Разработка и апробация анализатора сигналов Wi-Fi средствами программно-конфигурируемого радио

Д. Е. Мещеряков, Г. А. Фокин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

mecherikovvvv@gmail.com, grihafokin@gmail.com

***Аннотация*. Беспроводные локальные сети (WLAN) являются ключевым элементом современных систем передачи данных, гарантируя высокоскоростной доступ в интернет для многочисленных устройств. С появлением новых стандартов WLAN, включая Wi-Fi 6 и Wi-Fi 7, повышаются требования к гибкости и адаптивности сетевого оборудования. Применение технологий программно-конфигурируемого радио (SDR) совместно с библиотекой примеров из пакета WLAN Toolbox среды Matlab открывает новые возможности для решения задач проектирования систем связи. Это позволяет гибко настраивать параметры физического уровня, адаптируя их под конкретные условия работы. Разработанный в рамках данного исследования макет поддерживает программную настройку сетевых параметров посредством SDR-платформ, обеспечивая динамическое изменение частотных диапазонов, адаптацию пропускной способности и оптимизацию работы сети даже при интенсивных нагрузках и наличии помех. В работе представлены результаты экспериментальной проверки SDR-макета для передачи и приема служебных кадров стандарта 802.11, что создает основу для реализации более сложных исследовательских проектов в будущем.**

Ключевые слова WLAN, LibreSDR, SDR, Beacon, прием служебного кадра

I. Общие сведенния

Приём и передача Wi-Fi Beacon являются ключевыми процессами в работе беспроводных сетей IEEE 802.11. Точка доступа периодически отправляет Beacon-кадры, содержащие информацию о сети, такую как имя сети, поддерживаемые стандарты, ширина канала и текущие параметры синхронизации. Клиентские устройства, принимая эти кадры, могут обнаруживать доступные сети, синхронизировать время и оценивать качество соединения. Передача Beacon осуществляется с фиксированным интервалом (обычно 100–1024 TU) на полосе шириной 20 МГц. Благодаря анализу Beacon-кадров, устройства выбирают оптимальные параметры для подключения и передачи данных, что обеспечивает стабильность и эффективность работы сети. Основные функции кадра-маяка: 1) обнаружение сети: содержит информацию о сети (SSID, стандарты, каналы), позволяя устройствам находить и подключаться, 2) синхронизация времени: обеспечивает точную синхронизацию между устройствами в сети, 3) оценка качества связи: помогает клиентам выбрать лучшую точку доступа, 4) управление мощностью снижает энергопотребление и увеличивает время работы от аккумулятора, 5) управление доступом содержит данные о состоянии сети и загруженности канала [1].

На физическом уровне модели OSI Wi-Fi Beacon использует средства, которые обеспечивают передачу кадров через радиочастотный канал. Основные механизмы и технологии включают: 1) модуляция сигнала: beacon-кадры передаются с использованием методов модуляции, таких как BPSK (Binary Phase-Shift Keying) и QPSK (Quadrature Phase-Shift Keying), а также более сложных методов, таких как QAM (Quadrature Amplitude Modulation), в зависимости от стандарта Wi-Fi (например, 802.11a/b/g/n/ac). 2) Частотное разделение: DSSS (Direct Sequence Spread Spectrum), расширение спектра прямой последовательностью – это метод модуляции, который расширяет спектр передаваемых данных путем кодирования информации с использованием псевдослучайной последовательности. Этот метод позволяет улучшить устойчивость данных к шуму и межканальным интерференциям. OFDM (Orthogonal Frequency-Division Multiplexing), ортогональное мультиплексирование с частотным разделением – это метод модуляции, который разделяет передаваемые данные на несколько ортогональных непересекающихся поднесущих и передает их параллельно. Этот метод позволяет значительно больше, чем DSSS повысить скорость передачи данных и улучшить качество связи. 3) Радиочастотный спектр: Beacon-кадры передаются в стандартизированных диапазонах частот Wi-Fi, таких как 2.4 ГГц или 5 ГГц. Каналы внутри этих диапазонов имеют ширину 20, 40, 80 или 160 МГц, что зависит от используемого стандарта. 4) Кодирование сигналов: Для повышения устойчивости к шуму и помехам применяется канал кодирования, например, с использованием схем FEC (Forward Error Correction). 5) Синхронизация: точки доступа и клиентские устройства синхронизируются с использованием временных меток, передаваемых в Beacon-кадре. 6) Антенны и радиопередатчики: Используются одно- или многоантенные конфигурации (MIMO – Multiple Input Multiple Output) для увеличения пропускной способности и улучшения качества сигнала [2].

