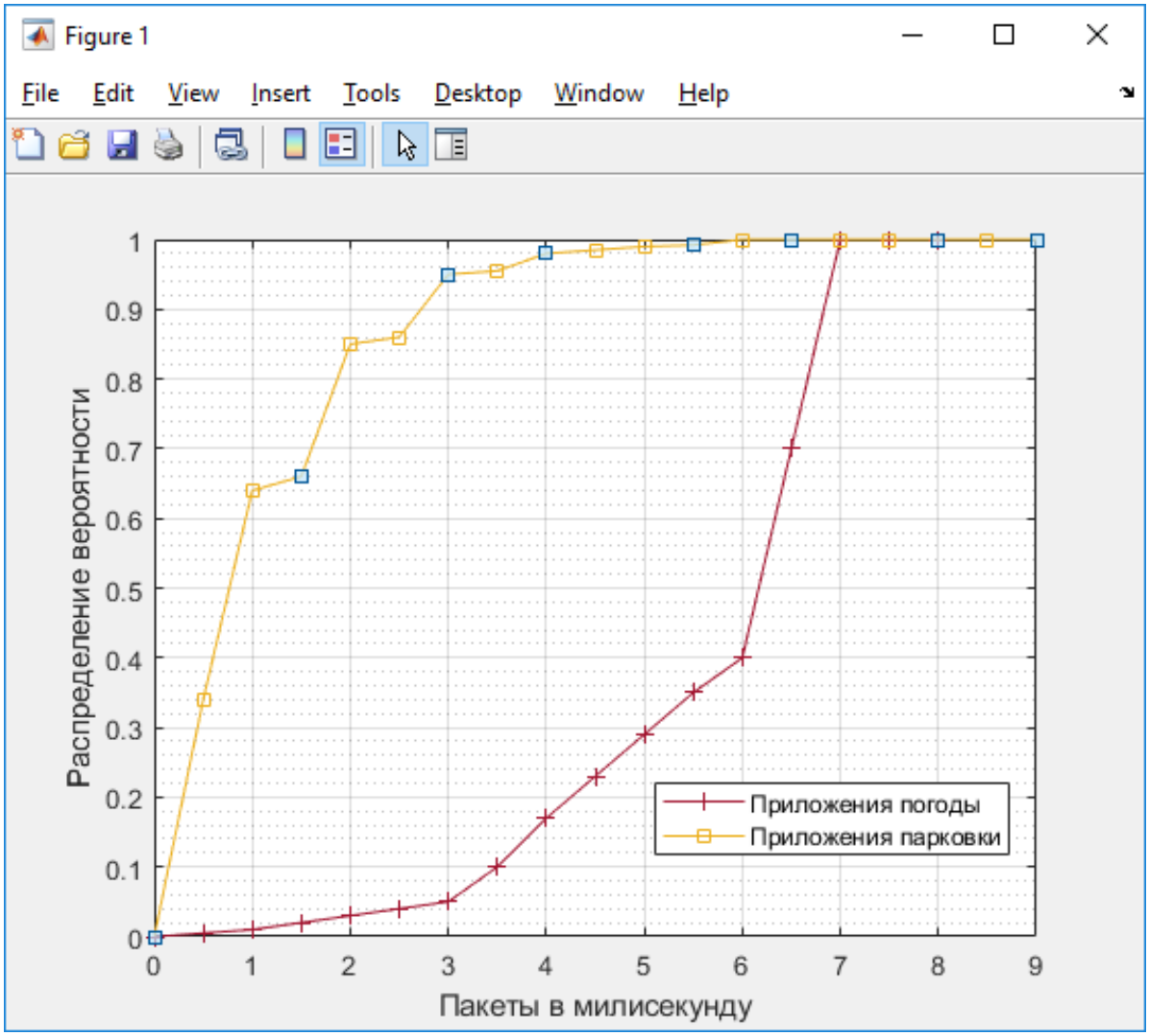


Рисунок 3.8 – Распределение скорости поступления пакетов

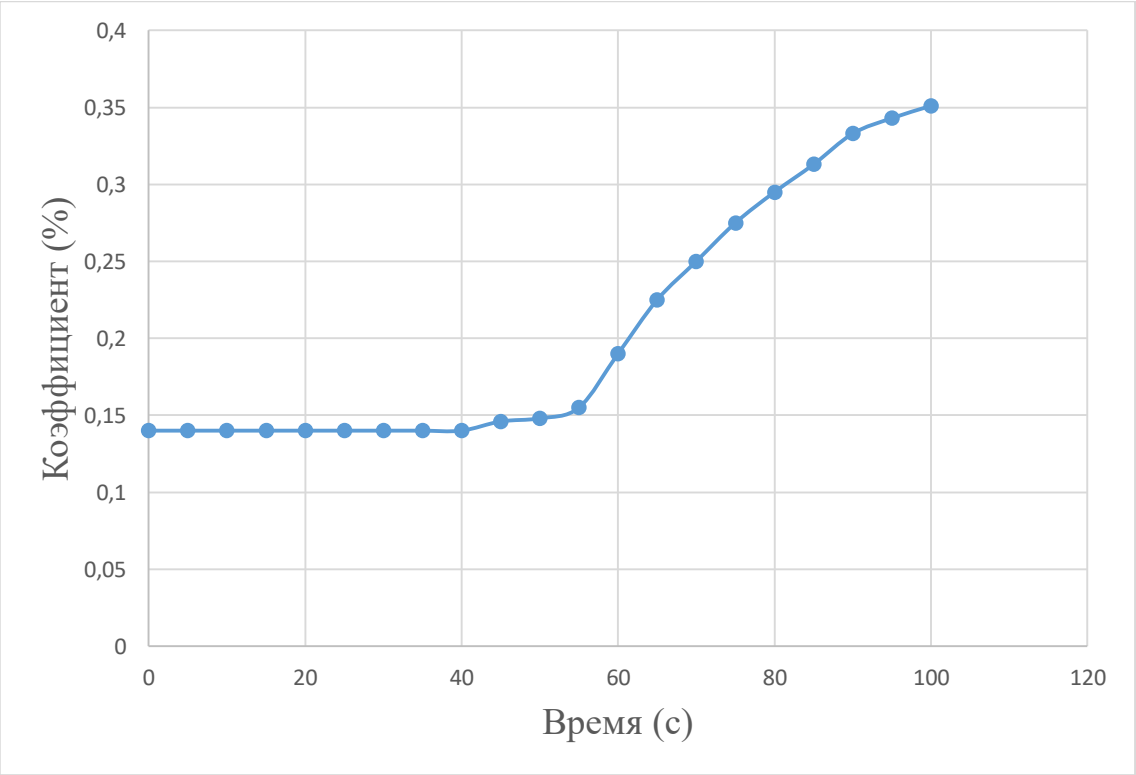


Рисунок 3.9 – Моделирование коэффициента