Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

**Институт Компьютерных Наук и Кибербезопасности**

**Высшая школа Кибербезопасности и Защиты Информации**

**КУРСОВАЯ РАБОТА**

**Технология Zigbee**

по дисциплине «Безопасность интернета вещей»

Выполнила

студентка гр. 5151003/90801 Кулеева А.Г.

Руководитель:

Профессор, д.т.н. Лаврова Д.С.

«\_\_\_» \_\_\_\_\_\_\_\_\_ 2023 г.

Санкт-Петербург

2023

СОДЕРЖАНИЕ

|  |  |  |
| --- | --- | --- |
| Введение ………………………………………………………………….. | | 4 |
| 1. | Описание принципов работы………………………………….. | 5 |
| 1.1. | Сетевые технологии для беспроводной связи……………….. | 5 |
| 1.2. | Сравнение сетевых топологий………….…………………….. | 6 |
| 1.3. | Типовая структура сети ZigBee………..……………………… | 7 |
| 1.4. | Энергосбережение………….………………………………….. | 8 |
| 1.5. | Разработка стандартных ZigBee-устройств………………….. | 9 |
| 1.6. | С чего начать?………………………………………………….. | 11 |
| 1.6.1. | Радиомодуль………………….………………………………… | 11 |
| 1.6.2. | Программная реализация стека ZigBee………………………. | 12 |
| 2. | Применение в умных домах…………………………………... | 13 |
| 2.1. | Использование хаба…………….…………………….……….. | 14 |
| 2.2. | Как избежать перегрузки Wi-Fi сети…………………………. | 15 |
| 2.3. | Как улучшить качество соединения Zigbee………………….. | 16 |
| 2.4. | Голосовой помощник………………………………………….. | 17 |
| 3. | Спецификация ZigBee. Безопасность………………………… | 18 |
| 3.1. | Архитектура безопасности……………………………………. | 20 |
| 3.2. | Центр управления безопасностью……………………………. | 22 |
| 4. | Уязвимости ZigBee……………………………………………. | 24 |
| 4.1. | По структуре сети……………………………………………… | 24 |
| 4.1.1. | Атаки на физический уровень………………………………… | 24 |
| 4.1.2. | Атаки на сетевой уровень…………………………………….. | 25 |
| 4.1.3. | Атаки на прикладной уровень………………………………… | 26 |
| 4.2. | По целям злоумышленника…………………………………… | 27 |
| 4.2.1. | Атаки на конфиденциальность……………………………….. | 27 |
| 4.2.2. | Атаки на целостность………………………………….……… | 28 |
| 4.2.3 | Атаки на доступность…………………………………………. | 28 |
| 5 | Подходы к устранению проблем безопасности……………… | 29 |
| Заключение ……………………………………………………………… | | 31 |
| Список использованной литературы ………………………………….. | | 32 |

Введение

**Zigbee** — спецификация сетевых протоколов уровня приложений и сетевого уровня, использующих сервисы нижних уровней — уровня управления доступом к среде MAC и физического уровня, регламентированных стандартом IEEE 802.15.4. Спецификация Zigbee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

Основная особенность технологии Zigbee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация Zigbee содержит возможность выбора алгоритма маршрутизации в зависимости от требований приложения и состояния сети, механизм стандартизации приложений, профили приложений, библиотеку стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации. [1]

# Описание принципов работы

## Сетевые технологии для беспроводной связи

Существует большое количество беспроводных технологий, каждая из которых имеет свои особенности. В таблице ниже рассмотрены беспроводные протоколы связи для частоты 2,4 ГГц.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 1 — Сравнительная таблица популярных беспроводных технологий

**Технология Wi-Fi**. Технология Wi-Fi создавалась в качестве замены проводного интерфейса Ethernet. Поэтому эта технология предлагает большие скорости передачи данных, но не позволяет разрабатывать узлы, работающие длительное время от источников питания малой емкости ввиду большого энергопотребления.

**Технология Bluetooth**. Технология Bluetooth с появлением стандарта 4.0 (Bluetooth Smart или Bluetooth Low Energy) стала гораздо привлекательней для разработчиков носимой электроники, так как энергопотребление по сравнению с предыдущими версиями сократилось в разы. Но если стоит задача построения беспроводной малопотребляющей системы, которая будет охватывать несколько комнат или даже зданий, эта технология не подойдет, так как поддерживается только сетевая топология «*звезда*». Это же справедливо и для Wi-Fi.

Технология ZigBee. Технология ZigBee изначально разрабатывалась для создания надежных распределенных сетей датчиков и управляющих устройств с невысокими скоростями передачи данных. В этих технологиях реализована поддержка сетевой топологии «*mesh*», спящих и мобильных узлов, а также узлов, которые обеспечивают работу алгоритмов ретрансляции и самовосстановления. В таблице указана скорость 250 кбит/с — это максимальная пропускная способность сети. Полезная скорость будет порядка 30-40 кбит/с в пределах соседних узлов и 5-25 кбит/с при использовании ретрансляции. [2]

## Сравнение сетевых топологий

На Рисунке 2 рассмотрим отличия сетей с различными топологиями и протоколами.