II. Описание стэнда

Приём Beacon осуществляется в среде MATLAB с использованием функций WLAN Toolbox. Для стандарта WI-FI 802.11b определены диапазоны частот 2,4 и 5 ГГц. В диапазоне 2,4 ГГц могут применяться модуляции DSSS и OFDM, в диапазоне 5 ГГц, – только OFDM. Осуществляется поиск только пакетов non-HT (non High Throughput), так как использующий их стандарт 802.11n не поддерживает названные модуляции. Поиск beacon осуществляется в указанном диапазоне и при указанной

модуляции. По ним определяются диапазон частот и набор каналов поиска, а также частота дискретизации.

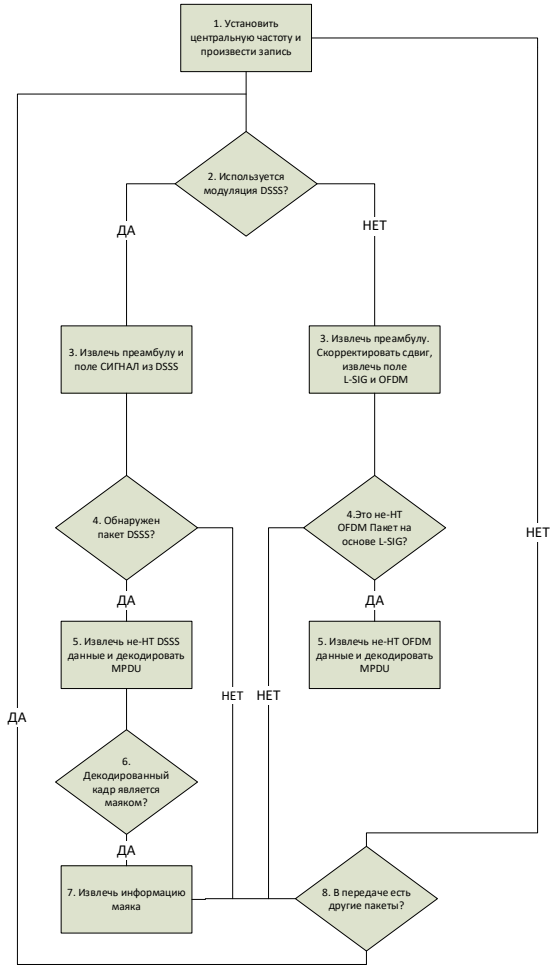

Рис. 1. Блок-схема процедуры приёма кадра-маяка

Для передачи и приёма кадра-маяка используется компьютер со средой MATLAB и платформа программно-конфигурируемого радио LibreSDR. Платформа LibreSDR представляет собой недорогое решение для реализации технологий программно-конфигурируемого радио (SDR), ориентированное на использование в академической и научной среде. Габаритные размеры платы компактны, что способствует удобству интеграции в лабораторные стенды. выполняющая функции приёмника и передатчика. Компьютер отвечает за настройку параметров передачи, включая частоту дискретизации, центральную частоту, усиление и число каналов, а также за обработку и анализ данных. Платформа LibreSDR обеспечивает преобразование цифрового сигнала в радиочастотный и обратно, позволяя передавать и принимать Beacon-кадры в WiFi диапазоне. На рис. 2 показана схема стенда, а на рис. 3 – его внешний вид.

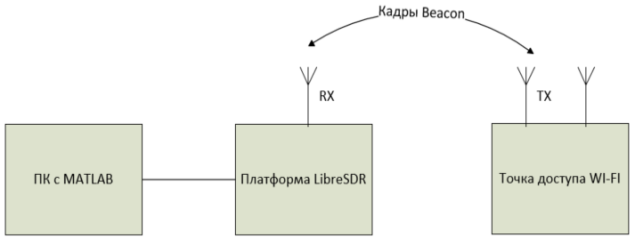

Рис. 2. Схема стенда приёмника

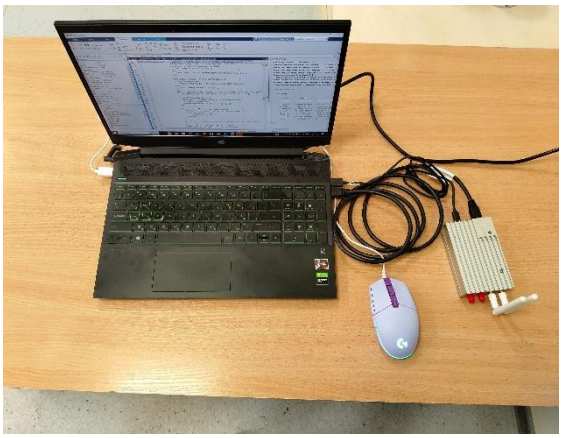

Рис. 3. Внешний вид стенда приёмника

В среде MATLAB осуществляется инициализация платформы LibreSDR, которая в свою очередь имеет достаточный функционал для работы с системами беспроводной связи и при этом имеет более низкую стоимость, чем другие устройства SDR [3]. Для работы с платой задаются следующие параметры: IP-адрес устройства, частота дискретизации, режим ручного управления усилением и его значение, количество каналов приёма и число отсчётов в одном кадре. Для каждого канала устанавливается центральная частота приёмника.

