Протокол ZigBee для автоматизации и мониторинга. Обзор архитектуры и использование SDR для приема и расшифровки данных

Д. Р. Богданов

Петербургский государственный университет путей сообщения Императора Александра I

dan.d9@yandex.ru

Д. Н. Роенков

Петербургский государственный университет путей сообщения Императора Александра I

roenkov_dmitry@mail.ru

***Аннотация*. В статье приведен обзор протокола ZigBee, рассмотрены особенности применения программно-определяемого радио (SDR) для приема и анализа радиосигналов от устройств ZigBee. Кроме того, в статье приводятся рекомендации по настройке оборудования и программного обеспечения для работы с устройствами мониторинга данного типа.**

Ключевые слова: ZigBee; мониторинг; датчики; программно-определяемое радио; SDR

I. Что такое протокол ZIGBEE

ZigBee – один из протоколов, который применяется для связи с устройствами умного дома. Его поддержкой наделяют [1] умные лампочки, беспроводные выключатели, датчики движения и прочие устройства. Стандарт появился в 2003 году, в нем реализована поддержка сетевой топологии mesh, спящих и мобильных узлов, а также модулей, которые обеспечивают работу алгоритмов ретрансляции и самовосстановления. Максимальная пропускная способность сети – 250 кбит/с. Полезная скорость составляет около 30-40 кбит/с в пределах соседних узлов и 5–25 кбит/с при использовании ретрансляции. Сравнение с аналогами по дальности, скорости и стоимости приведено на рис. 1.

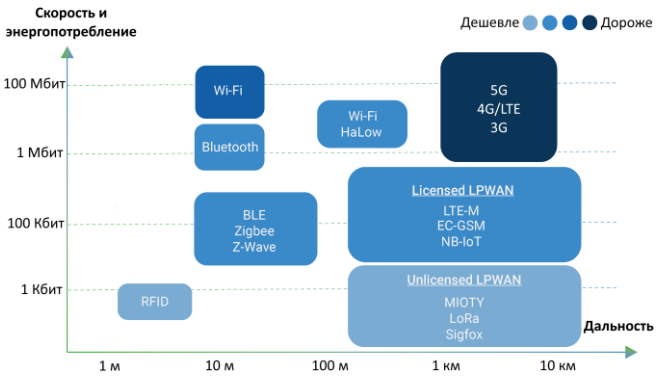

Рис. 1. Сравнение ZigBee с другими стандартами связи

На рис. 2 демонстрируется различие структуры сетей Wi-Fi и ZigBee.

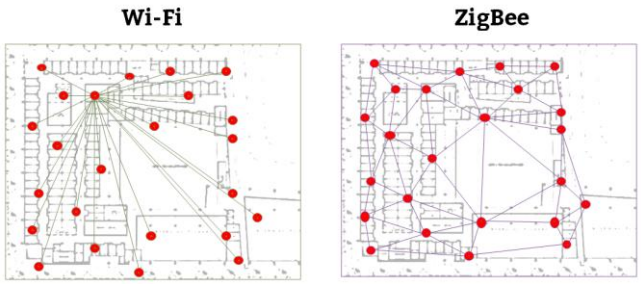

Рис. 2. Сравнение структуры сетей Wi-Fi и ZigBee

ZigBee отлично сбалансирован и при невысокой стоимости дает приемлемые дальность действия и скорость передачи данных. К тому же этот протокол прошел испытание временем и обладает повышенной стабильностью и оперативностью (например, запрос информации от 100 устройств LoRa может растянуться на несколько часов).

II. Топология сети ZIGBEE

Топология сети может быть одной из следующих: звезда, кластерное дерево или mesh-сеть. Графическое представление видов топологии приведено на рис. 3.