Изображение выглядит как диаграмма, текст, карта, линия

Автоматически созданное описание

Рисунок 2 — Различные сети

В сетях Bluetooth и Wi-Fi сетевое взаимодействие идет через центральный шлюз. И если он выйдет из строя, то обмен данными станет невозможным. Кроме этого, отдельные узлы могут остаться без связи, если неожиданно возникла преграда на пути следования радиосигнала.

В сетях ZigBee надежность связи повышается за счет наличия избыточных связей между устройствами. Все устройства, которые не уходят в спящий режим, выполняют роль **роутеров**, которые ответственны за маршрутизацию сетевого трафика, выбора оптимального маршрута следования и ретрансляцию пакетов. Даже если из строя выйдет устройство, которое выступало в качестве организатора сети, ZigBee-сеть продолжит функционировать дальше. Возникновение помехи или преграды, а также выход какого-либо из роутеров из строя не является критичным за счет наличия избыточных связей. Поэтому с введением дополнительных узлов, которые имеют стационарное питание и могут выполнять задачи роутера, сеть становится более отказоустойчивой. [2]

## Типовая структура сети ZigBee

Теперь остановимся на структуре самой сети ZigBee и типах устройств, которые в ней могут быть.

Изображение выглядит как круг, линия, диаграмма

Автоматически созданное описание

Рисунок 3 — Типовая структура сети ZigBee

**Координатор** — это узел, организовавший сеть. Именно 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.

**Роутер** — это узел, который имеет стационарное питание и следовательно 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. Например, роутерами в сети ZigBee могут быть умные розетки, блоки управления осветительными приборами или любое другое устройство, которое имеет подключение к сети электропитания.

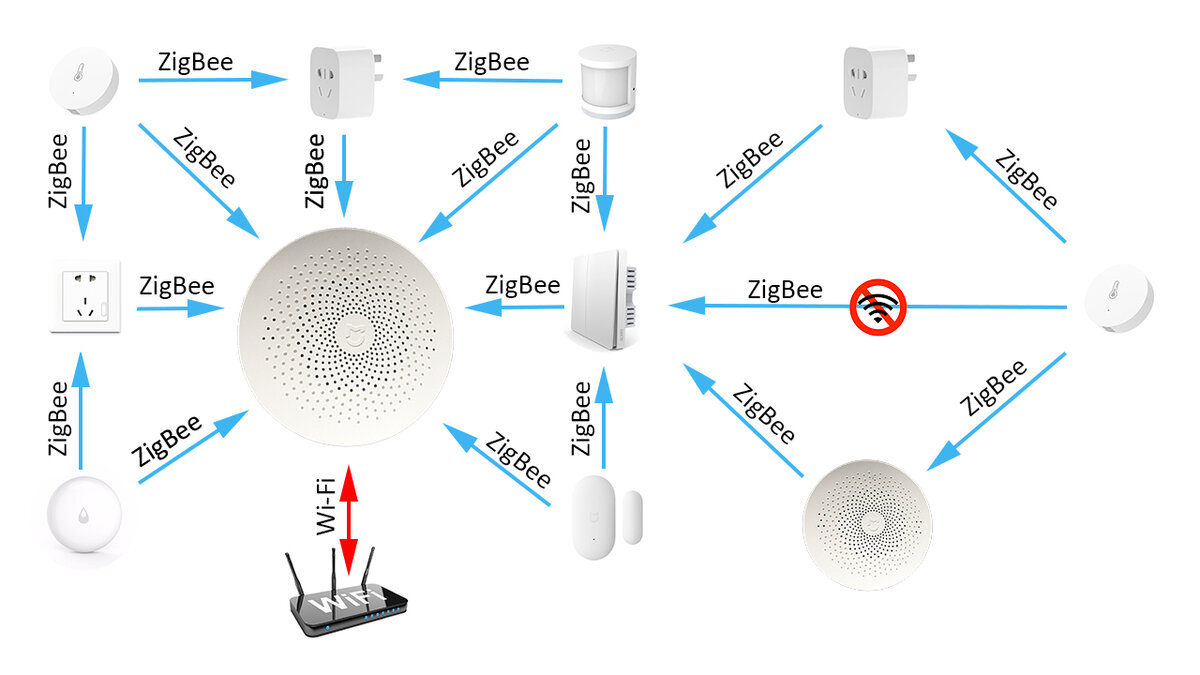
**Конечное устройство** — это устройство, которое подключается к сети через родительский узел и не участвует в маршрутизации трафика. Все общение с сетью для них ограничивается передачей пакетов на «родительский» узел либо считыванием поступивших данных с него же. «Родителем» для таких устройств может быть любой роутер или координатор. Конечные устройства большую часть времени находятся в спящем режиме и отправляют управляющее или информационное сообщение обычно только по определенному событию (нажатие кнопки выключателя, открытие окна или двери). Это позволяет им долго сохранять энергию встроенного источника питания. Примером конечных устройств в сетях ZigBee могут быть беспроводные выключатели, управляющие работой светильников и работающие от батареек, датчики протечки воды, датчики открытия/закрытия дверей. [2]

## Энергосбережение

Ещё одним не менее важным аспектом работы на этом протоколе является энергосбережение. Wi-Fi устройства имеют более высокое энергопотребление по сравнению с устройствами Zigbee. Для беспроводных датчиков такой уровень потребления недопустим, так как пришлось бы менять батарейки слишком часто.