использования MQTT брокера без идентификатора IoT

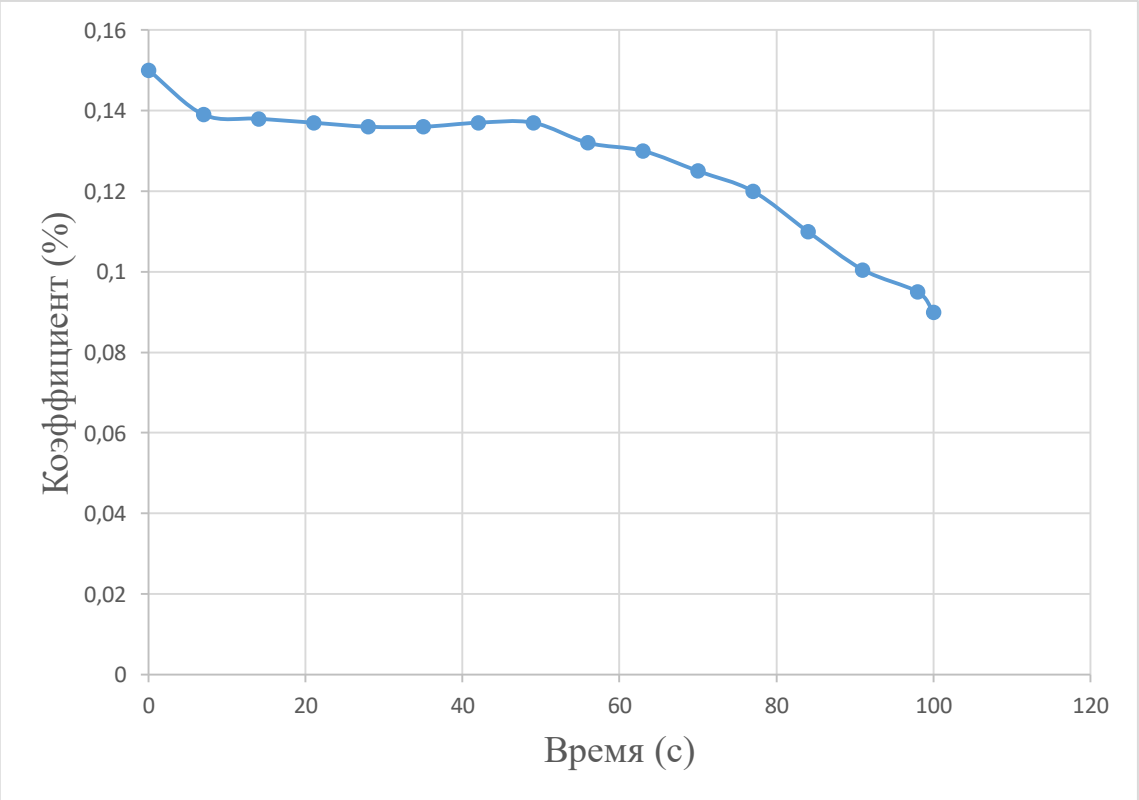
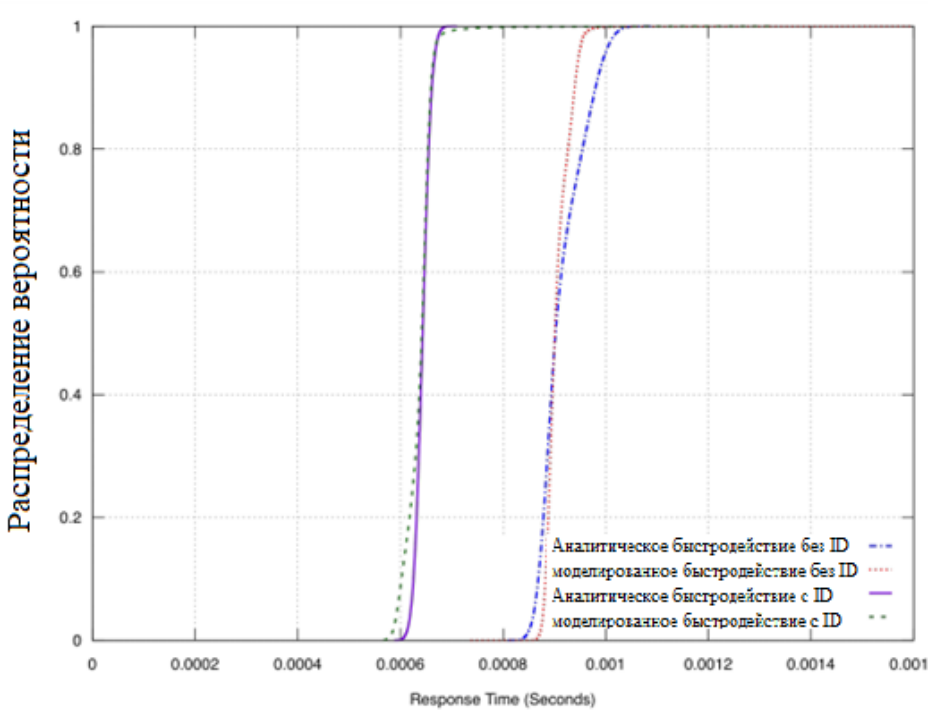
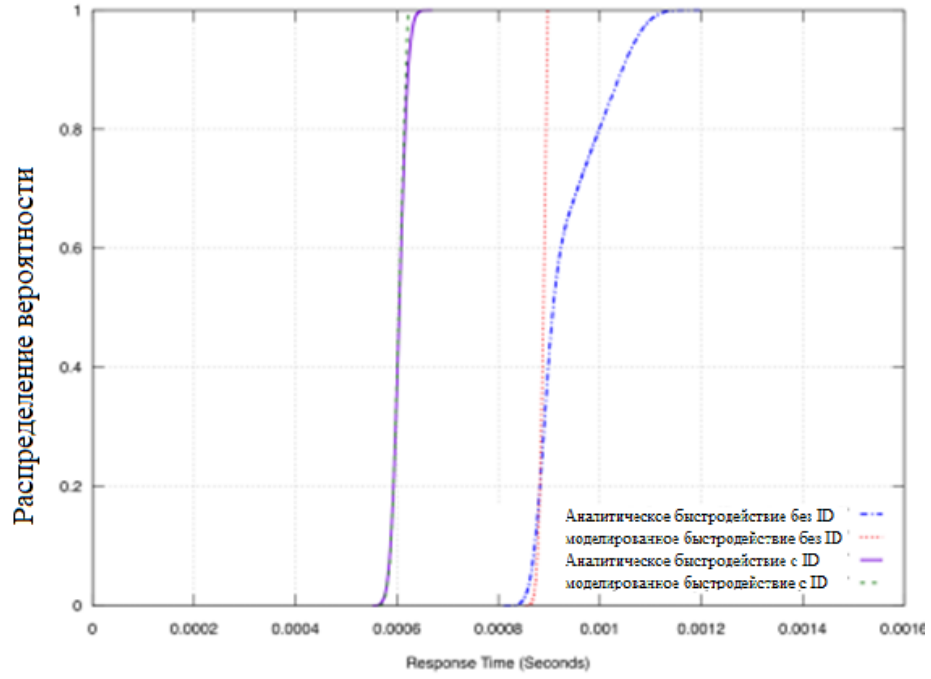


