Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий
Направление подготовки 11.03.02

# РЕФЕРАТ

«Zigbee — предназначение, устройство, преимущества и недостатки»

Выполнил:
Швалов Даниил Андреевич
Группа: К34211
Проверил:
Белоцерковец Сергей Александрович

Санкт-Петербург — 2024

**СОДЕРЖАНИЕ**

**ВВЕДЕНИЕ** . . . . . 4

**1 ОСНОВНЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ ZIGBEE** . . . . 5
1.1 Интернет вещей . . . . . 5
1.1.1 Основные понятия . . . . . 5
1.1.2 Устройство интернет вещей . . . . . 5
1.1.3 Сферы применения интернета вещей . . . . . 6
1.2 Роль Zigbee в интернете вещей . . . . . 7
1.2.1 Основные понятия . . . . . 7
1.2.2 Сферы применения Zigbee . . . . . 7

**2 ВНУТРЕННЕЕ УСТРОЙСТВО ZIGBEE** . . . . . 9
2.1 Типы устройств . . . . . 9
2.1.1 Координатор . . . . . 9
2.1.2 Роутер . . . . . 9
2.1.3 Конечное устройство . . . . . 10
2.1.4 Сравнение функциональных возможностей типов устройств . . . . . 11
2.2 Сетевые топологии . . . . . 12
2.2.1 Основные понятия . . . . . 12
2.2.2 Топология точка-точка . . . . . 12
2.2.3 Топология звезда . . . . . 12
2.2.4 Ячеистая топология . . . . . 13
2.3 Структура сети в Zigbee . . . . . 13

**3 СТЕК ПРОТОКОЛОВ ZIGBEE** . . . . . 15
3.1 Общие положения . . . . . 15
3.2 IEEE 802 . . . . . 15
3.2.1 Подуровень управления доступом к среде . . . . . 15
3.2.2 Подуровень управления логической связью . . . . . 16
3.3 IEEE 802.15.4 . . . . . 16
3.3.1 Радиочастотные диапазоны . . . . . 16
3.3.2 Множественный доступ с прослушиванием несущей волны и избеганием коллизий . . . . . 17

3.4 Сетевой уровень Zigbee . . . . . 17
3.4.1 Основные понятия . . . . . 17
3.4.2 Маршрутизация запросов . . . . . 18
3.4.3 Адресация . . . . . 19
3.5 Формирование сети . . . . . 21
3.5.1 MAC ассоциация . . . . . 21
3.5.2 Повторное сетевое присоединение . . . . . 22
3.5.3 Динамика сети . . . . . 22
3.6 Прикладной уровень Zigbee . . . . . 22
3.6.1 Основные понятия . . . . . 22
3.6.2 Ферма приложений . . . . . 23
3.6.3 Объекты приложений . . . . . 23
3.6.4 Объект устройства . . . . . 23
3.6.5 План управления . . . . . 23
3.6.6 Подуровень поддержки приложений . . . . . 24
3.6.7 Поставщик услуг безопасности . . . . . 24
3.7 Безопасность . . . . . 24
3.7.1 Основные понятия . . . . . 24
3.7.2 Центр управления безопасностью . . . . . 25
3.7.3 Режимы безопасности . . . . . 25
3.7.4 Типы ключей . . . . . 26
3.7.5 Архитектура безопасности . . . . . 26

**4 СРАВНЕНИЕ С КОНКУРИРУЮЩИМИ ТЕХНОЛОГИЯМИ** . 28
4.1 Преимущества и недостатки Zigbee . . . . . 28
4.2 Сравнение с другими стандартами связи . . . . . 29
4.2.1 Сравнение с Wi-Fi . . . . . 30
4.2.2 Сравнение с Bluetooth . . . . . 31
4.2.3 Сравнение с Z-Wave . . . . . 31
4.2.4 Сравнение с Thread . . . . . 32
4.2.5 Сравнение с Matter . . . . . 33

**ЗАКЛЮЧЕНИЕ** . . . . . 34

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** . . . . . 35

# ВВЕДЕНИЕ

С каждым годом технологии для работы с интернетом вещей становятся все популярнее и популярнее. Этому способствует тот факт, что интернет вещей помогает упростить и автоматизировать большое количество рутинных процессов из бытовой жизни.

Одной из важнейших технологий в работе интернет вещей является технология передачи данных между устройствами. Zigbee является одним из самых распространенных стандартов передачи данных при использовании интернета вещей. Понимание того, как устроен Zigbee, какие у него есть сильные и слабые стороны, позволяет создавать эффективные, масштабируемые и отказоустойчивые сети для работы интернета вещей.

**Целью** работы является исследование возможности создания масштабируемых и отказоустойчивых сетей для работы интернета вещей на основе Zigbee.

В соответствии с поставленной целью в данной работе решались следующие **задачи**:

1. Определить основные сценарии использования Zigbee.
2. Изучить внутреннее устройство Zigbee.
3. Изучить стек протоколов Zigbee.
4. Выявить преимущества и недостатки Zigbee, провести сравнительный анализ с конкурирующими технологиями.

**Структура работы** строилась в соответствии с поставленными задачами и состоит из введения, четырех основных глав, заключения и списка использованных источников. В первой главе определены основные сценарии и направления, для которых создавался и используется Zigbee. Во второй главе рассматриваются основные концепции, в соответствии с которыми работает Zigbee. В третьей главе рассматривается стек протоколов Zigbee, устройство и предназначение каждого из уровней. В четвертой главе описываются преимущества и недостатки Zigbee, а также Zigbee сравнивается с другими стандартами беспроводной связи.

# 1 ОСНОВНЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ ZIGBEE

## 1.1 Интернет вещей

### 1.1.1 Основные понятия

Интернет вещей (Internet of things, IoT) — объединение разных устройств в общую сеть, в которой они могут собирать информацию, обрабатывать ее и обмениваться данными между собой, с человеком и серверами в дата-центре или облаке.

Классическим примером интернета вещей является умный дом, в котором можно управлять устройствами удаленно, а сами устройства могут взаимодействовать друг с другом. Например, умная колонка по голосовой команде включает свет, датчик передает данные о температуре в систему отопления, розетка отключается, если не был выключен утюг.

При этом интернет вещей не ограничивается бытовой жизнью. Другим примером может служить завод, в котором на каждом станке установлены датчики. Эти датчики следят за состоянием оборудования и подают сигнал, если что-то будет работать не так или сломается. Самими станками при этом тоже можно управлять дистанционно: подавать с пульта команды на остановку или старт работ.

### 1.1.2 Устройство интернет вещей

Система интернета вещей включает в себя датчики и устройства, взаимодействие которых осуществляется через сетевое соединение. Как только данные попадают в сеть, осуществляется их обработка программными средствами и принимается решение о необходимости выполнения определенных действий, например настройки датчиков и устройств без необходимости ввода данных пользователем или отправки уведомлений.

Полная система интернета вещей состоит из четырех отдельных компонентов. Датчики устройств, средства подключения, инструменты обработки данных и пользовательский интерфейс. Рассмотрим каждый из них:

– **Датчики устройств**. Собирают данные в определенной среде. Устройство может иметь несколько датчиков, например, смартфон оснащен GPS, камерой, акселерометром и другими датчиками.

Датчики собирают данные из окружающей среды для решения определенных задач.