Так как конечные устройства большую часть времени находятся в спящем режиме и просыпаются лишь для опроса родительского узла на наличие сообщений для себя, либо для передачи данных, то это позволяет менять батарейку придется раз в несколько лет.

Сеть умеет автоматически настраиваться для создания наилучшей связи. При отключении одного из роутеров, конечные устройства ищут другой роутер или координатор.



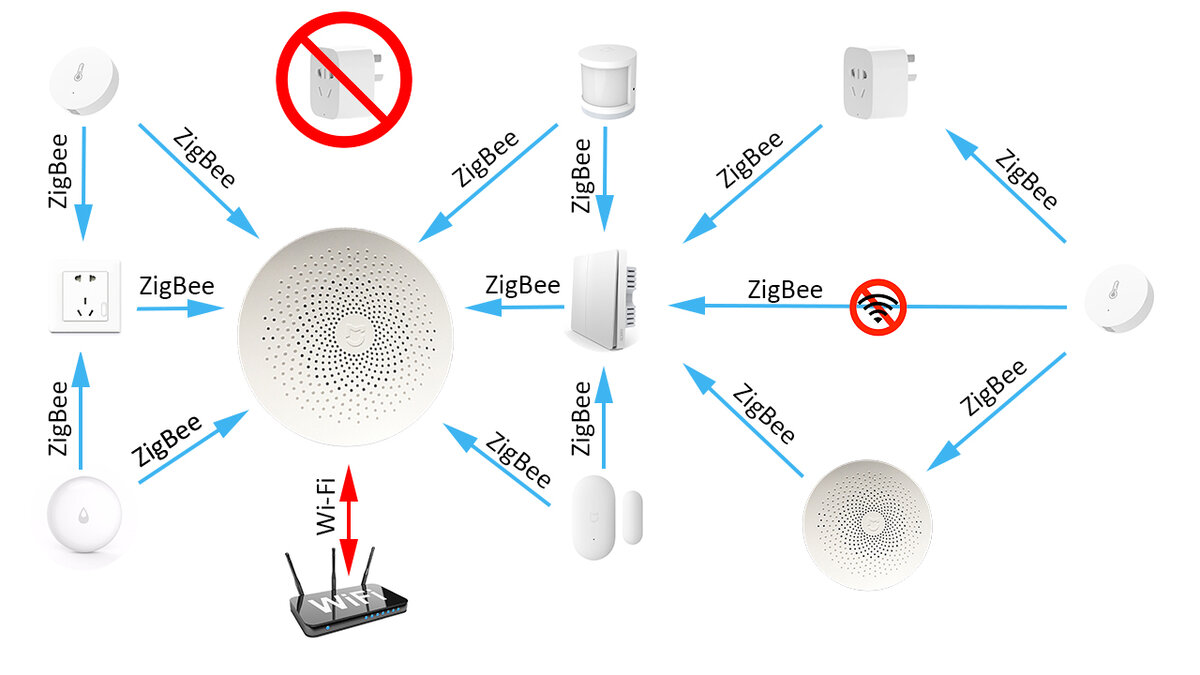


Рисунок 4 — Пример самостоятельной переорганизации сети

## Разработка стандартных ZigBee-устройств

Чем выделяется ZigBee среди других таких же проприетарных протоколов с поддержкой mesh-топологии? Альянсом ZigBee за все те годы, что существует технология, была проведена большая работа по стандартизации не только сетевого уровня, но и уровня приложения разрабатываемых устройств. Имеется большая библиотека кластеров ZigBee (ZCL), описывающая свыше 200 устройств, таких как выключатели, блоки управления освещением, интерфейс для подключения датчиков, счетчиков и многое другое. И для некоторых типов систем (системы домашней автоматизации, системы сбора показаний со счетчиков и др.) разработаны специальные профили, в которые входит целый набор стандартных устройств. Они позволяют беспроводным узлам различных производителей понимать друг друга на уровне приложения. Стандартный профиль описывает стандартные команды и поведения конкретного устройства, например блока управления системой климат-контроля или блока управления светильником.

**Пример взаимодействия устройств со стандартным профилем**

Изображение выглядит как текст, снимок экрана, диаграмма, круг

Автоматически созданное описание

Рисунок 5 — Пример использования протокола

Пример того, как может быть реализована система управления освещением с использованием стандартной библиотеки кластеров:

* у лампочки есть набор хранимых атрибутов (состояние: включена/выключена; уровень яркости)
* выключатель может отправлять команды для изменения доступных атрибутов лампочки
* при получении команды лампочка принимает указанное состояние

В библиотеке кластеров указывается, какие атрибуты и команды являются обязательными для тех или иных устройств, а какие опциональными. Это позволяет реализовать стандартный интерфейс взаимодействия между ZigBee-устройствами.