Рисунок 3.10 – Моделирование коэффициента использования MQTT брокера с идентификатором IoT

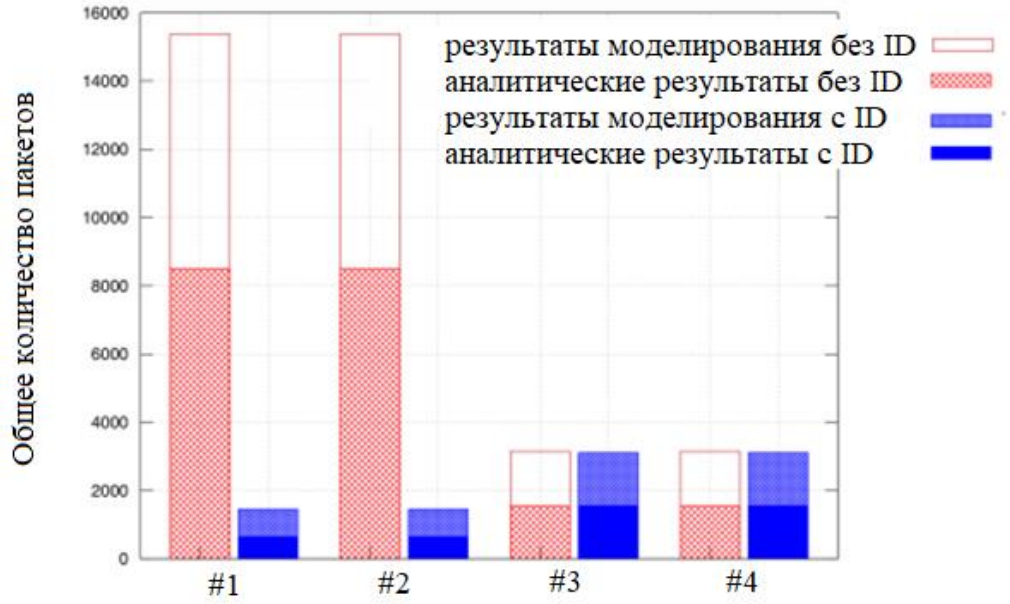


а)