– **Средства подключения**. После сбора данных устройство должно отправить их в сеть. Это делается это по-разному: по Wi-Fi, Bluetooth, Zigbee, Ethernet. Вариант подключения зависит от области применения конкретного устройства интернета вещей.
– **Инструменты обработки данных**. Как только данные попадают в сеть, осуществляется их программная обработка с целью последующего решения о выполнении определенных действий. Эти действия могут включать отправку предупреждений или автоматическую настройку датчиков устройства без участия пользователя. Однако иногда требуется ввод данных со стороны пользователя. В этом случае применяется пользовательский интерфейс.
– **Пользовательский интерфейс**. Позволяет осуществить ввод данных со стороны пользователя или выполнить проверку работоспособности системы. Все действия пользователя передаются через систему: от пользовательского интерфейса в сеть, а затем к датчикам устройств для внесения запрошенных изменений.

### 1.1.3 Сферы применения интернета вещей

Существует множество областей применения интернета вещей. Далее перечислены самые популярные:

– **носимые устройства**: фитнес-трекеры, умные часы, умные очки, гарнитуры виртуальной реальности;
– **умные дома**: беспроводные кухонные приборы, интеллектуальные системы освещения, жалюзи с электрическим приводом, автоматические окна и двери, интеллектуальные счетчики коммунальных услуг;
– **умные города**: датчики и счетчики для сбора и анализа данных;
– **медицина**: зонды, кардиостимуляторы, анализаторы химического состава пота, телемедицина;
– **розничная торговля**: автоматизированные кассы, умные полки;
– **транспорт**: телематика и умное управление автопарком.

## 1.2 Роль Zigbee в интернете вещей

### 1.2.1 Основные понятия

Как было описано ранее, одним из важнейших компонентов, без которого невозможно существование интернета вещей, являются средства покдлючения. На данный момент существует обширное множество технологий, позволяющих связать умные устройства. Zigbee является одной из таких технологий.

Zigbee — это стандарт беспроводной связи, предназначенный для систем управления и сбора данных. Основным принципом умной сети Zigbee является малый объем передаваемых данных и низкое энергопотребление. Устройства в сети используют технологию малого радиуса действия, что позволяет им работать с минимальным энергопотреблением и продлить срок службы батареи. Это особенно актуально для беспроводных устройств, которые работают на энергозатратах исключительно батарейного типа.

Одно из важных свойств сетей Zigbee — это возможность организации сложных децентрализованных сетей. В таких сетях каждый узел напрямую связан с несколькими другими узлами. Эти связи могут обновляться и оптимизироваться при отключении устройств от сети или при появлении новых. Динамическая структура сети позволяет быстро устранять аварии, прокладывая новые пути передачи данных в обход сбойного участка.

В добавок ко всему, Zigbee предусматривает криптографическую защиту данных, передаваемых по беспроводным каналам, и гибкую политику безопасности. Это является несомненным преимуществом, поскольку нетрудно представить, к чему может привести несанкционированное вмешательство в работу, например, системы управления тех-процессом или системы охраны.

### 1.2.2 Сферы применения Zigbee

Основными областями, в которых применяется протокол Zigbee, являются практически все то, что относится к интернету вещей. Из них можно выделить наиболее популярные:

– умный дом;
– беспроводные сенсорные сети;

– промышленные системы управления;
– встроенные датчики;
– сбор медицинских данных;
– оповещение о задымлении и вторжении посторонних лиц;
– автоматизация зданий.

При этом стоит учитывать, что Zigbee, в силу своей архитектуры, не подходит для ситуаций, требующих высокой мобильности между узлами.

# 2 ВНУТРЕННЕЕ УСТРОЙСТВО ZIGBEE

## 2.1 Типы устройств

В Zigbee устройства разделяются на три типа: координаторы, роутеры и конечные устройства. Каждый из типов устройств может иметь как инфраструктурные функции, необходимые для передачи сигнала и построения сети, так и функции для выполнения основного предназначения устройства. Рассмотрим их поподробнее.

### 2.1.1 Координатор

Координатор (Zigbee coordinator, ZC) — это устройство, организующее сеть. Он выбирает политику безопасности сети, разрешает или запрещает подключение к сети новых устройств, а также при наличии помех в радиоэфире инициирует процесс перевода всех устройств в сети на другой частотный канал.

В качестве координатора могут выступать USB-стики (рисунок 1а) и беспроводные шлюзы (рисунок 1б).

а) USB-стик б) Беспроводной шлюз

Рисунок 1 — Примеры координаторов

### 2.1.2 Роутер

Роутер (Zigbee router, ZR) — это устройство, которое имеет стационарное питание и может постоянно участвовать в работе сети. Координатор

также является роутером. На узлах этого типа лежит ответственность по маршрутизации сетевого трафика. Роутеры постоянно поддерживают специальные таблицы маршрутизации, которые используются для прокладки оптимального маршрута и поиска нового, если вдруг какое-либо устройство вышло из строя.

В качестве роутеров могут выступать умные розетки (рисунок 2а), блоки управления осветительными приборами (рисунок 2б) или любое другое устройство, которое имеет подключение к сети электропитания.

а) Умная розетка

б) Умный выключатель

Рисунок 2 — Примеры роутеров

### 2.1.3 Конечное устройство

Конечное устройство (Zigbee end device, ZED) — это устройство, которое подключается к сети через родительский узел (роутер или координатора) и не участвует в маршрутизации трафика. Все общение с сетью для них ограничивается передачей пакетов на родительский узел, либо считыванием поступивших данных с него же. Устройства этого типа чаще всего работают от встроенного источника питания.

Конечные устройства большую часть времени находятся в спящем режиме и отправляют управляющие или информационные сообщения только по определенному событию (например, нажатие умной кнопки). Это позволяет им долго сохранять энергию встроенного источника питания.

Примером конечных устройств в сетях Zigbee могут быть датчики движения (рисунок 3а), датчики температуры (рисунок 3б) и тому подобные.


а) Датчик движения б) Датчик-температуры

Рисунок 3 — Примеры конечных устройств

### 2.1.4 Сравнение функциональных возможностей типов устройств

В таблице 1 приведено сравнение функциональных возможностей ранее перечисленных типов устройств. В первом столбце описана функция, которую может выполнять определенный тип устройства. С помощью символа «X» обозначается, обладает ли тип данной возможностью или нет.

Таблица 1 — Функциональные возможности разных типов устройств

| **Функция** | **Координатор** | **Роутер** | **Конечное устройство** |
|---|---|---|---|
| Создание Zigbee сети | X | | |
| Включение и исключение устройств в/из сети | X | X | |
| Присвоение сетевых адресов | X | X | |
| Поиск и хранение оптимальных маршрутов | X | X | |
| Поиск и ведение списка ближайших соседей | X | X | |
| Маршрутизация пакетов | X | X | |
| Отправка и получение пакетов | X | X | X |
| Подключение или отключение от сети | X | X | X |
| Пребывание в режиме сна | | | X |

## 2.2 Сетевые топологии

### 2.2.1 Основные понятия

Существует множество способов реализации беспроводных сетей, удовлетворяющих тем или иным требованиям приложения. Беспроводной узел в сети может быть передатчиком, приемником или приемопередатчиком. Некоторые узлы являются только ведомыми, они только управляются или контролируются. Другие становятся ведущими или агрегаторами данных, и используются для подключения к внешним коммуникациям. Некоторые узлы могут использоваться в качестве повторителей при передаче данных от одного узла к другому.