## С чего начать?

### Радиомодуль

Для быстрого старта, когда нет желания или возможности разбираться с программным стеком ZigBee, стоит обратить внимание на модули ETRX357. Все модули имеют встроенную прошивку от производителя, которая позволяет работать с аналоговой и цифровой периферией, а также с сетевыми функциями, с помощью набора AT-команд. Для начала работы с радиомодулем достаточно подключить линии питания и линии TxD и RxD последовательного интерфейса UART.

Изображение выглядит как текст, Электронный компонент, Компонент схемы, Пассивный компонент цепи

Автоматически созданное описание

Рисунок 6 — Радиомодуль

В стандартную прошивку входит также ряд функций, которые могут вызываться по прерыванию от порта ввода/вывода, таймера/счетчика или при определенных событиях, таких как подключение к сети или инициализация радиомодуля. Пример доступных функций:

* Переключение состояния порта ввода/вывода
* Отправка информации на узел сбора данных о состоянии 16 цифровых выводов радиомодуля, оцифрованных данных от подключенных датчиков и информацию об уровене напряжения питания
* Переход в активный режим или режим энергосбережения
* Открытие «прозрачного канала» с другим устройством в сети

Пару слов о «прозрачном канале». При переходе в данный режим вся информация, поступающая по интерфейсу UART на радиомодуль транслируется на интерфейс UART другого радиомодуля. Данный канал является двунаправленным, а также наследует преимущества технологии ZigBee: при наличии роутеров в сети не будет происходить потери данных в таком канале связи так как все пакеты «прозрачного канала» будут в случае необходимости автоматически ретранслироваться. За счет этого можно организовать канал связи с предельной дальностью в несколько километров. [2]

### Программная реализация стека ZigBee

Если стандартных возможностей прошивки не хватает, то можно использовать реализацию программного стека ZigBee от компании Silicon Labs — Ember ZNet PRO. Так как модули выполнены на базе микросхемы EM357, то переход от стандартной прошивки к разработке собственного приложения потребует лишь приобретение программатора-отладчика ISA3 с помощью которого можно делать как внутрисхемную отладку устройства, так и отлаживать приложение на сетевом уровне. Справа на рисунке показан пример того, как отображаются данные о пути следования пакета и его расшифровка.

**Изображение выглядит как текст, программное обеспечение, снимок экрана, веб-страница

Автоматически созданное описание**

Рисунок 7 — Сниффинг пакетов

Для упрощения процесса создания приложения предоставляется компоновщик приложений, который для выбранной конфигурации ZigBee-устройства генерирует каркас приложения и создает функции, в которых разработчик должен дописать требуемую логику приложения.  
Все утилиты входят в программный пакет Simplicity Studio, куда также входит демонстрационная версия стека Ember ZNet PRO. Поэтому можно прямо сейчас скачать и посмотреть, как это работает. [2]

# Применение в умных домах

Сети Zigbee используются в промышленной автоматике, в коммерческой недвижимости и в медицинском оборудовании. Но, безусловно, наиболее широкое и популярное применение Zigbee — это системы умного дома.

До того, как на рынок умного дома вышли компании Apple, Google и Amazon, некоторое время был популярен стандарт Z-Wave. Этот протокол был конкурентом Zigbee, но он закрытый, и производители устройств для умного дома должны покупать модуль Z-Wave у европейского производителя. Zigbee же — открытый стандарт, и любая компания может производить свои модули согласно открытой спецификации. Поэтому Zigbee-устройства дешевле, чем приборы с Z-Wave, и сейчас уже однозначно можно сказать, что протокол Zigbee победил и стал де-факто стандартом для систем умного дома. ZigBee используют все крупные компании на рынке умного дома: Amazon, Philips, Samsung, Xiaomi, LG, Logitech, IKEA и многие другие. Однако у тандема ZigBee + Z-Wave есть один существенный минус: гаджеты зачастую несовместимы с гаджетами других производителей. При покупке устройств стоит обращать внимание на их совместимость.

В продаже есть все электроприборы с Zigbee, какие только можно себе представить: лампочки, выключатели, розетки; датчики движения, утечки и дыма, открытия дверей и окон; кондиционеры, термостаты, камеры и многое другое. Но нужно отметить, что само наличие Zigbee-модуля не делает устройства от разных производителей совместимыми между собой (также, как в устройствах для умного дома с Wi-Fi модулем). Например, зигби-лампочка Икея не будет работать с зигби-хабом Xiaomi. Но некоторые компании добавляют поддержку конкретных устройств от других производителей, например те же лампочки от Икеи будут работать совместно с мостом Philips Hue Bridge. [5]

## Использование хаба

Для построения большой сети в умном доме стоит приобрести Хаб. Хаб — это управляющий центр умного дома. Через него проходят все команды, которые он в дальнейшем передаёт нужному датчику. Хаб связывает беспроводную ZigBee-сеть с интернетом. Он позволяет вам из любой точки мира соединяться с домом, проверить его состояние и управлять устройствами. Для удаленного управления Умным домом ZigBee-сеть должна быть подключена к интернету, как раз для этого и используются сетевые мосты, они же смарт хабы.