III. Анализ программы

A. Программная реализация приёма и анализа Beacon-кадров

Для реализации процесса приёма и анализа Beacon-кадров в среде MATLAB была использована программа, которая содержит библиотеку WLAN Toolbox и платформу программно-конфигурируемого радио (SDR). Программа позволяет гибко настраивать параметры приёма и передачи, а также анализировать данные, извлечённые из Beacon-кадров. Ниже приведено подробное описание работы программы.

B. Инициализация и настройка параметров

Программа начинается с инициализации параметров, которые определяют диапазон частот (2.4 ГГц или 5 ГГц), тип модуляции (OFDM или DSSS), а также другие параметры, такие как частота дискретизации, усиление и количество каналов. Эти параметры задаются в зависимости от выбранной конфигурации (например, «OFDM, band 5» для работы в диапазоне 5 ГГц с использованием OFDM).

Если программа работает с SDR, то настраиваются параметры для захвата сигнала, такие как центральная частота, усиление и время захвата. В противном случае данные загружаются из файла.

C. Захват и обработка сигналов

Программа поддерживает два режима работы: с использованием SDR и с загрузкой данных из файла. Если используется SDR, программа настраивает платформу для захвата сигнала на указанной частоте. Захваченные данные затем обрабатываются для поиска Beacon-кадров.

D. *Декодирование Beacon кадров*

После захвата данных программа выполняет декодирование Beacon-кадров. В зависимости от типа сигнала (OFDM или DSSS) используются разные функции для обработки:

- Для OFDM: recoverNonHTOFDM(capturedData, rxsim)
- Для DSSS: recoverDSSS(capturedData)

Эти функции выполняют синхронизацию, демодуляцию и извлечение данных из Beacon-кадров. Если кадр успешно декодирован, программа извлекает информацию о точке доступа, такую как SSID, BSSID, SNR, канал, ширина канала и т. д.

E. *Анализ и отображение информации*

Программа анализирует извлечённые данные и сохраняет их в структуру APs, которая содержит информацию о каждой обнаруженной точке доступа. После завершения сканирования всех каналов, программа преобразует структуру в таблицу и отображает результаты.

F. *Визуализация данных*

Программа поддерживает возможность визуализации спектра и спектрограммы захваченного сигнала, что позволяет анализировать качество сигнала и наличие помех.

G. *Результаты работы программы*

Программа успешно обнаруживает Beacon-кадры в указанных диапазонах частот и извлекает информацию о точках доступа. На рис. 4 и рис. 5 показаны примеры извлечённых данных для диапазонов 2.4 ГГц и 5 ГГц соответственно. Программа также подтверждает успешный приём Beacon-кадров с помощью сторонних инструментов, таких как анализатор Wi-Fi на Android (рис. 6 и рис. 7).

H. *Используемые функции MATLAB*

Программа активно использует функции из библиотеки WLAN Toolbox, приведенные в табл. 1.

ТАБЛИЦА I.

Функция	Описание
wlanChannelFrequency()	Расчет центральной частоты канала Wi-Fi по номеру и диапазону (2.4/5 ГГц)
wlanMPDUDecode()	Декодирование MAC Protocol Data Unit (MPDU) из битового потока
wlanMACFrameConfig	Конфигурация параметров MAC-фрейма (тип, подтип, адреса и т.д.)
recoverNonHTOFDM()	Синхронизация/демодуляция OFDM-пакетов
recoverDSSS()	Декодирование DSSS-пакетов

IV. Вывод о работе программы

Из принятого кадра Beacon извлекаются следующие данные: идентификатор сети SSID (Service Set Identifier), идентификатор точки доступа BSSID (Basic Service Set Identifier), соотношение сигнал/шум SNR, основной рабочий канал (Primary Operating Channel), ширина канала (Channel Width), используемая полоса частот (Band), поддерживаемый точкой доступа режим работы(Mode), конфигурация MAC-кадра и метка времени.