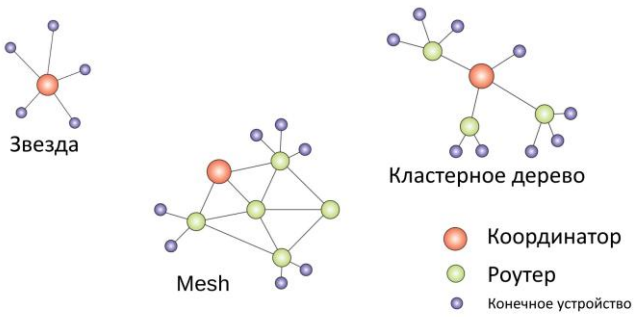

Рис. 3. Виды топологии сетей ZigBee

Координатор (он же **Fully Function Device**) – это главный узел. Он создает сеть, выбирает, на каком канале будет производиться обмен данными, может выступать как «центр доверия» (trust center).

Роутер – устройство, которое служит ретранслятором сообщений от конечных устройств. В малых сетях при отсутствии роутера координатор может

выполнять его функцию. Роутеры регулярно обновляют таблицы маршрутизации, которые используются для прокладки оптимального маршрута и поиска нового, если вдруг какое-нибудь устройство вышло из строя.

Конечное устройство (end device) – мельчайшие объекты сети (выключатели, лампочки, датчики, транспондеры, пульты управления и другие гаджеты). Конечные устройства преимущественно находятся в спящем режиме и отправляют управляющее или информационное сообщение по определенному событию, что позволяет им сохранять свою работоспособность в течение длительного промежутка времени.

Информация по функциональности каждого типа устройств приведена в табл. 1.

ТАБЛИЦА I. СВОДНАЯ ТАБЛИЦА ФУНКЦИОНАЛЬНОСТИ КАЖДОГО ТИПА УСТРОЙСТВ

Функция/Тип устройства	Координатор	Роутер	Конечное устройство
Создание сети ZigBee	+	-	-
Выдача разрешений на присоединение к сети другим устройствам	+	+	-
Назначение сетевого адреса	+	+	-
Обнаружение и запись путей для эффективной доставки сообщений	+	+	-
Обнаружение и хранение списка соседей, доступных в один хоп	+	+	-
Маршрутизация сетевых пакетов	+	+	+
Присоединение и выход из сети	+	+	+
Режим сна	-	-	+

III. Архитектура ZigBee

ZigBee базируется [2] на IEEE 802.15.4, который может работать в трех частотных диапазонах (рис. 4).

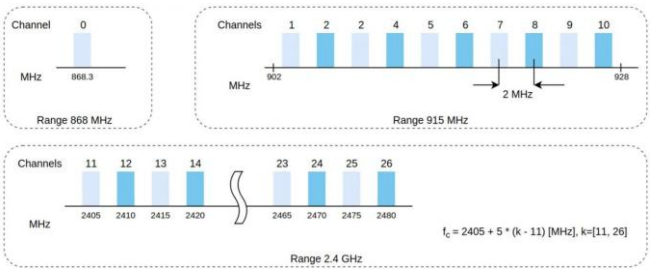

Рис. 4. Частотные диапазоны ZigBee

Стандарт поддерживает функцию **Energy Detection**, что позволяет координатору выбирать канал с наименьшим числом помех. Для уменьшения перекрестных помех между Wi-Fi и ZigBee выбираются следующие каналы (рис. 5).

Рис. 5. Выбор каналов для уменьшения перекрестных помех

При передаче данных по радиоканалу устройства должны определять, в какой момент можно передавать данные, а когда занята несущая и стоит подождать. Для этого в сетях ZigBee/IEEE 802.15.4 применяется режим **Beacon**. В этом случае координатор отправляет маячки (beacons), на основе которых остальные устройства синхронизируются и принимают решения о передаче данных.

PHY и MAC определены стандартом IEEE 802.15.4, вышележащие уровни – это ZigBee. Иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия узлов в сети (стек протокола) ZigBee представлен на рис. 6.