Современный умный дом нельзя себе представить без возможности удалённого управления. Например: вы гладили вещи перед работой, очень торопились, ведь с утра назначено важное совещание, на которое вы сильно опаздываете. Вы выбегаете из дома, садитесь в такси и уже подъезжая к работе, вспоминаете, что не выключили утюг. Но есть удалённый доступ! Вам достаточно зайти в приложение на своем телефоне и проверить выключили ли вы утюг из розетки, а если нет — выключить розетку. [3, 4]

## Как избежать перегрузки Wi-Fi сети

Выше уже говорилось о высоком энергопотреблении Wi-Fi: если бы умный дом использовал этот тип соединения, датчикам понадобились мощные аккумуляторы — сделать их такими же миниатюрными стало бы невозможно. Но у Wi-Fi также есть и другая проблема: чем больше устройств подключается к Wi-Fi-роутеру, тем выше нагрузка на роутер и тем менее стабильна сеть.

В этом успели убедиться покупатели WiFi-лампочек: одна или две лампочки никак не влияют на работу сети. Но когда лампочек становится пять-десять, многие роутеры перестают справляться, начинают перезагружаться, а скорость интернета на смарт-тв, ноутбуках и смартфонах становится все ниже.

В умном доме Aqara к роутеру подключается только одно устройство — сам Aqara Hub. Таким образом умный дом не помешает работе интернета на основных устройствах пользователя — нагрузка равномерно распределится между устройствами:

Изображение выглядит как диаграмма, зарисовка, круг, графическая вставка

Автоматически созданное описание Изображение выглядит как диаграмма, зарисовка, рисунок, дизайн

Автоматически созданное описание

Рисунок 8 — Распределение нагрузки на сеть

Но, как всегда, есть тонкости. Zigbee работает на той же частоте что и Wi-Fi-роутеры — 2.4GHz. Хотя протоколы и отличаются, физику не обманешь: пересечение радиоканалов дурно сказывается на стабильности соединения. Причем, как показывают отзывы пользователей, чаще страдает соединение устройств умного дома, в то время WiFi продолжает работать без сбоев. Заметить проблему можно по долгому отклику: если между нажатием беспроводного выключателя и выключением лампочки проходит больше пары секунд, следует поискать способ оптимизировать домашнюю сеть. Есть несколько способов решить эту проблему. [4]

## Как улучшить качество соединения Zigbee

* Разместить Хаб дальше от роутера. Так Хаб не окажется в радиусе действия максимально сильного сигнала Wi-Fi.
* Увеличить число умных розеток. Поскольку каждая умная розетка усиливает сигнал Zigbee, стабильность сети возрастет.
* Исключить пересечение сигналов Zigbee и Wi-Fi. Обычно Wi-Fi-роутер позволяет выбрать канал, на котором раздается сигнал. В диапазоне 2.4.GHz есть три канала, область действия которых не пересекается. Их принято обозначать числами: 1, 6 и 11:

Изображение выглядит как снимок экрана, дизайн

Автоматически созданное описание

Рисунок 9 — Каналы Wi-Fi

Точно так же и Zigbee: он работает на одном и каналов в диапазоне 11-26. Правда нумерация каналов здесь отличается от каналов Wi-Fi. Если совместить две системы обозначений, получится такая схема:

Изображение выглядит как снимок экрана, искусство, дизайн

Автоматически созданное описание

Рисунок 10 — Каналы Zigbee

Скорее всего, Хаб работает на одном из каналов между 20 и 22. Нужно настроить роутер, так чтобы он работал только на первом канале Wi-Fi —у него нет пересечений с каналами 20-26 Zigbee. Перезагрузим его и спустя 10 минут проверим, не ускорится ли работа умного дома. [4]

## Голосовой помощник

Помимо возможности удалённого использования, подключение умного дома из Zigbee устройств к интернету открывает ещё одну возможность, без которой в 2023 году нельзя себе представить современный умный дом. Это возможность голосового управления умным домом через голосового помощника: Яндекс Алиса, Apple Siri, Google Ассистент или Amazon Alexa.

Чтобы эта функция работала, у производителя хаба должна быть сертификация от соответствующей IT-компании. Например, для управления Zigbee лампочками с помощью Сири на iPhone или HomePod, необходимо выбирать умный хаб с поддержкой HomeKit (ищите логотип “Works with Apple HomeKit”). Некоторые хабы предоставляют интеграцию сразу со всеми голосовыми помощниками, например Philips Hue Bridge, в то время как другие поддерживают только одного помощника. [5]

# Спецификация ZigBee. Безопасность

Отличительной чертой сетей ZigBee является гарантированная, устойчивая к помехам, многолучевому затуханию, различным сбоям и отказам передача данных. К этому следует добавить: не только гарантированная, но и безопасная передача, что важно для многих критических приложений. Нетрудно представить, к чему может привести несанкционированное вмешательство в работу системы управления техпроцессом или системы охраны. Вместе с тем, в менее критических приложениях должна существовать возможность снижения цены устройств за счет некоторого снижения требований к уровню безопасности. Именно такой подход реализуется в модели безопасности ZigBee.

Основным механизмом обеспечения конфиденциальности в сетях ZigBee является надлежащая защита всех ключевых данных. А основой безопасности — доверительные отношения, которые обязательны как на стадии первоначальной установки ключей, так и в процессе обработки информации, касающейся безопасности. То есть, обмен данными должен производиться только между доверяемыми сторонами. Этот подход последовательно пронизывает всю иерархию обмена данными.