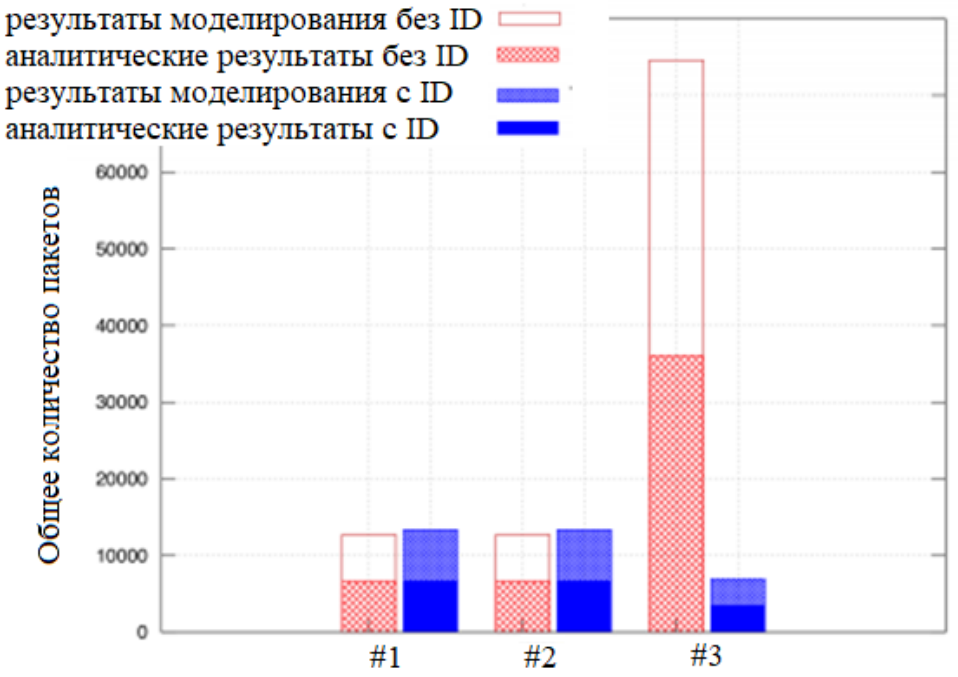


б)

Рисунок 3.11 – Время отклика системы: а)для приложений на основе событий (умная парковка) б)для приложений на основе участия (сигнал погоды)



а)



б)

Рисунок 3.12 – Общее количество пакетов: а)для приложений на основе событий (умная парковка) б)для приложений на основе участия (сигнал погоды)

Загрузка сети просто задерживает или препятствует обработке пакетов данных для законных соединений; такие дополнительные задержки ухудшают QoS трафика текущих соединений. IDIoT должен быть надежным и эффективным для улучшения производительности QoS для трафика, когда он

подвергается такой угрозе. Чтобы проверить это дополнительно изучили правильность аналитических выражений для T (то есть время отклика в одиночных приоритетных очередях M / G / 1). Как показано на рисунке 3.12, предлагаемый метод уменьшил время отклика системы и предотвратил снижение производительности QoS, заблокировав переоцененные узлы. Приложение парковки на рисунке 3.11, имеет среднее время отклика 0,91 миллисекунды при высокой нагрузке на сеть без использования нашей методики и в среднем 0,64 миллисекунды с методом IDIoT. Применение погодного сигнала на рисунке 4b имеет почти одинаковую реакцию в среднем 0,65 миллисекунды и 0,93 миллисекунды с и без IDIoT соответственно. Количество заблокированных пакетов - это еще одна важная мера, и в нужное время следует принять определенное решение, чтобы предотвратить переполнение системы огромным количеством бесполезных пакетов данных. Рассматривая общее количество пакетов N для каждого клиента, очевидно, можем показать преимущество нашего метода. В обычной ситуации на рисунке 3.12 (а) можно заметить, что каждая автостоянка участвует примерно в 1556 пакетах, а когда скорость передачи данных увеличивается, неправильно ведущие автостоянки отправляют около 8513 пакетов. В нашем предлагаемом способе и до того, как загрузка произойдет, первая и вторая автостоянка отправят брокеру только 648 пакетов, затем брокер обнаружил увеличение скорости поступления и запретил им доступ к системе. На рисунке 3.12 (б) показана та же самая ситуация, которая произошла с приложением сигнала погоды. IDIoT предотвращает около 35000 ненужных пакетов из третьего города, которые могут быть ответственны за нарушение общего качества системы.