В зависимости от требований к сети, используются различные топологии. Их делят на такие топологии, как точка-точка, звезда и ячеистую топологию. Рассмотрим каждую из них.

### 2.2.2 Топология точка-точка

Точка-точка — это простейший вид соединения, при котором два узла соединяются между собой напрямую (рисунок 4). В качестве примера сетевой топологии вида точка-точка может быть соединение передатчика и приемника или двух приемопередатчиков.

Рисунок 4 — Соединения в топологии точка-точка

### 2.2.3 Топология звезда

Звезда — это соединение, при котором конечные узлы подключаются к центральному контроллеру (рисунок 5). В таком соединении узлы не взаимодействуют непосредственно друг с другом, обмен данными идет только с центральным контроллером.

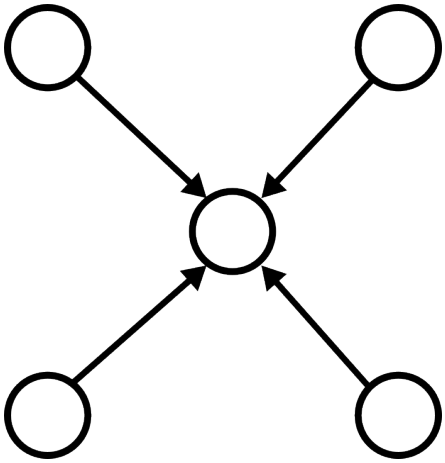

Рисунок 5 — Соединение в топологии «звезда»

### 2.2.4 Ячеистая топология

Ячеистая топология — это соединение, при котором большинство узлов или каждый узел могут быть ретрансляторами, что позволяет передавать данные от одного узла к другому, даже если они не имеют непосредственного соединения (рисунок 6).

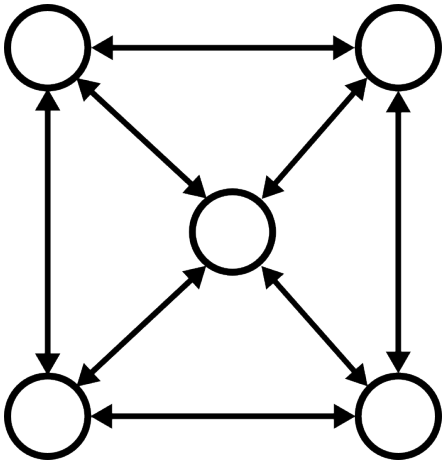

Рисунок 6 — Соединение в ячеистой топологии

## 2.3 Структура сети в Zigbee

На рисунке 7 представлена схема структуры сети в Zigbee. На ней обозначены ранее описанные типы устройств: координатор, роутеры и конечные устройства. Координатор обозначен черным кругом, роутеры — окружностями со сплошной линией, конечные устройства — окружностями с прерывистой линией.

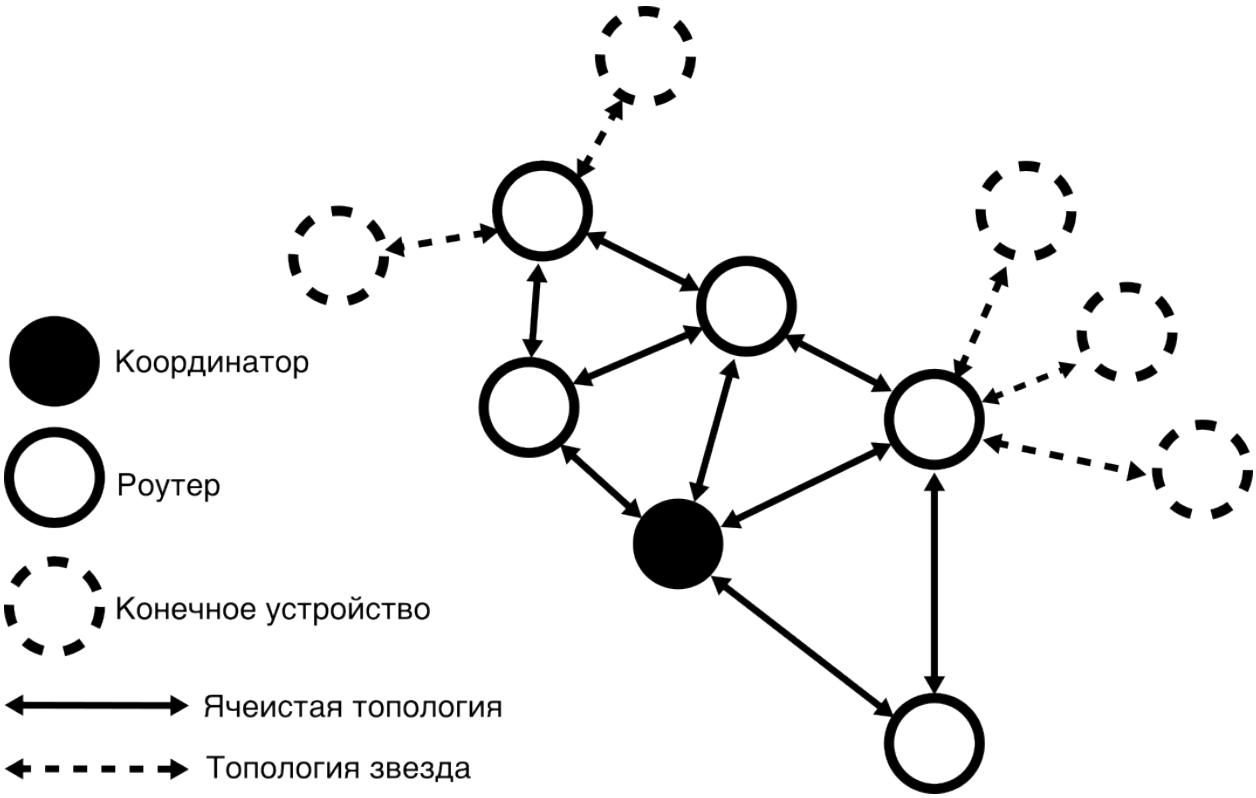


Рисунок 7 — Структура сети Zigbee

Как видно из схемы, устройства в Zigbee могут объединяться в различные топологии: сплошными линиями соединены устройства, относящиеся к ячеистой топологии, прерывистыми линиями — устройства, относящиеся к топологии звезда. При этом в ячеистую топологию входят только координатор и роутеры, объединенные между собой, а к топологии звезда относятся только конечные устройства, подключенные к роутерам или координатору.

Другими словами, все устройства, которые не имеют потребности в экономии энергии (т. е. они подключены в сеть и не имеют аккумулятора), такие как роутеры, устанавливают не только соединение с координатором, но и с другими роутерами.

Благодаря наличию избыточных связей между устройствами повышается надежность всей системы связи в Zigbee. Даже если из строя выйдет устройство, которое выступало в качестве координатора сети, сеть сможет продолжить функционировать дальше.

# 3 СТЕК ПРОТОКОЛОВ ZIGBEE

## 3.1 Общие положения

Спецификация Zigbee охватывает только два уровня стека по модели OSI/ISO: сетевой уровень и частично прикладной уровень. Нижние уровни стека описываются стандартом IEEE 802.15.4 (рисунок 8).