Спецификация ZigBee регламентирует безопасность на уровнях NWK и APS и опирается на базовую структуру безопасности, регламентированную стандартом IEEE 802.15.4. Безопасность приложений обеспечивается посредством профилей приложений. [6]

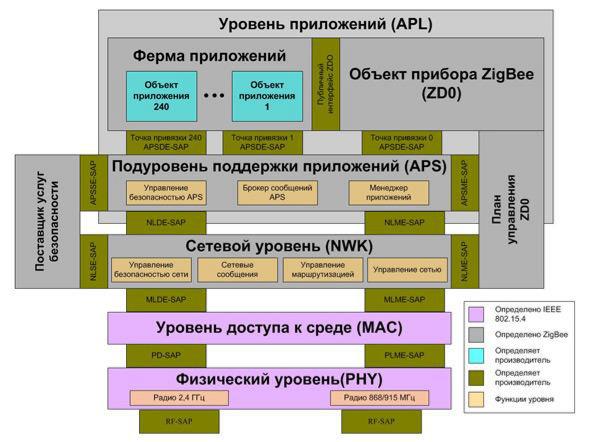


Рисунок 11 — Стек протоколов ZigBee

Ключи являются краеугольным камнем архитектуры безопасности ZigBee. Их защита имеет первостепенное значение, и ключи никогда не должны передаваться по не защищенным каналам. Кратковременное (и единственное) исключение из этого правила имеет место только в момент присоединения к сети ранее не настроенного устройства.

Спецификация ZigBee предусматривает особые меры безопасности, поскольку создаваемые в том или ином случае сети могут оказаться физически доступными для внешних устройств, а конкретные рабочие среды могут быть непредсказуемы. Более того, различные приложения, запускаемые одновременно и использующие для связи один и тот же трансивер, должны быть взаимно доверенными, поскольку из соображений стоимости модель не предусматривает брандмауэра между объектами приложений.

В стеке протокола различные слои не разделены криптографически, поэтому политика доступа обязательна и требует правильного проектирования. Открытая модель доверия внутри устройства позволяет разделение ключа, что особенно уменьшает потенциальную стоимость устройства.

Тем не менее, слой, который создает фрейм, отвечает за его безопасность. Если существует риск появления вредоносных устройств, вся полезная нагрузка на создающем ее слое должна шифроваться, чтобы несанкционированный трафик мог быть немедленно отсечен. Исключением, как уже упоминалось, является передача новому присоединяемому устройству сетевого ключа, который передает ему уровень единой безопасности сети.

## Архитектура безопасности

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. Этот стандарт тоже предоставляет кое-какие возможности в плане безопасности и дает возможность провести взлом систем умного дома по этому протоколу.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 12 — Система безопасности

Когда выставлен третий бит в FC (Frame Control), появляется дополнительный заголовок **AUX Security Header**, который, в свою очередь, определяет уровень безопасности (Security Level), а также включает в себя 32-битный счетчик, позволяющий исключить простейшие атаки типа replay.

ZigBee использует 128-битные ключи для реализации механизмов безопасности. Ключ может быть ассоциирован либо с сетью (и использоваться уровнями ZigBee и MAC подуровнем), 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. Главный ключ и ключи каналов связи видны только на уровне приложений. Различные сервисы используют различные вариации ключа канала связи во избежание утечки и риска для безопасности.

Распределение ключей является одной из наиболее важных функций безопасности сети. В защищенной сети назначается одно специальное устройство, которому другие устройства доверяют распределение ключей безопасности — центр управления безопасностью. В идеале каждое устройство в сети должно иметь предварительно загруженные адрес центра управления безопасностью и первоначальный главный ключ. Приложения без особых требований к безопасности могут использовать сетевой ключ, передаваемый центром управления безопасностью через не защищенный на момент передачи канал.

Таким образом центр управления безопасностью поддерживает ключ сети и обеспечивает безопасность точка-точка. Устройства будут принимать только сообщения, зашифрованные с использованием ключа, предоставленного центром управления безопасностью, за исключением первоначального главного ключа.

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 фреймы 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.
* Уровень приложений устанавливает ключи и оказывает транспортные услуги как объекту устройства (ZDO), так и приложениям. Он отвечает также за распространение сообщений об изменениях в устройствах внутри сети, которые могут исходить как от самих устройств (например, простое изменение статуса), так и от центра управления безопасностью (который может сообщить, что определенное устройство удаляется из сети). Уровень также маршрутизирует запросы устройств центра управления безопасностью и обновления сетевого ключа от центра управления безопасностью всем устройствам.

Объект устройства ZDO поддерживает политики безопасности устройства.

## 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. 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. Обычно центром управления безопасностью по совместительству является координатор сети, но это может быть и выделенное устройство. Центр управления играет следующие роли в обеспечении безопасности:

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

Типы ключей. ZigBee использует три типа ключей для управления безопасностью:

1. главный ключ,
2. сетевой ключ и
3. ключ канала связи.

**Главный ключ**

Этот 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.