Интервал выборки играет важную роль для поддержания предопределенных ограничений QoS. Когда объем трафика увеличился, наша система по-прежнему устойчива к экстремальным случаям (новый коэффициент прибытия $\lambda_{new} = 5\lambda$) и точно идентифицирует переоцененные устройства по их идентификатору клиента с некоторыми дополнительными затратами в очереди. Эта задержка в очереди может быть минимизирована путем оптимизации интервала выборки, используемого для расчета текущей частоты поступления, как показано на рисунке 3.13. При интервале выборки в 100 миллисекунд задержка в очереди составляла около 1 миллисекунды, которую можно дополнительно уменьшить до 0,2 миллисекунды, уменьшив Интервал выборки до 20 миллисекунд. Оптимизация интервала выборки должна добавить другое измерение, чтобы существенно снизить накладные расходы производительности. Выьирается оптимизацию интервала выборки как будущую работу. Общее количество издателей IoT должно контролироваться для поддержания стабильности системы и предотвращения загрузки сети IoT на ранних этапах. Любая система может обслуживать указанное количество пользователей. Когда количество устройств IoT увеличится выше адекватного предела, появится ухудшение качества обслуживания. Таким образом, проводится простой эксперимент, чтобы

измерить задержку в очереди, поскольку количество устройств IoT (для обоих приложений) увеличилось в 2 раза, 4 раза, 6 раз, 8 раз, 10 раз и 12 раз. Как показано на рисунке 3.14, задержка в очереди составляла около 0,42, 0,5 и 0,68 миллисекунды для 2x, 4x и 6x соответственно. Задержка продолжает увеличиваться на порядок секунд, пока не достигнет 7 секунд для (12x), что совершенно неприемлемо для большинства приложений. Следовательно, периодический мониторинг системы на границах сети поможет достичь требований QoS сети. Как видно из вышесказанного, результаты нашего моделирования близко соответствуют аналитическим результатам для всех показателей производительности.

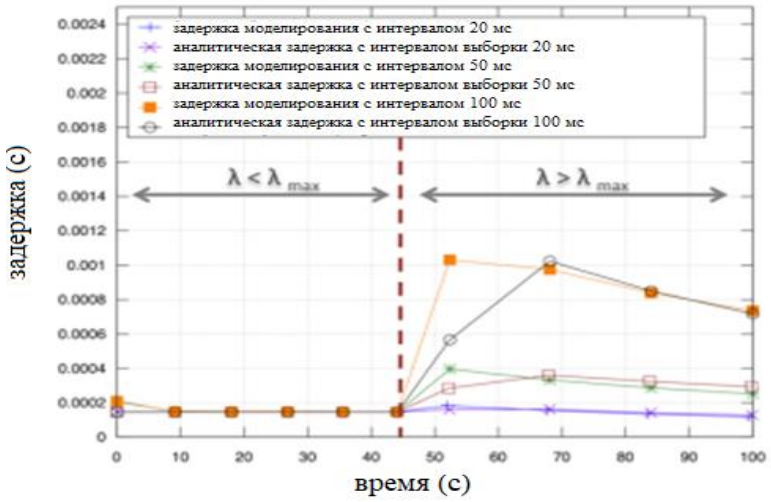


Рисунок 3.13 – Задержка в очереди против интервала выборки

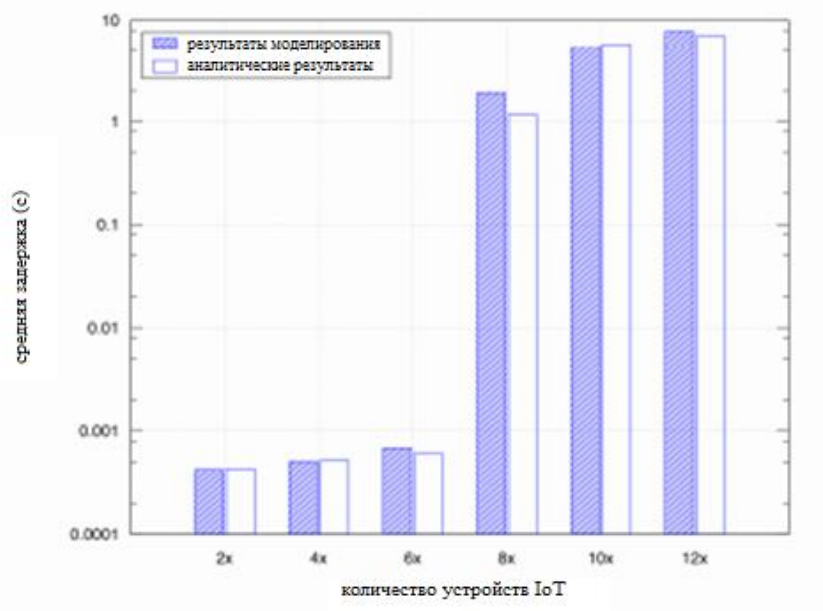


Рисунок 3.14 – Задержка в очереди против количества IoT-издателей

Заключения

В первой главе магистерской диссертации было определено современное состояние таких технологий как IoT/M2M, было исследовано их степени разработанности, обоснована актуальность решения проблемы связанных со стандартизацией межмашинных коммуникаций, показано возможные направления применений технологий M2M. Рассмотрены технологии, которых можно разделить как аппаратная часть и прикладная. Проведен анализ существующих работ по стандартизации IoT. Подробно было описано проблема адресаций в этих сетях. Проведен теоретический анализ трафика сетей IoT.

Во второй главе выполнен анализ развития IoT, и было доказано что направление уже актуально и в будущем нарастает. Было рассмотрено несколько вариантов анализа трафика интернета вещей, и выбор был сделан на модели конечных автоматов. С использованием имитатора дискретных событий он дает возможность сравнивать его с аналитическими результатами, полученными с помощью предложенной модели связи. Результаты показали значительное улучшение в прогнозировании количества пакетов по времени с использованием предложенной модели. Следовательно, результаты моделирования, представленные в этой работе, отражают передачу данных в упрощенных теоретических каналах.