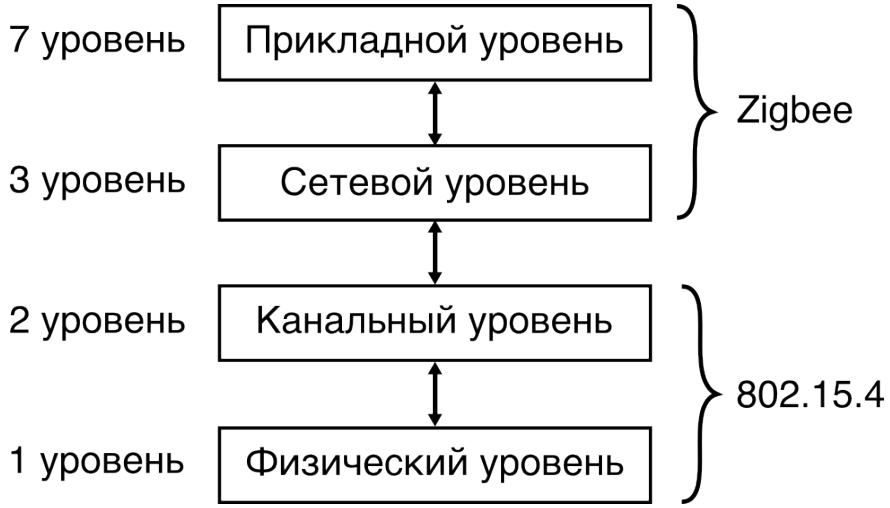


Рисунок 8 — Соответствие уровней модели OSI/ISO и протоколов Zigbee, IEEE 802.15.4

Для начала рассмотрим устройство стандарта IEEE 802.15.4, а затем перейдем к рассмотрению протоколов Zigbee.

## 3.2 IEEE 802

В модели OSI/ISO второй уровень соответствует канальному уровню. Стандарт IEEE 802 разделяет этот уровень на два подуровня: подуровень управления доступом к среде (MAC) и подуровень управления логической связью (LLC). Рассмотрим каждый из них.

### 3.2.1 Подуровень управления доступом к среде

Подуровень управления доступом к среде (media access control, MAC) обеспечивает адресацию, корректное совместное использования общей среды передачи данных, а также задает механизмы управления доступом к среде, что позволяет нескольким точкам доступа общаться между собой в многоточечной сети.

### 3.2.2 Подуровень управления логической связью

Подуровень управления логической связью (logical link control, LLC) управляет передачей данных посредством кадров и обеспечивает проверку правильности передачи информации.

## 3.3 IEEE 802.15.4

IEEE 802.15.4 — это стандарт, который определяет физический уровень (physical, PHY) и подуровень управления доступом к среде (media access control, MAC), рассмотренный ранее. IEEE 802.15.4 создан для беспроводного соединения с низкой скоростью передачи данных к стационарным, портативным и передвижным устройствам без батареи или с очень ограниченными требованиями к потреблению батареи.

### 3.3.1 Радиочастотные диапазоны

IEEE 802.15.4 определяет радиочастотные диапазоны, разделенные на каналы, для передачи информации. К ним относятся следующие:

– 1 канал в диапазоне 868 МГц, до 20, 100 или 250 Кбит/с;
– 10 каналов в диапазоне 915 МГц, до 40 или 250 Кбит/с;
– 16 каналов в диапазоне 2.4 ГГц, до 250 Кбит/с или до 1 Мбит/с.

Наличие нескольких частотных диапазонов позволяет обеспечить оптимальную передачу сигнала в различных условиях. Сигналы стандарта IEEE 802.15.4 могут успешно сосуществовать с другими источниками излучения на той же частоте, к примеру, устройствами, соединенными посредством Wi-Fi. В стандарте также предусмотрены каналы, не пересекающиеся с WiFi, что позволяет реализовать сеть даже в непосредственной близости с очень мощными источниками излучения.

Наличие нескольких частотных диапазонов также обосновывается существованием различных региональных ограничений. Так, например, частота 868 МГц используется в Европе, 915 МГц — в США и Австралии, а 2.4 ГГц — в России и в большинстве стран мира.

### 3.3.2 Множественный доступ с прослушиванием несущей волны и избеганием коллизий

Доступ к каналу IEEE 802.15.4 основан на принципе множественного доступа с прослушиванием несущей волны и избеганием коллизий. Поддерживаются как сети без маячков, так и с маячками. Рассмотрим каждый из этих случаев.

- **Сети без маячков**. Когда устройство планирует начать передачу, оно посылает в сеть специальный jam-сигнал и некоторое время ожидает аналогичных сигналов от других источников излучения. Если jam-сигналов от других передающих устройств не поступает, устройство начинает передачу. Если же обнаруживается «чужой» сигнал, то передатчик «засыпает» на случайный промежуток времени, а затем снова пробует начать передачу. В таком случае одновременно передача может исходить только от одного устройства.
- **Сети с маячками**. В сети используется координатор, который рассылает маячки. Пока устройство не примет такой маячок, оно не сможет начать передачу сигнала. Благодаря такой синхронизации можно уменьшить вероятность одновременной передачи сообщений несколькими узлами сети и увеличить ее общую пропускную способность.

Таким образом, механизмы множественного доступа и маячковой синхронизации подразумевают отключение приемо-передающих устройств при отсутствии данных для пересылки, обеспечивая низкое энергопотребление устройств. В результате время автономной работы оконечных устройств может измеряться годами.

## 3.4 Сетевой уровень Zigbee

### 3.4.1 Основные понятия

Сетевой уровень (Network layer, NWK) в Zigbee использует функции подуровня управления доступом к среде (MAC) и обеспечивает интерфейс для вышестоящего прикладного уровня. На этом уровне реализована поддержка разных сетевых топологий: звездная топология и ячеистая топология.

Именно на этом уровне происходит первоначальное создание сети, включение в нее новых устройств, их исключение и сетевой поиск.

Взаимодействие с уровнем приложения осуществляется посредством *сервиса передачи данных* (NWK Layer Data Entity, NLDE) и *сервиса управления* (NWK Layer Management Entity, NLME). Доступ к этим сервисам с уровня приложения идет через соответствующие программные интерфейсы, называемые точками доступа. Посредством сервиса передачи данных и сервиса управления обеспечивается передача команд и данных приложений к подуровню управления доступом к среде, который для этого предоставляет собственные интерфейсы.

### 3.4.2 Маршрутизация запросов

Одна из важнейших функций, которая выполняется на сетевом уровне протокола Zigbee, — это функция управления маршрутизацией. Именно здесь реализуется алгоритм, который определяет путь следования пакетов данных от отправителя к получателю через цепочку связанных узлов. Этот алгоритм опирается на специальные метрики, отражающие сложность различных путей пересылки данных. Сами метрики вычисляются и обновляются в процедурах поиска и оценки доступных маршрутов. Любой координатор или роутер в сети Zigbee может поддерживать собственную таблицу маршрутов, которая строится с учетом описанных метрик.