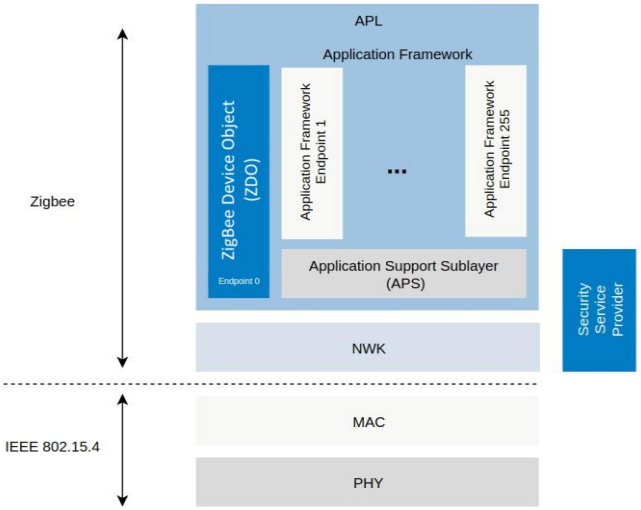

Рис. 6. Стек протокола ZigBee

ZigBee Device Object (ZDO) отвечает за инициализацию устройства – будет ли оно FFD (координатором) или конечным устройством. Также производит настройку и инициализацию NWK (Network Layer) и SSP (Security Service Provider).

Application Support Sublayer (APS) предоставляет программный интерфейс между уровнем NWK и приложениями, которые могут работать на устройстве.

Application Framework – изолированная среда, где выполняются приложения ZigBee.

Основная цель протокола – обеспечить наивысшую совместимость между устройствами. Например, если взять систему освещения с поддержкой ZigBee вендора А от 2015 года и выключатель вендора Б, произведенного в 2025 году, то они без проблем смогут работать в связке.

IV. Защита информации

Для шифрования применяется алгоритм AES-128. Стандартный ключ на расшифровки сообщения ZigBee называется **Pre-configured global link key**. Его значение – 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39, что можно расшифровать как ZigBeeAlliance09. Он нужен,

чтобы выполнять шифрование network key. Помимо этого возможен **Network Rejoin** – подключение к сети на уровне NWK. Но в этом случае конечный узел уже должен знать network key (узел уже подключался к сети).

Network key (NWK key) – используется для шифрования на уровне NWK. Он применяется для коммуникации между всеми узлами сети, произвольно генерируется координатором. Передается, когда происходит подключение нового узла.

Application link key – этот ключ, который работает на уровне APL. Используется он для того, чтобы два узла могли установить шифрованное общение друг с другом.

Помимо этого на каждом из уровней имеется **Frame Counter**, который не позволяет злоумышленнику провести атаку, подменив валидный пакет на свой.

V. Расшифровка сообщений с помощью SDR

Расшифровка сообщений ZigBee с использованием SDR (Software-Defined Radio) [5, 6, 7] – сложная, но выполнимая задача при соблюдении определенных условий. Потребуется соответствующее оборудование [4] (SDR-приемник, такой как RTL-SDR, HackRF, USRP, LimeSDR или координатор ZigBee, подключаемый к ПК через USB) и программное обеспечение (Wireshark, GNU Radio и иные утилиты).

Расшифровка трафика во время подключения нового устройства показана на рис. 7.