В третьей главе был представлен метод мгновенного обнаружения и предотвращения загрузки сети в сетях IoT, поддерживаемых моделью публикации / подписки (протокол MQTT). Предложенная схема направлена на предотвращение массового трафика, генерируемого устройствами IoT. Модель собирает и анализирует исторические коэффициенты поступления трафика и позволяет центральному брокерскому узлу реагировать в соответствии с собранными коэффициентами поступления и текущим числом узлов публикатора в случае возникновения события высокого спроса. Анализ и моделирование очереди M / G / 1 были использованы для проверки предложенной модели. Сравнивается наш механизм с обычным случаем, чтобы оценить полученные результаты. Результаты моделирования показали, что понимание базовых шаблонов трафика может помочь определить высокую нагрузку на сеть на ранней стадии.

Полученные в работе результаты могут применяться при анализе обслуживания, а также при прогнозировании M2M трафика.

Список литературы

1 Dovgal V.A., Dovgal D.V. Management of resources on the Internet of Things // Distance educational technologies: proceedings of the II Russian scient.-pract. conf., Yalta, 2017. Simferopol: ARIAL, 2017. P. 168–173.

2 K. Ashton, “That ‘internet of things’ thing,” RFiD Journal, vol. 22, no. 7, pp. 97–114, 2009.

3 B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen and M. Sorensen, "Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5. doi: 10.1109/VTCSpring.2017.8108666

4 Lloret, Jaime & Tomás, Jesús & Canovas, Alejandro & Parra, Lorena. (2016). An Integrated IoT Architecture for Smart Metering. IEEE Communications Magazine. 54. 50-57. 10.1109/MCOM.2016.1600647CM.

5 Sureeya, Kritsana & Inthasuth, Tanakorn. (2019). Packet Traffic Measurement of IEEE1888 WRITE Procedure between ZigBee Gateway and Storage for Building Energy Management System. 10.1109/ITC-CSCC.2019.8793437.

6 АНАЛИЗ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ О.Н. Лоднева, Е.П. Ромасевич Modern Information Technologies and IT-Education Vol. 14, no. 1. 2018

7 Aloufi, Khalid. (2019). 6LoWPAN Stack Model Configuration for IoT Streaming Data Transmission over CoAP. International Journal of Communication Networks and Information Security. 11. 304-3012.

8 Leal, Roberto & Santos, Leonel & Vieira, Leandro & Gonçalves, Ramiro & Rabadão, Carlos. (2019). MQTT Flow Signatures for the Internet of Things. 1-5. 10.23919/CISTI.2019.8760849.

9 Kodali, Ravi & Soratkal, Sreeramya. (2016). MQTT based home automation system using ESP8266. 1-5. 10.1109/R10-HTC.2016.7906845.

10 Jeelani, Tabinda & Pathania, Nahita. (2017). Traffic Prioritization in an MQTT Gateway. International Journal of Computer Applications. 164. 32-38. 10.5120/ijca2017913595.

11 https://www.mathworks.com/help/thingspeak/mqtt-basics.html

12 ОСОБЕННОСТИ МУЛЬТИСЕРВИСНОГО ТРАФИКА с учетом сообщений, создаваемых устройствами IoT В.Зайцев, Н.Соколов ПЕРВАЯ МИЛЯ 6/2017

13 Cisco Systems. (2016) Visual networking index (VNI).

14 В.О. Тихвинский, Г.С. Бочечка, Б.И. Нургожин, А.З. Айтмагамбетов Сети IoT/M2M: технологии, приложения и регулирование. Алматы. «Ақ-Шағыл», 2016. 332 стр

15 F. Loi, A. Sivanathan, H. Habibi Gharakheili, A. Radford, and V. Sivaraman, “Systematically Evaluating Security and Privacy for Consumer IoT Devices”, in Proc. IoT S&P Workshop on Internet of Things Security and Privacy, Dallas, Texas, USA, 2017.

16 Tractable Stochastic Geometry Model for IoT Access in LTE Networks Mohammad Gharbieh, Hesham ElSawy, Ahmed Bader, and Mohamed-Slim Alouini URL: https://arxiv.org/abs/1607.03349v1

17 Asensio, Angel & Marco, Álvaro & Blasco, Rubén & Casas, Roberto. (2014). Protocol and Architecture to Bring Things into Internet of Things. International Journal of Distributed Sensor Networks. 2014. 18. 10.1155/2014/158252.

18 Mehmood, Yasir & Pötsch, Thomas & Marwat, Safdar Nawaz Khan & Ahmad, Farhan & Görg, Carmelita & Rashid, Imran. (2015). Impact of Machine-to-Machine Traffic on LTE Data Traffic Performance. 10.1007/978-3-319-23512-7_25.

19 Gharbieh M. et al. Пространственно-временная модель для трафика IoT восходящей линии связи: планирование и парадокс произвольного доступа // IEEE Transactions on Wireless Communications. - 2018. - Т. 17. - №. 12. - С. 8357-8372.

20 C, Dr. Lakshmi Devasena. (2016). IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) - Analyzing its suitability for IoT. 9. 10.17485/ijst/2016/v9i30/98730.

21 A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic Noah Apthorpe Dillon Reisman Nick Feamster arXiv:1705.06805v1 [cs.CR] 18 May 2017

22 Аджемов, А.С. От e-России к u-России: направления развития телекоммуникаций / А.С. Аджемов, А.Е. Кучерявый // Инновационная экономика России. – 2006. – апрель. С. 56 - 59.