Чтобы осуществлять поиск маршрутов и их оценку в сетях Zigbee используется несколько модифицированный алгоритм Ad hoc On Demand Distance Vector (AODV). Протокол подразумевает реактивную реакцию на поступающие запросы, т. е. сеть остается «спящей» до момента поступления конкретного запроса на передачу данных. Когда одному из узлов требуется установить связь с другим удаленным узлом в неизвестном местоположении, он генерирует специальный широковещательный запрос Route Request (RREQ), который получают все узлы, находящиеся с отправителем в непосредственной взаимосвязи (как это установлено топологией сети при ее создании). Они ретранслируют данный запрос далее всем своим соседям и дополняют свои таблицы маршрутизации обратным маршрутом к узлу-отправителю. Когда запрос RREQ доходит до получателя, он отправляет ответный пакет данных Route Reply (RREP), который следует назад единственным оптимальным маршрутом с учетом того, что все узлы на пути

следования уже внесли его в свои таблицы маршрутизации. После получения ответного пакета узел-отправитель тоже вносит соответствующую запись в свою таблицу маршрутизации и начинает передачу данных по установленному маршруту. Если какой-то узел в цепочке передачи данных «выпадает» из сети, то соответствующие ему записи удаляются из таблиц маршрутизации, и процедура рассылки широковещательных запросов повторяется заново.

Так как координатор выступает инициатором создания сети и управляет процессом включения в нее новых устройств, то он является и главным держателем таблицы маршрутизации, то есть знает оптимальный маршрут к любому из устройств в сети. Координатору всегда присваивается нулевой адрес в адресном пространстве сети. Роутеры выполняют ретрансляцию пакетов с данными по оптимальному маршруту. Важнейшее следствие из этого — ни координатор, ни маршрутизаторы не могут выключаться для экономии энергии, т. е. должны работать непрерывно, чтобы устройства, инициирующие передачу данных, могли в любой момент воспользоваться действующим маршрутом.

Алгоритм AODV, используемый в сетях Zigbee для поиска маршрутов, не лишен недостатков. В частности, в сетях с большим количеством конечных устройств, которые обслуживаются единственным роутером по схеме «звезда», аккумулирующим всю информацию с этих устройств, классические широковещательные запросы могут порождать большой ответный трафик — ведь все устройства в сети будут одновременно пытаться выстроить маршрут и посылать собственные широковещательные запросы и ответы на них. Такие запросы, поступающие в большом количестве, снижают пропускную способность сети и отнимают ресурсы на их обработку.

Чтобы решить проблему, описанную выше, в спецификации Zigbee существует специальный механизм маршрутизации «многие-к-одному» (many-to-one routing). Это альтернативная схема поиска маршрутов, которая работает в дополнение к схеме AODV. В ней не требуется генерировать множество широковещательных запросов к каждому узлу — достаточно одной посылки, по которой сразу же и строятся маршруты ко всем узлам сети.

### 3.4.3 Адресация

В сетях Zigbee существует такое понятие как Personal Area Network ID (PAN ID) — это глобальных 16-бит идентификатор сети. PAN ID использу-

ется для логического отделения узлов одной сети Zigbee от узлов другой, если сети расположены на одной и той же территории либо работают на одном и том же канале. Также существует Extended PAN ID — 64-битный уникальный идентификатор. Он может использоваться для избегания конфликтов PAN ID.

Каждому узлу в сети соответствует свой адрес (NwkAddr), который характеризует расположение в сети. Координатор всегда имеет адрес 0x0000. Адрес может быть как коротким (16-битным), так и длинным (64-битным). Короткие адреса присваиваются при присоединении к сети, а длинные адреса являются глобально уникальными и присваиваются устройству на производстве.

Кроме адресов, которые необходимы для определения узла в сети, Zigbee также обеспечивает совместимость на уровне приложения за счет использования кластеров, конечных точек, команд, атрибутов и профилей. Каждый запрос должен содержать PAN ID (поле MAC), NwkAddr (поле NWK), адрес конечной точки приемника и передатчика, ID профиля и кластера. Рассмотрим остальные определения.

Конечные точки позволяют относить один узел к различным профилям или объединять несколько Zigbee-устройств в узел. Каждый узел сети может содержать 1-240 конечных точек в соответствии с количеством выполняемых приложений. Например, выключатель может быть предназначен как для внутреннего, так и для внешнего освещения. Соответственно, он представляет собой две конечные точки.

Кластеры определяются 16-битным идентификатором и являются объектами приложения. В то время как адрес сети и конечные точки относятся к адресации, кластер определяет назначение приложения. Например, кластер включения и выключения On/Off выполняет действие перевода устройства из одного состояния в другое. При этом тип исполнительного устройства неважен.

Профиль приложения — это совокупность настроек узлов сети, обеспечивающая их совместную работу. Спецификация профиля определяет способы задания идентификационных параметров, режимы формирования сети, методы защиты данных, список используемых кластеров, конечные точки и т.д. Для уникальной идентификации приложений каждому приложению выделяется 16-битный идентификатор профиля.

### 3.5 Формирование сети

Сеть Zigbee — самоорганизующаяся, и ее работа начинается с формирования. Устройство, назначенное при проектировании координатором сети, определяет канал, свободный от помех, и ожидает запросов на подключение. Устройства, пытающиеся присоединиться к сети, рассылают широковещательный запрос. Пока координатор является единственным участником сети, то только он отвечает на запрос и предоставляет присоединение к сети. В дальнейшем присоединение к сети могут предоставлять также присоединившиеся к сети роутеры. Устройство, получившее ответ на широковещательный запрос, обменивается с присоединяющим устройством сообщениями, чтобы определить возможность присоединения. Возможность определяется способностью присоединяющего роутера обслужить новые устройства в дополнение к ранее подключенным.

Существует два способа присоединения: MAC ассоциация и повторное сетевое присоединение. Рассмотрим каждый из них.

#### 3.5.1 MAC ассоциация

MAC ассоциация доступна любому устройству Zigbee и осуществляется на MAC уровне. Механизм MAC ассоциации следующий:

1. Устройство, позволяющее присоединиться к нему, выставляет на MAC уровне разрешение на присоединение.
2. Устройство, вступающее в сеть, выставляет на MAC уровне запрос на присоединение и передает широковещательный запрос маячка.
3. Получив маячок от устройств, готовых подключить присоединяемое устройство, последнее определяет, в какую сеть и к какому устройству оно желает присоединиться, и выставляет на MAC уровне требование о вступлении с флажком «повторное присоединение» в значении FALSE.
4. Затем вступающее устройство направляет на выбранное для присоединения устройство запрос присоединения и получает ответ с присвоенным ему сетевым адресом.

При MAC ассоциации данные передаются не зашифрованными, поэтому MAC ассоциация не является безопасной.

### 3.5.2 Повторное сетевое присоединение

Повторное сетевое присоединение вопреки названию может применяться и при первичном присоединении. Оно выполняется на сетевом уровне. При этом, если вступающее устройство знает текущий сетевой ключ, обмен пакетами может быть безопасным. Ключ может быть получен, например, при настройке.

При повторном подключении присоединяющееся устройство выставляет на сетевом уровне запрос присоединения и обменивается с подключающим устройством пакетами «запрос присоединения» — «ответ на запрос присоединения».

### 3.5.3 Динамика сети

Кроме случаев присоединения новых устройств структура сети меняется и в случаях, когда устройства покидают сеть и повторно присоединяться в других местах. Это может происходить , например, в случае перезагрузки устройства.

## 3.6 Прикладной уровень Zigbee

### 3.6.1 Основные понятия

Прикладной уровень (Application Layer, APL) в Zigbee содержит несколько подуровней. Так же, как и на сетевом уровне, взаимодействие между различными подуровнями осуществляется через специализированные программные интерфейсы — точки доступа.