**Сетевые ключи**

Эти ключи обеспечивают 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.

**Ключи каналов связи**

Эти ключи обеспечивают безопасную одноадресную передачу сообщений между двумя устройствами на уровне приложений.

**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.

# Уязвимости ZigBee

## По структуре сети

### Атаки на физический уровень

Это атаки на физическую безопасность устройств, такие как физический доступ к узлам или перехват радиочастотного сигнала. Тут может быть, например зашумление частотного канала, как описывалось выше в разделе об улучшении качества Wi-Fi. Поскольку в сети есть роутеры, питающиеся от электричества, можно попытаться вывести из строя некоторые розетки, повредить проводку. Тогда упадет либо вся система, либо если отключится несколько роутеров, нагрузка на оставшиеся станет выше, к тому же некоторые роутеры также участвуют в сети типа «звезда», соответственно, конечные устройства тоже упадут. Менее кардинальный способ — повредить конкретно сеть Wi-Fi. Тогда пользователь потеряет возможность удаленного управления или управления с помощью голосового помощника.

### Атаки на сетевой уровень

Это атаки на протоколы и маршрутизацию в сети ZigBee, такие как атаки на маршруты, перенаправление трафика. Один из их основных видов — это использование link key при подключении новых устройств. Но тут приходится выбирать между удобством для рядовых пользователей и безопасностью. В распределенной сети (только роутеры без координатора) роутеры могут создавать сеть и генерировать ключ к сети (network key). Чтобы устройства могли подключиться к такой сети, они должны иметь pre-configured link key. Pre-configured global link key — дефолтный ключ для ZigBee. Его значение — 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39, что означает ZigBeeAlliance09. Он используется, чтобы шифровать network key. Зачем вообще использовать дефолтный link key, когда можно задать свой и в разы улучшить взломостойкость? Ответ простой: кастомный link key нарушит совместимость, о которой мы говорили чуть ранее. Да и не всякий пользователь захочет подключать лампочку или розетку к программатору или джамерами задавать приватный ключик. Вот и приходится искать баланс между удобством и безопасностью.

Как мы узнали ранее replay атаки исключены, так как каждом из уровней есть Frame Counter, который препятствует этому виду атак.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 13 — Уровни протоколов

Еще один вектор — это конфликт PAN ID. Суть этой атаки в том, что злоумышленник разворачивает ложный координатор. В результате валидный координатор сменяет PAN ID на какое-то другое значение. Но устройства по-прежнему могут быть привязаны к старому PAN ID. Получается, что злоумышленнику удается нарушить целостность сети. Это может привести к тому, что датчик открытия или датчик движения не подаст вовремя тревогу [7].

Также не стоит забывать про разные варианты атак типа DoS или флуд в канале. Например, весь канал может быть забит фреймами ACK.

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Рисунок 14 — ACK Frame

ACK Frame — фрейм подтверждения. Он подтверждает принятые данные по радиоканалу.

Также существует угроза подделки значения frame counter: если узел не проверяет MIC, то, когда придет валидный пакет, его frame counter будет меньше. Согласно стандарту, такие пакеты стоит отбрасывать.

### Атаки на прикладной уровень

Это атаки на приложения и службы, используемые в сети ZigBee, такие как атаки на уязвимости в программном обеспечении или несанкционированный доступ к функциям устройств. Кроме того, есть уязвимости 0 дня в прошивках, протоколе IEEE802, приложениях для удалённого доступа. Например, был случай атак на лампочки Phillips с помощью дрона, а также хакеры показали вариант распространения впо от лампочки к лампочке (на сегодняшний день уязвимость закрыта).

Существуют различные софты для взлома систем умного дома по протоколу ZigBee.

* KillerBee — в описании говорится, что это фреймворк и утилиты для атак на сети ZigBee и IEEE 802.15.4 networks.
* Attify ZigBee Framework — то же самое, что и KillerBee, но с графическим интерфейсом.
* SecBee — для работы требует Scapy-radio, KillerВee и GNU Radio block.
* Z3sec — для полноценной работы требует много дополнительных пакетов.

На самом деле разнообразие только кажущееся и обычно нужно либо дорогое SDR, либо старое вроде Atmel RZ RAVEN USB Stick [8].

## По целям злоумышленника

### Атаки на конфиденциальность:

* Подслушивание (Eavesdropping): Злоумышленник перехватывает и анализирует трафик в сети ZigBee, с целью получить конфиденциальную информацию, такую как пароли, ключи шифрования или другую чувствительную информацию.
* Перехват аутентификационных данных: Злоумышленник злоупотребляет уязвимостями в протоколе аутентификации и перехватывает данные, необходимые для подлинной аутентификации в сети ZigBee. Далее он может сам аутентифицироваться в системе от имени легитимного пользователя, изменить сценарии устройств, отключить их.
* Взлом шифрования: Злоумышленник пытается анализировать или сломать используемый шифр в сети ZigBee, с целью расшифровки зашифрованной информации и получения конфиденциальных данных.