23 Кучерявый, А.Е. От e-России к u-России: тенденции развития электросвязи / А.Е. Кучерявый, Е.А.. Кучерявый. – М. : Электросвязь, 2005. - №5. – С. 10-12

24 Кучерявый, А.Е. LTE и беспроводные сенсорные сети / А.Е. Кучерявый, А. Футахи, Е.А. Кучерявый // Мобильные телекоммуникации. – 2012 – ноябрь – С. 38-41.

25 Семенов, Ю.В. Умные всепроникающие сети / Ю.В. Семенов, А.Е. Кучерявый, В.О. Пяттаев // 14 Всероссийский Форум “Развитие телекоммуникаций в России”, Сочи, 26-27 апреля 2011г. : материалы Форума, М. : ЗАО “Экспо – Телеком”, 2011. – С. 44 – 47

26 Gorlatova, M. Energy Harvesting Active Networked Tags (EnHANTs) for Ubiquitous Object Networking / M.Gorlatova at all // IEEE Wireless Communications, Dec. – 2010. - V.17. - №6. – PP. 18 – 25.

27 Kim, B.-T. Broadband convergence Network (BcN) for Ubiquitous Korea Vision / B.-T. Kim // The 7th International Conference on Advanced Communication Technology ICACT’2005. Phoenix Park, Korea, February 21-23, 2005. – PP. 168 – 181.

28 Schneps-Schneppe, M. M2M Applications and Open API: What Could Be Next? / M.Schneps-Schneppe, D.Namiot // The 12th International Conference on

Next Generation Wired/Wireless Networking NEW2AN 2012. - Saint-Petersburg. Springer LNCS 7469. - Aug. 2012. – PP. 429 – 439.

29 M.Schneps-Schneppe, A.Maximenko, D.Namiot. On M2M communications standards for smart metering. Internet of Things and its Enablers / M.Schneps Schneppe, A.Maximenko, D.Namiot // (INTHITEN) Conference, State University of Telecommunication, St. Petersburg, Russia, June 3-4 2013. – PP. 15 – 18.

30 Potsch, T. Influence of Future M2M Communication on the LTE System / T.Potsch, S.N.K.Marwat, Y.Zaki, C.Gorg // Wireless and Mobile Networking Conference. Dubai, United Arab Emirates, 23-25 April 2013. – 4 p

31 Shafig, M.Z. A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization / M.Z. Shafig and all. // 12th ACM Sigmetrics/Performance International Conference. June 11-15, London, England, UK, 2012. – PP. 65 – 76.

32 Drajic, D. Traffic Generation Application for Simulating Online Games and M2M applications via Wireless Networks / D.Drajic and all // 9th Conference on Wireless On-demand Network Systems and Services WONS., Courmayeur, Italy. Jan. 9-11. - 2012. – PP. 167 – 174.

33 Кендалл, М. Многомерный статистический анализ и временные ряды / А. Стьюарт. — М. : Наука, 1976. — 736 с.

34 M. Laner, P. Svoboda, N. Nikaein, and M. Rupp, “Traffic models for machine type communications,” 10th IEEE Int. Symp. Wirel. Commun. Syst. 2013, ISWCS 2013, vol. 9, no. i, pp. 651–655, 2013.

35 M. Johnston and E. Modiano, “A New Look at Wireless Scheduling with Delayed Information,” IEEE Int. Symp. Inf. Theory - Proc., pp. 1407– 1411, 2015.

36 O. Al-Khatib, W. Hardjawana, and B. Vucetic, “Traffic modelling for Machine-to-Machine (M2M) last mile wireless access networks,” 2014 IEEE Glob. Commun. Conf. GLOBECOM 2014, pp. 1199–1204, 2014.

37 S. Floyd and V. Jacobson, “The Synchronization of Periodic Routing Messages,” IEEE/ACM Trans. Netw., vol. 2, no. 2, pp. 122–136, 1994.

38 Cisco Visual Networking Index (VNI) and VNI Service Adoption Global Forecast Update, 2015–2020 Thomas Barnett, Jr. Arielle Sumits June 2016

39 В. О. Тихвинский и С. В. Терентьев, “Использование инфраструктуры сетей LTE при построении сетей M2M”, ISSN 0013-5771. «ЭЛЕКТРОСВЯЗЬ», № 9, 2012

40 N. Nikaein, M. Laner, K. Zhou, P. Svoboda, D. Drajic, M. Popovic, and S. Krco, “Simple traffic modeling framework for machine type communication,” 10th IEEE Int. Symp. Wirel. Commun. Syst. 2013, ISWCS 2013, pp. 783–787, 2013.

44 C. Ide, B. Dusza, M. Putzke, C. Muller, and C. Wietfeld, “Influence of M2M communication on the physical resource utilization of LTE,” in Wireless Telecommunications Symposium, 2012, pp. 1–6.

42 Mathworks, “SimEvents®: User’s Guide,” MATLAB Manual. pp. 1–458, 2020.

43 “MQTT.org.” http://mqtt.org. Accessed: 3-March-2017

44 MQTT Sparkplug / Tahu . www.cirrus-link.com . Проверено ноябрь +5, 2019

45 Фам В.Д., Юлчиева Л.О., Кричек Р.В. Исследование взаимодействия интернета вещей на базе лабораторного стенда// Информационные технологии и телекоммуникаций. 2016. Том 4. №1 .с.55-67

46 Давлетов З.С. Анализ трафика IoT/M2M на основе сетевого протокола MQTT// Журнал «Поиск» - №4 /2019. – Алматы, 263-266 стр.