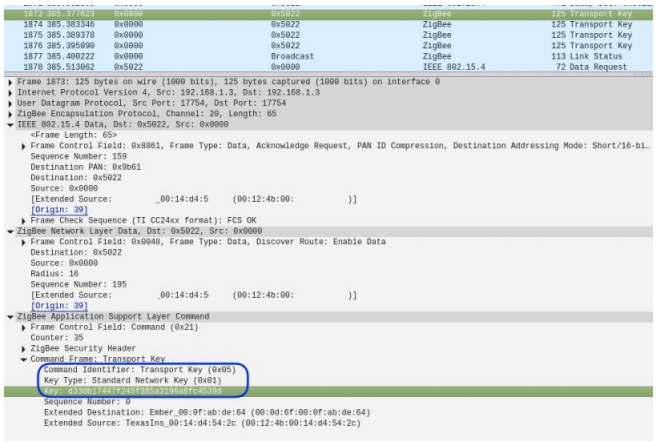

Рис. 7. Расшифровка сообщения ZigBee с ключом network key

Для приема сообщения может использоваться программа анализатор трафика Wireshark. Она прекрасно справляется с обработкой данных, полученных с устройств ZigBee. Для этого в настройках нужно прописать Pre-configured global link key.

Пример блок-схемы приемо-передающего устройства, собранного в GNU Radio представлен на рисунке 8. Частота дискретизации SDR должна быть не менее 4 МГц для корректного захвата сигнала, а усиление следует подбирать экспериментально, чтобы избежать перегрузки и высокого уровня шумов.

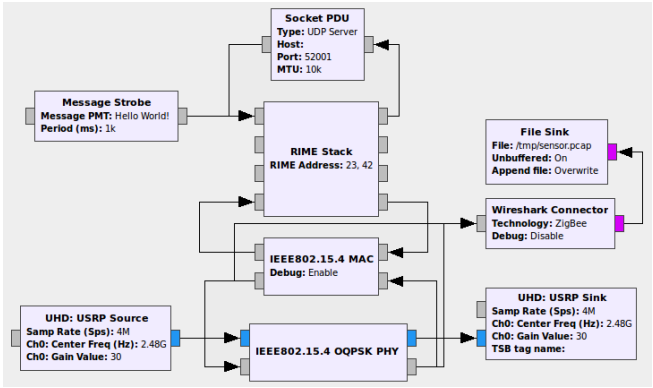

Рис. 8. Блок-схема приемо-передающего устройства ZigBee в GNU Radio

VI. Заключение

На сегодняшний день ZigBee остается одним из наиболее надежных и энергоэффективных протоколов для умного дома, обеспечивая стабильную связь между устройствами при низком энергопотреблении. Благодаря поддержке mesh-топологии, алгоритмам самовосстановления и ретрансляции, сеть ZigBee демонстрирует высокую отказоустойчивость даже при выходе из строя отдельных узлов. ZigBee оптимально подходит для сценариев, где важны низкое энергопотребление, умеренная скорость передачи данных и масштабируемость сети. При этом стоимость устройств ZigBee остается доступной, что делает его популярным решением для систем автоматизации мониторинга и контроля.

Список литературы

[1] Беспроводные сети ZigBee [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/efo/articles/281048/ (дата обращения 05.03.2025)

[2] Обзор стека протокола ZigBee [Электронный ресурс]. Режим доступа: https://www.rovdo.com/zigbee-stack?ysclid=m8rlbqw7qe213075582 (дата обращения 07.03.2025)

[3] Zigbee Security 101 (Architecture and Security Issues) https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/ (дата обращения 12.03.2025)

[4] ZigBee – GNU Radio [Электронный ресурс]. Режим доступа: https://www.wime-project.net/tutorials/zigbee/ (дата обращения 13.03.2025)

[5] Роенков Д.Н., Богданов Д.Р. Программно-определяемое радио для мониторинга состояния элементов инфраструктуры. // Автоматика, связь, информатика. 2024. № 9. С. 2-4.

[6] Роенков Д.Н., Богданов Д.Р. Программно-определяемое радио для мониторинга состояния элементов инфраструктуры. // Автоматика, связь, информатика. 2024. № 10. С. 18-21.

[7] Роенков Д.Н., Богданов Д.Р. Программно-определяемое радио для мониторинга состояния элементов инфраструктуры. // Автоматика, связь, информатика. 2024. № 11. С. 5-9.