Прикладной уровень включает в себя:

– ферму приложений;
– объекты приложений;
– объект устройства;
– план управления;
– подуровень поддержки приложений;
– поставщик услуг безопасности.

Рассмотрим каждый из них.

### 3.6.2 Ферма приложений

Ферма приложений (Application Framework) — это среда исполнения для объектов приложений (их в устройстве может быть до 240), которая позволяет им принимать и отправлять данные. Ферма приложений задает порядок создания профилей и определяет стандартные типы данных, дескрипторы, форматы кадров и значения пар ключей.

### 3.6.3 Объекты приложений

Объекты приложений (Application Objects) — это программные модули, которые функционируют внутри фермы приложений и управляют устройствами Zigbee. Объекты приложений являются верхним компонентом всего уровня приложения, а их состав и структура определяются производителем устройства Zigbee. Именно объекты приложения, по сути, задают логику работы реализуемого устройства. Это может быть лампа, выключатель света и т.п.

Каждый объект приложения адресуется через свою конечную точку с определенным адресом от 1 до 240. Адрес 0 соответствует объекту устройства Zigbee. Адрес 255 используется для широковещательной передачи сразу во все конечные точки выбранного узла. Адреса от 241 до 254 являются зарезервированными и могут использоваться только по согласованию с разработчиками спецификации Zigbee.

### 3.6.4 Объект устройства

Объект устройства (Zigbee Device Object, ZDO) — это специальный объект, отвечающий за общее управление устройством. В частности, он обеспечивает: первичную инициализацию сервисов подуровня прикладного и сетевого уровней, задание роли устройства в сети (координатор, роутер или конечное устройство), инициацию запросов присоединения и ответов на них, а также управление безопасностью коммуникаций.

### 3.6.5 План управления

План управления (ZDO Management Plane) — это подуровень, поддерживающий связь объекта устройства с подуровнями прикладного и сетевого

уровней. Позволяет объекту устройства обрабатывать запросы приложений на доступ к сети и обеспечивает безопасность.

### 3.6.6 Подуровень поддержки приложений

Подуровень поддержки приложений (Application Support Sublayer, APS) — это подуровень, отвечающий за предоставление данных приложениям через точки доступа, управляет сетевыми присоединениями, хранит данные о присоединениях в таблице, обеспечивает трансляцию 64-битных расширенных адресов в 16-битные сетевые адреса, разбиение на пакеты и их обратную сборку при передаче больших объемов данных.

### 3.6.7 Поставщик услуг безопасности

Поставщик услуг безопасности (Security Service Provider, SSP) — это программный сервис, обеспечивающий механизмы безопасности для использующих шифрование уровней (т. е. сетевой и прикладной уровни). Конфигурируется объектом устройства.

## 3.7 Безопасность

### 3.7.1 Основные понятия

Система безопасности в соответствии со спецификацией Zigbee основана на 128-битном AES алгоритме. Предусмотренные спецификацией Zigbee службы безопасности определяют создание ключей, управление устройствами и защиту данных.

Ключ может быть ассоциирован либо с сетью, либо с каналом связи. Ключ может быть получен путем предварительной установки, соглашения или передачи. Создание ключей канала связи основано на использовании главного ключа, который контролирует соответствие ключей канала связи. Первоначальный главный ключ должен быть получен через безопасную среду (передачей или предварительной установкой), так как безопасность всей сети зависит от него.

### 3.7.2 Центр управления безопасностью

Ключевым элементом концепции безопасности Zigbee является центр управления безопасностью. На этапе формирования или реконфигурации сети центр управления безопасностью разрешает или запрещает присоединение к сети новых устройств. Обычно центром управления безопасностью по совместительству является координатор сети, но это может быть и выделенное устройство.

Центр управления безопасностью может периодически обновлять ключ сети и переходить на новый ключ. Сначала он транслирует новый ключ, зашифрованный с помощью старого ключа сети. Затем сообщает всем устройствам о переходе на новый ключ.

Центр управления играет следующие роли в обеспечении безопасности сети:

1. проверяет подлинность устройств, которые хотят присоединиться к сети;
2. поддерживает и распространяет сетевые ключи;
3. обеспечивает безопасность взаимодействия устройств.

### 3.7.3 Режимы безопасности

**Режим стандартной безопасности**

В режиме стандартной безопасности перечень устройств, главные ключи, ключи каналов связи и сетевые ключи можно хранить как в центре управления безопасностью, так и в самих устройствах. Центр управления безопасностью, тем не менее, отвечает за поддержание стандартного сетевого ключа и контролирует политику приема в сеть. В этом режиме требования к ресурсам памяти центра управления безопасностью гораздо ниже, чем для режима повышенной безопасности.

**Режим повышенной безопасности**

В режиме повышенной безопасности центр управления безопасностью хранит перечень устройств, главные ключи, ключи каналов связи и сетевые ключи, необходимые для контроля и применения политики обновления сетевых ключей и доступа в сеть. В этом режиме по мере роста количества

устройств в сети быстро возрастает необходимый центру управления безопасностью объем памяти.

### 3.7.4 Типы ключей

Zigbee использует три типа ключей для управления безопасностью: главный ключ, сетевой ключ и ключ канала связи. Рассмотрим каждый из них.

**Главный ключ**

Главный ключ не используется для шифрования. Он используется как разделяемый двумя устройствами секретный код при выполнении устройствами процедуры генерации ключа канала связи.

Главные ключи, создаваемые центром управления безопасностью, называются главными ключами центра безопасности, все другие ключи называются основными ключами уровня приложений.

**Сетевой ключ**

Сетевой ключ обеспечивает безопасность сетевого уровня. Сетевой ключ имеет каждое устройство в сети Zigbee.

По беспроводным каналам сетевые ключи высокой безопасности должны пересылаться только в зашифрованном виде. Стандартные сетевые ключи могут пересылаться как в зашифрованном, так и в не зашифрованном виде.

**Ключ канала связи**

Ключ канала связи обеспечивает безопасную одноадресную передачу сообщений между двумя устройствами на уровне приложений.

### 3.7.5 Архитектура безопасности

Архитектура безопасности распределяется между сетевыми уровнями:

– **Подуровень MAC**. Способен устанавливать надежную связь с соседним устройством. Как правило, он использует уровень безопасности, определяемый верхними уровнями.
– **Сетевой уровень**. Управляет маршрутизацией, обрабатывает полученные сообщения и может направлять запросы. Исходящие запросы

будут использовать ключ соответствующего канала связи согласно маршрутизации, если он доступен. В противном случае для защиты полезной нагрузки от внешних устройств будет использоваться сетевой ключ.

– **Прикладной уровень**. Устанавливает ключи и оказывает транспортные услуги как объекту устройства, так и приложениям. Он отвечает также за распространение сообщений об изменениях в устройствах внутри сети, которые могут исходить как от самих устройств, так и от центра управления безопасностью. Уровень также маршрутизирует запросы устройств центра управления безопасностью и обновления сетевого ключа от центра управления безопасностью всем устройствам.

# 4 СРАВНЕНИЕ С КОНКУРИРУЮЩИМИ ТЕХНОЛОГИЯМИ

## 4.1 Преимущества и недостатки Zigbee

Изучив устройство Zigbee, необходимо также рассмотреть его преимущества и недостатки. Понимание преимуществ и недостатков позволяет использовать стандарт связи более правильно и эффективно.