Стоит отметить, что в сети ZigBee нет как таковых чувствительных данных, поскольку весь трафик представляет из себя сообщения вида «выполнить действие над устройством». Самое опасное здесь может быть это перехват паролей при аутентификации с целью дальнейшей выдачи себя за легитимного пользователя. Также можно представить ситуацию, что злоумышленник анализирует трафик с целью составить картину «типичный день владельца умного дома»: когда он приходит домой и когда уходит, когда ложится спать, если в доме есть голосовой помощник, то какие команды ему дает пользователь, отсюда можно выявить хобби владельца. Далее эти данные можно использовать с целью социальной инженерии.

### Атаки на целостность:

* Манипулирование данных: Злоумышленник изменяет передаваемые данные в сети ZigBee, чтобы создать ложное представление о событиях или вводящее в заблуждение влияние на принимающие системы.
* Внедрение вредоносного программного обеспечения: Злоумышленник внедряет вредоносное программное обеспечение в сеть ZigBee для получения контроля над системами, эскалации привилегий или уклонения от обнаружения и антивирусной защиты.
* Рассылка ложных сообщений: Злоумышленник отправляет ложные или манипулированные сообщения в сети ZigBee, вводя других участников в заблуждение или вызывая нежелательные действия на их стороне.

### Атаки на доступность:

* Атаки отказа в обслуживании (DoS): Злоумышленник перегружает сеть ZigBee или конкретное устройство, отправляя большое количество запросов или вызывая другие ошибки, чтобы сделать сеть или устройство недоступными для легитимных пользователей.
* Флуд атаки: Злоумышленник отправляет большое количество бесполезных или нежелательных пакетов данных в сеть ZigBee, перегружая ее и вызывая снижение производительности или отказ в обслуживании.
* Атаки на маршрутизацию: Злоумышленник намеренно изменяет или вводит в заблуждение процесс маршрутизации в сети ZigBee, чтобы перенаправить трафик или создать окружение, в котором легитимные узлы не могут достичь своего назначения.

# Подходы к устранению проблем безопасности

1. Шифрование данных: Один из наиболее эффективных методов защиты сетей ZigBee — использование надежных алгоритмов шифрования для защиты передаваемых данных. Рекомендуется использовать сильные алгоритмы шифрования, такие как AES (Advanced Encryption Standard), для обеспечения конфиденциальности и целостности данных.
2. Аутентификация и авторизация: Реализация механизмов аутентификации и авторизации позволяет удостовериться в идентичности устройств в сети и контролировать их права доступа к ресурсам. Это помогает предотвратить несанкционированный доступ и защитить сеть от злоумышленников.
3. Обновление прошивки: Регулярное обновление прошивки устройств ZigBee помогает исправлять уязвимости и восполнять проблемы безопасности. Обновления прошивки могут исправлять известные уязвимости, улучшать производительность и обеспечивать новые функциональные возможности.
4. Физическая защита: Ограничение физического доступа к устройствам ZigBee также является важным аспектом обеспечения их безопасности. Размещение устройств в надежных, запираемых помещениях и использование механических защитных средств, таких как замки или сенсоры взлома, могут предотвратить несанкционированный доступ к устройствам.
5. Проверка безопасности устройств: При выборе и установке устройств ZigBee важно выбирать только доверенных производителей и проверять их степень безопасности. Проверка уровня безопасности устройств перед их вводом в эксплуатацию или приобретением поможет избежать использования незащищенных устройств.
6. Мониторинг сети: Установка механизмов мониторинга, таких как механизмы обнаружения вторжений или системы контроля доступа, позволит мониторить и анализировать активность в сети ZigBee для раннего обнаружения подозрительной активности или атак.
7. Обучение и осведомленность пользователей: Обучение пользователей по вопросам безопасности и осведомленность о возможных угрозах помогает предотвратить социальные инженерные атаки и повышает общий уровень безопасности в сети ZigBee. Комбинирование этих подходов поможет устранить проблемы безопасности в сети ZigBee и защитить ее от внешних угроз. Важно выполнять регулярное обновление мер безопасности и быть в курсе последних разработок в этой области для эффективной защиты сети.

Заключение

Использование протокола Zigbee обеспечивает стабильную связь между устройствами умного дома:

* снижается нагрузка на WiFi-роутер,
* снижается энергопотребление устройств,
* с помощью умных розеток можно расширить площадь покрытия сигнала Zigbee,
* с помощью настроек роутера можно избежать конфликта сигналов Zigbee и Wi-Fi.

# Список источников

1. <https://ru.wikipedia.org/wiki/Zigbee>
2. <https://habr.com/ru/companies/efo/articles/281048/>
3. <https://vc.ru/s/1308276-vsesmart/551508-tehnologiya-besprovodnoy-svyazi-dlya-umnogo-doma-protokol-zigbee>
4. <https://aqara.ru/2020/03/17/zigbee-технология-сделавшая-возможным/>
5. <https://voiceapp.ru/articles/zigbee#zigbee-smart-home>
6. <https://habr.com/ru/articles/155037/>
7. <https://www.slideshare.net/bishopfox/smarter-home-invasion-with-zigdiggity-165606623>
8. <https://cryptoworld.su/vzlom-sistem-umnogo-doma-ot-a-do-ya-na-primere-protokola-zigbee/#Uazvimosti_ZigBee>