Приём кадра-маяка в диапазоне 2,4 ГГц выполняется на всех каналах диапазона. На рис. 4 показаны извлечённые из кадра данные о точке доступа.

SSID	BSSID	Vendor
"CAT1"	"300505A81B14"	"Intel Corporate"
"LIS"	"CC9DA2C2B9A0"	"Eltex Enterprise Ltd."
"Work ÐÐÐ¢Ð ÐÐ by OBIT"	"7EACB9646708"	"Unknown"
"LIS"	"CC9DA2C2B9A0"	"Eltex Enterprise Ltd."
"photost"	"50FF201E9A98"	"Keenetic Limited"
"photost"	"50FF20786769"	"Keenetic Limited"
"elena"	"0492263BE738"	"ASUSTek COMPUTER INC."
"LIS"	"CC9DA2C24B00"	"Eltex Enterprise Ltd."
"elena"	"0492263BE738"	"ASUSTek COMPUTER INC."

Рис. 4. Информация кадров-Beacon диапазона 2,4 ГГц

Приём кадра-маяка диапазона 5 ГГц осуществляется на протяжении всего диапазона рис. 5. На рисунке заметно, что beacon принят несколько раз это связано с тем, что у каждой точки доступа может быть своя конфигурация данного кадра и поэтому при сканировании диапазона частот стоит учитывать, что временной интервал и длительность сообщения может разительно отличаться.

SSID	BSSID	Vendor	SNR (dB)
"LIS"	"ECB1E020A8D9"	"Eltex Enterprise LTD"	26.376
"LIS"	"ECB1E020A8D9"	"Eltex Enterprise LTD"	25.701
"5GHz_A-rial_wpa2"	"C64BD1C10521"	"Unknown"	10.574

Рис. 5. Информация кадров-Beacon диапазона 5 ГГц

Для подтверждения работы программы, а том, что точки доступа существуют в радиоэфире, можно использовать внешнее приложение. В данном случаи используется Android приложение «Wifi Analyzer» от компании olgor.com, кроме этого, точка доступа будет видна в списке доступных сетей Wi-Fi на мобильном телефоне в диапазоне 2.4 ГГц на рис. 6 и в 5 ГГц на рис. 7.

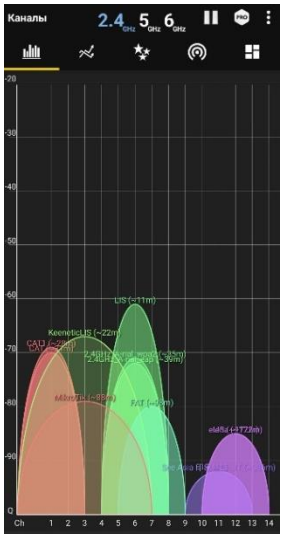

Рис. 6. Beacon в диапазоне 2,4 ГГц на спектре, зафиксированном анализатором Wi-Fi

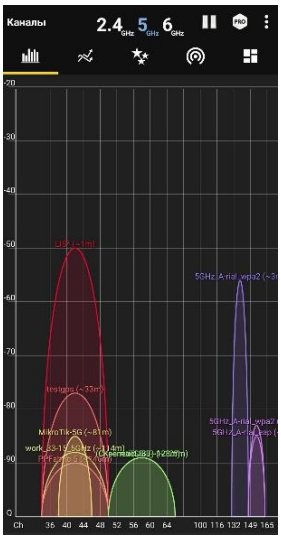

Рис. 7. Beacon в диапазоне 5 ГГц на спектре, зафиксированном анализатором Wi-Fi

V. Заключение

Программа демонстрирует эффективность использования LibreSDR в MATLAB для анализа Wi-Fi сетей. Она позволяет гибко настраивать параметры приёма и передачи, а также извлекать и анализировать информацию из Beacon-кадров. Программа может быть использована для исследований в области беспроводных сетей, а также для тестирования и оптимизации сетевого оборудования.

Список литературы

[1] WLAN Beacon Receiver Using Software-Defined Radio. MathWorks. [Электронный ресурс]. URL: https://www.mathworks.com/help/wlan/ug/ofdm-beacon-receiver-using-software-defined-radio.html (дата обращения 24.02.2025).

[2] 802.11 OFDM Beacon Frame Generation. MathWorks. [Электронный ресурс]. URL: https://www.mathworks.com/help/wlan/ug/802-11-ofdm-beacon-frame-generation.html (дата обращения 24.02.2025).

[3] Фокин Г.А. Экспериментальная апробация SDR платформы LibreSDR / Г.А. Фокин, К.Е. Рютин // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио. 2024. № 1 (79). С. 174-177.