В качестве преимуществ Zigbee выделяют:

– **Низкое энергопотребление**. Zigbee был специально разработан для устройств с батарейным питанием, что позволяет им работать в течение длительного времени без частых замены батарей. Такая эффективность имеет решающее значение для сокращения усилий и затрат на техническое обслуживание домовладельцев.

– **Надёжная сеть**. Ячеистая сетевая архитектура Zigbee обеспечивает надёжную сеть связи в умном доме. Если устройство, напрямую взаимодействующее с центральным сервером, выходит из строя, другие устройства Zigbee могут ретранслировать сообщения, обеспечивая бесперебойное соединение. Эта самовосстанавливающаяся сеть устраняет отдельные точки отказа, повышая общую надежность системы.

– **Расширенный диапазон частот**. Zigbee поддерживает больший диапазон частот по сравнению с другими беспроводными протоколами, что позволяет устройствам обмениваться данными на больших расстояниях. Это преимущество особенно полезно в больших домах или зданиях, где сигналы должны распространяться через стены и другие препятствия. С помощью Zigbee домовладельцы могут беспрепятственно контролировать устройства по всему жилому пространству.

– **Функциональная совместимость**. Zigbee обладает высокой функциональной совместимостью, что позволяет устройствам разных производителей беспрепятственно работать вместе. Эта совместимость позволяет выбирать и комбинировать устройства различных марок, создавая индивидуальную систему умного дома, отвечающую их конкретным потребностям и предпочтениям. Независимо от бренда, устройства, сертифицированные Zigbee, могут легко взаимодействовать друг с другом.

– **Повышенная безопасность**. Безопасность является серьёзной проблемой для любой системы умного дома, и Zigbee предлагает надёжные меры для решения этих проблем. В протоколе используются передовые методы шифрования, обеспечивающие безопасную связь между устройствами. Кроме того, топология ячеистой сети Zigbee затрудняет проникновение в сеть неавторизованных устройств, обеспечивая дополнительный уровень безопасности.
– **Масштабируемость**. Сети Zigbee обладают высокой масштабируемостью и поддерживают большое количество устройств (до 65 000 узлов). По мере расширения и развития умных домов их хозяева могут легко добавлять новые устройства в существующую сеть, не нарушая работу всей системы. Такая масштабируемость обеспечивает готовность к будущему, гарантируя, что умный дом сможет адаптироваться к меняющимся потребностям и технологическим достижениям.

В качестве недостатков Zigbee выделяют:

– **Слабая помехоустойчивость**. Zigbee плохо справляется с ситуациями, когда в зоне действия сети существуют сильные помехи, создаваемые другими устройствами. Будучи одноканальным решением, Zigbee далеко не всегда может эффективно бороться с помехами, которые часто встречаются в перегруженной полосе 2,4 ГГц, совместно используемой протоколом с такими вездесущими технологиями, как Wi-Fi или Bluetooth.
– **Низкая скорость передачи данных**. Zigbee не подходит для ситуаций, когда требуется высокая скорость передачи данных (например, потоковая передача видео с камеры видеонаблюдения).

### 4.2 Сравнение с другими стандартами связи

Как известно, стандарт связи не существует в вакууме, и чаще всего одну и ту же задачу могут решать сразу несколько стандартов. Далее будет рассмотрено сравнение Zigbee с другими стандартами связи, такими как Wi-Fi, Bluetooth, Z-Wave, Thread и Matter.

### 4.2.1 Сравнение с Wi-Fi

Wi-Fi — это технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11. Является самым простым способ связать между собой устройства умного дома. Они подключаются напрямую к существующей сети без необходимости создания сложных конфигураций. Универсальность протокола Wi-Fi позволяет подключать по нему лампочки, розетки, светодиодные ленты и многое другое.

В качестве преимуществ Wi-Fi выделяют:

- **Высокая скорость передачи данных**. Wi-Fi позволяет передавать большие объемы данных, что может быть необходимо для некоторых видов устройств (например, для камер видеонаблюдения).
- **Простота**. Умные устройства с поддержкой Wi-Fi обычно требуют минимальной настройки.
- **Доступность**. Благодаря Wi-Fi можно удаленно управлять своими устройствами из любого места, где есть подключение к интернету.
- **Универсальность**. Устройства с поддержкой Wi-Fi совместимы с любым маршрутизатором, который поддерживает беспроводные сети.
- **Масштабируемость**. К сети Wi-Fi можно добавить большое количество дополнительных устройств.

В качестве недостатков Wi-Fi выделяют:

- **Высокое энергопотребление**. Умные устройства, работающие через Wi-Fi, имеют высокое энергопотребление, из-за чего продолжительность работы батарей в таких устройствах сильно ограничена.
- **Низкая отказоустойчивость**. Если маршрутизатор Wi-Fi перестанет работать, то перестанут работать и сами устройства.
- **Безопасность**. Wi-Fi сети могут быть уязвимы к атакам хакеров, если не защищены надлежащим образом. Низкий уровень безопасности может представлять риск для конфиденциальности и безопасности данных.
- **Дальность передачи**. Дальность передачи ограничивается возможностями маршрутизатора, из-за чего для расширения сети могут потребоваться повторители и другие вспомогательные устройства.

**Вывод**. Из-за высокого энергопотребления Wi-Fi не подходит для устройств с встроенным источником питания. Поэтому, если в сети преобладают автономные устройства, Zigbee будет более хорошим выбором. Однако Wi-Fi хорошо работает с устройствами со стационарным питанием, требующих высокую скорость передачи данных. В случае, если сеть состоит из таких устройств, то Wi-Fi будет более хорошим решением.

### 4.2.2 Сравнение с Bluetooth

Bluetooth — это технология беспроводной связи, которая позволяет устройствам обмениваться данными на коротких расстояниях.

В качестве преимуществ Bluetooth выделяют:

– **Энергоэффективность**. Bluetooth потребляет малое количество энергии, что позволяет автономным устройствам долгое время работать от аккумулятора.
– **Простота настройки**. Процесс парного соединения устройств по технологии Bluetooth обычно прост и понятен даже неопытным пользователям.
– **Распространенность**. Bluetooth поддерживается множеством устройств, включая смартфоны, планшеты, наушники и другие умные устройства.

В качестве недостатков Bluetooth выделяют:

– **Ограниченное расстояние**. Радиус действия Bluetooth ограничен 10 метрами, чего может быть недостаточно для больших помещений.
– **Ограниченное количество подключений**. Каждое устройство Bluetooth может подключаться только к ограниченному количеству устройств одновременно.

**Вывод**. Несмотря на простоту и распространенность, Bluetooth плохо подходит для средних и больших помещений, а также для одновременной работы множества устройств. Это может стать ключевой проблемой при построении сети. Zigbee лишен данных недостатков.

### 4.2.3 Сравнение с Z-Wave

Z-Wave — это технология беспроводной домашней автоматизации для квартир, домов и небольших офисов. По факту Z-Wave является аналогом

Zigbee, работающим на других частотах (если Zigbee работает на 2,4 ГГц, то Z-Wave на 800-900 МГц).