47 Ивченко Г.И., Каштанов В.А., Коваленко И.Н. Теория массового обслуживания. — Учебное пособие для вузов. — М.: Высшая школа, 1982. — 256 с. — 20 000 экз

48 MatLab, "Discrete Event Simulation Software - SimEvents -Simulink," [Accessed 2019],http://www.mathworks.com/products/simevents/

49 Ng, Chee-Hock and Boon-Hee, Soong, “Queueing Modelling Fundamentals: With Applications in Communication Networks”, 2 ed., England: John Wiley & Sons Ltd Publishing Ltd., 2008

Аббревиатуры

IoT – Internet of Things
ИВ – Интернет вещей
M2M – Machine to machine
WPAN - Wireless personal area network
WLAN - Wireless local area network
RFID - Radio Frequency IDentification
NFC – near field communication
BLE – Bluetooth low energy
Ant - Adaptive Network Topology
6LowPAN - IPv6 over Low power Wireless Personal Area Networks
LPWAN - Low-power Wide-area Network
LoRaWAN – Long rage Wide-area Network
eMTC - enhanced Machine Type Communication
NB-IOT – narrowband IoT
EC-GSM-IoT - Extended coverage GSM IoT
HTTP - HyperText Transfer Protocol
MQTT - message queuing telemetry transport
CoAP - Constrained Application Protocol
QUIC - Quick UDP Internet Connections
UDP - User Datagram Protocol
AMPQ - Advanced Message Queuing Protocol
TLS - transport layer security
LTE-M - Long Term Evolution for Machines
NoT – Network of Things
BPM Everywhere - beats per minute Everywhere
ISO - International Organization for Standardization
IEC - International Electrotechnical Commission
ITU - International Telecommunication Union
IETF - Internet Engineering Task Force
IEEE - Institute of Electrical and Electronics Engineers
ETSI - European Telecommunications Standards Institute
3GPP - 3rd Generation Partnership Project
W3C - World Wide Web Consortium
XMPP - eXtensible Messaging and Presence Protocol
QoS – Quality of Service
MMPP - Markov-Modulated Poisson Processes
CMMPP – Coupled Markov-Modulated Poisson Processes

ПРИЛОЖЕНИЕ А

Анализ существующих технологий IoT

Технология	Диапозон частот	Диапозон	Скорость передачи данных	Жизнь батареи	Топология	Стандартизация	Организация
RFID	варьируется	1 см	1 – 10 кбит/с	3-5 года	Одноранговая сеть	открытый стандарт	ни один орган
NFC	13.56 МГц	0.2 м	424 кбит/с	3-5 года	Одноранговая сеть	открытый стандарт	ISO/IEC
BLE	2.4 ГГц	10 – 100 м	1 Мбит/с	месяц-год		открытый стандарт	Bluetooth SIG
Ant	2.4 ГГц	30 м	1Мбит/с	годы	Одноранговая сеть	патентованный	Garmin
EnOcean	1 ГГц	30 – 300 м	125 кбит/с		Звезда / дерево / меш	патентованный (стандарт на 1-3 слоя)	EnOcean Alliance
Z-Wave	1 ГГц	40 – 200 м	100 кбит/с	месяц-год	Меш	патентованный	Z-Wave Alliance
ZigBee	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	месяц-год	Звезда/ Меш/ дерево	открытый стандарт	ZigBee Alliance
MiWi	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	месяц-год	Звезда/ Меш/ дерево	патентованный	Microchip Technol- ogy
DigiMesh	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	годы	Одноранговая сеть	патентованный	Digi International
WirelessHART	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	годы	Одноранговая сеть	открытый стандарт	HART Communica-tion Foundation

Продолжения приложения А

Технология	Диапозон частот	Диапозон	Скорость передачи данных	Жизнь батареи	Топология	Стандартизация	Организация
Thread	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	месяц-год	Звезда/ Меш/ дерево	открытый стандарт	Thread Group Al-liance
6LowPAN	1 ГГц, 2.4 ГГц	10 – 100 м	250 кбит/с	месяц-год	Звезда/ Меш/ дерево	открытый стандарт	IETF
Wi-Fi	2.4 ГГц , 5 ГГц	100 м; 1км	Мбит/с - Гбит/с	дни-месяцы	Звезда	открытый стандарт	Wi-Fi Allianc e
NB-IoT	450МГц – 3.5 ГГц (2G/3G/4 G спектр)	10 – 15 км	250 кбит/с	10 с лишним лет	Звезда	открытый стандарт	3GPP
eMTC	450 МГц – 3.5 ГГц (такой же как и унаследо ванные LTE)	10 – 15 км	1 Мбит/с	10 с лишним лет	Звезда	открытый стандарт	3GPP
EC-GSM-IoT	850 – 900 МГц, 1800 – 1900 МГц (как GSM)	10 – 15 км	70 кбит/с	10 с лишним лет	Звезда	открытый стандарт	3GPP
LoRa WAN	1 ГГц	10 – 15 км	50 кбит/с	10 с лишним лет	Звезда	открытый стандарт	LoRa Allianc e
SIGF OX	1 ГГц	10 – 50 км	100 бит/с	10 с лишним лет	Звезда	патентова нный	Sigfox
DASH 7	1 ГГц	2 – 5 км	167 кбит/с	10 с лишним лет	Звезда / дерево	открытый стандарт	Dash7 Allianc e