В качестве преимуществ Z-Wave выделяют:

– **Низкое энергопотребление**. Как и Zigbee, Z-Wave был специально разработан для устройств с батарейным питанием.
– **Надёжная сеть**. Как и в Zigbee, ячеистая сетевая архитектура обеспечивает надёжную сеть связи в умном доме.
– **Функциональная совместимость**. Как и Zigbee, Z-Wave обладает высокой функциональной совместимостью, что позволяет устройствам разных производителей беспрепятственно работать вместе.
– **Повышенная безопасность**. Как и Zigbee, Z-Wave предлагает надёжные меры для решения проблем с безопасностью.

В качестве недостатков Z-Wave выделяют:

– **Низкая скорость передачи данных**. Как и Zigbee, Z-Wave не подходит для ситуаций, когда требуется высокая скорость передачи данных (например, потоковая передача видео с камеры видеонаблюдения).
– **Ограниченное количество устройств**. Максимальное количество устройств для одной сети Z-Wave составляет 232 устройства.

**Вывод**. Zigbee и Z-Wave являются очень похожими стандартами, поэтому конечный выбор ними, вероятно, будет зависеть от выбора устройств, поддерживающих тот или иной стандарт связи.

### 4.2.4 Сравнение с Thread

Thread — это новая технология беспроводной связи, сочетающая сильные стороны Zigbee и Wi-Fi. Концептуально, Thread очень похож на Zigbee, за исключением использования IPv6 для адресации.

В качестве преимуществ Thread выделяют:

– **Низкое энергопотребление**. Как и Zigbee, Thread был специально разработан для устройств с батарейным питанием.
– **Надёжная сеть**. Как и в Zigbee, ячеистая сетевая архитектура обеспечивает надёжную сеть связи в умном доме.
– **Повышенная безопасность**. Как и Zigbee, Thread предлагает надёжные меры для решения проблем с безопасностью.

В качестве недостатков Thread выделяют:

– **Низкая скорость передачи данных**. Как и Zigbee, Thread не подходит для ситуаций, когда требуется высокая скорость передачи данных (например, потоковая передача видео с камеры видеонаблюдения).
– **Малое количество устройств**. Thread является молодой технологией, поэтому устройств с его поддержкой еще достаточно мало.

**Вывод**. Thread является интересной, но молодой технологией, в связи с чем еще достаточно мало устройств поддерживают этот стандарт связи. Из-за этого в большинстве случаев Zigbee будет являться более предпочтительным решением.

### 4.2.5 Сравнение с Matter

Matter — это новая технология беспроводной связи, которая повторяет внутреннее устройство Thread, а также поддерживает работу с Wi-Fi, Ethernet и Bluetooth.

В качестве преимуществ Matter выделяют:
– **Низкое энергопотребление**. Как и Zigbee, Matter был специально разработан для устройств с батарейным питанием.
– **Надёжная сеть**. Как и в Matter, ячеистая сетевая архитектура обеспечивает надёжную сеть связи в умном доме.
– **Повышенная безопасность**. Как и Matter, Thread предлагает надёжные меры для решения проблем с безопасностью.
– **Работа на высоких и низких скоростях**. Matter позволяет разным устройствам, в зависимости от требований, работать как на низких скоростях (например, для экономии энергии), так и на высоких (например, для передачи видеоконтента).

В качестве недостатков Matter выделяют:
– **Малое количество устройств**. Matter является молодой технологией, поэтому устройств с его поддержкой еще достаточно мало.

**Вывод**. Matter является самым амбициозным из всех ранее перечисленных стандартов связи. Однако он также является молодой технологией, в связи с чем еще достаточно мало устройств поддерживают этот стандарт связи. Из-за этого в большинстве случаев Zigbee будет являться более предпочтительным решением.

# ЗАКЛЮЧЕНИЕ

Как было показано, технология Zigbee имеет ряд преимуществ, которые выгодно выделяют ее на фоне конкурирующих технологий. Таковыми являются и низкое энергопотребление, и высокая надежность сети, равно как и повышенная безопасность.

Технология Zigbee существует уже несколько десятилетий. За это время было выпущено немало устройств, которые поддерживают и работа которых основывается на данной технологии. Это, в свою очередь, доказывает, что Zigbee является зрелой и проверенной технологией.

Все вышеперечисленное в совокупности демонстрирует, что Zigbee отлично подходит для создания масштабируемых и отказоустойчивых сетей для работы интернета вещей.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Что такое интернет вещей и как он устроен [Электронный ресурс]. — URL: https://practicum.yandex.ru/blog/chto-takoe-internet-veschey-primenenie-tehnologii/ (дата обр. 14.09.2024).
2. IoT для умных часов и IIoT для умных станков: что такое интернет вещей и каким он бывает [Электронный ресурс]. — URL: https://cloud.vk.com/blog/iot-dlya-umnyh-chasov-iiot-umnyh-stankov-internet-veshchej (дата обр. 14.09.2024).
3. Что такое интернет вещей? Определение и описание [Электронный ресурс]. — URL: https://www.kaspersky.ru/resource-center/definitions/what-is-iot (дата обр. 14.09.2024).
4. Особенности проектирования беспроводных ZigBee-сетей на базе микроконтроллеров фирмы Jennic [Электронный ресурс]. — URL: https://wireless-e.ru/wpan/zigbee/jennic/ (дата обр. 14.09.2024).
5. Сети ZigBee. Зачем и почему? [Электронный ресурс]. — URL: https://habr.com/ru/articles/155037/ (дата обр. 14.09.2024).
6. Беспроводные сети ZigBee. Часть 1 [Электронный ресурс]. — URL: https://habr.com/ru/companies/efo/articles/281048/ (дата обр. 14.09.2024).
7. Сети стандарта IEEE 802.15.4 [Электронный ресурс]. — URL: https://www.rovdo.com/ieee-802-15-4-networks (дата обр. 14.09.2024).
8. Обзор стека протокола ZigBee [Электронный ресурс]. — URL: https://www.rovdo.com/zigbee-stack (дата обр. 14.09.2024).
9. Сетевой уровень [Электронный ресурс]. — URL: https://www.rovdo.com/zigbee-stack-nwk (дата обр. 14.09.2024).
10. Как устроена сеть ZigBee [Электронный ресурс]. — URL: https://tech-geek.ru/zigbee-network-security/ (дата обр. 14.09.2024).
11. Адресация и профили ZigBee [Электронный ресурс]. — URL: https://russianelectronics.ru/adresacziya-i-profili-zigbee/ (дата обр. 14.09.2024).
12. Уровень приложения (APL) [Электронный ресурс]. — URL: https://www.rovdo.com/zigbee-stack-apl (дата обр. 14.09.2024).

13. Спецификация ZigBee. Безопасность [Электронный ресурс]. — URL: https://habr.com/ru/articles/158355/ (дата обр. 14.09.2024).

14. Чем отличаются протоколы умного дома и какой выбрать [Электронный ресурс]. — URL: https://journal.citilink.ru/articles/chem-otlichayutsya-protokoly-umnogo-doma-i-kakoj-vybrat/ (дата обр. 14.09.2024).

15. Wi-Fi, Bluetooth, Z-Wave или ZigBee: какой протокол умного дома выбрать [Электронный ресурс]. — URL: https://www.ixbt.com/live/chome/wi-fi-bluetooth-z-wave-ili-zigbee-kakoy-protokol-umnogo-doma-vybrat.html (дата обр. 14.09.2024).

16. Как работает Matter и другие протоколы умного дома [Электронный ресурс]. — URL: https://thecode.media/kak-rabotaet-matter-i-drugie-protokoly-umnogo-doma/ (дата обр. 14.09.2024).