

УДК 621.396.969

Разработка и апробация анализатора сигналов стандарта LTE средствами программно-конфигурируемого радио

Цап В. В. ✉, Фокин Г. А.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Санкт-Петербург, 193232, Российская Федерация

Цель работы — программная реализация и экспериментальная апробация анализатора сигналов стандарта LTE средствами программно-конфигурируемого радио для позиционирования с точностью до принадлежности к соте. **Результат:** разработано программное обеспечение анализатора сигналов стандарта LTE на языке MATLAB, реализующее прием, обработку и извлечение необходимых блоков системной информации, которая передается базовыми станциями стандарта LTE по широкополосным каналам; сконфигурирован интерфейс для работы с платой USRP B210; в ходе экспериментальной апробации выполнен прием и обработка блоков системной информации из радиоз эфира с извлечением идентификаторов операторских базовых станций и последующим обращением в открытую базу данных OpenCellID для получения глобальных координат. **Новизна:** из обзора открытых отечественных источников следует, что настоящее исследование является первой работой, в которой детально описан порядок анализа широкополосных сигналов стандарта LTE для определения местоположения пользовательского устройства, не являющегося абонентом сети. **Практическая значимость:** программно реализованный и экспериментально апробированный анализатор сигналов стандарта LTE позволяет определять местоположение пользователя, не являющегося абонентом какой-либо сети, с точностью до принадлежности к ближайшей соте в условиях недоступности глобальных навигационных спутниковых систем.

Ключевые слова: стандарт LTE, программно-конфигурируемое радио, среда разработки MATLAB, блок системной информации, позиционирование

Источник финансирования: статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Введение

На сегодняшний день сети стандарта LTE (аббр. от англ. Long-Term Evolution — букв. «долгосрочное развитие») являются доминирующими системами радиосвязи по радиопокрытию и обслуживанию; в частности, за последние восемь лет радиопокрытие сетями LTE в странах СНГ выросло на 49,1 %, достигнув 92 % [1]. В связи с санкционными ограничениями по ввозу телекоммуникационного оборудования на территорию России [2] ожидать стремительного развертывания сетей пятого поколения 5G стандарта NR (аббр. от англ. New Radio) не приходится, поэтому в ближайшее десятилетие сети стандарта LTE останутся основными сетями сотовой подвижной радиосвязи.

Одним из возможных подходов к программно-аппаратной реализации систем радиосвязи и устройств приема и передачи сигналов является программно-конфигурируемое радио (SDR, аббр. от англ. Software Defined Radio) [3–10]. Аппаратные модули SDR реализуются на архитектуре с нулевой

Библиографическая ссылка на статью:

Цап В. В., Фокин Г. А. Разработка и апробация анализатора сигналов стандарта LTE средствами программно-конфигурируемого радио // Вестник СПбГУТ. 2024. Т. 2. № 2. С. 4. EDN: LPOWHF

Reference for citation:

Tsap V., Fokin G. Development and Testing of LTE Signal Analyzer Using Software-Defined Radio // Herald of SPbSUT. 2024. Vol. 2. Iss. 2. P. 4. EDN: LPOWHF

промежуточной частотой [4–7], что снижает сложность оборудования, производящего обработку радиосигнала, за счет уменьшения частоты дискретизации и, следовательно, снижения требований к аналого-цифровому и цифро-аналоговому преобразователям. После преобразования сигнала в цифровую форму его можно обрабатывать методами и средствами цифровой обработки сигналов, реализованными на языках программирования высокого уровня, что упрощает и тем самым ускоряет разработку прототипов систем радиосвязи [8–10].

Помимо систем радиосвязи существующие программно-аппаратные средства SDR позволяют разрабатывать и системы радиотехнического позиционирования [11–13].

В настоящее время в России осуществляется разработка радиотехнических систем навигации, реализующих услуги позиционирования независимо от глобальных навигационных спутниковых систем (ГНСС) [14]. В условиях отсутствия сигналов ГНСС для определения местоположения пользовательских устройств (UE, *аббр. от англ.* User Equipment) могут использоваться сигналы базовых станций (БС) сетей связи стандарта LTE. Анализируя широкополосные сигналы стандарта LTE средствами SDR, можно извлекать координаты ближайших БС всех работающих в данном районе операторов, не будучи абонентом какой-либо отдельной сети. В связи с широко развитой инфраструктурой и подавляющим радиопокрытием сетей связи LTE разработка и экспериментальная апробация анализатора сигналов стандарта LTE средствами SDR для решения задач позиционирования UE по сигналам нескольких БС представляется достаточно актуальной и востребованной.

Материал настоящей работы организован далее следующим образом: сначала выполняется обзор существующих технических решений по анализу сигналов стандарта LTE; затем приводится обоснование выбора программной среды разработки анализатора сигналов стандарта LTE; после формализации процедур обработки рассматриваются особенности программной реализации и экспериментальной апробации анализатора широкополосных сигналов стандарта LTE применительно к задаче определения местоположения ближайшей БС.

Обзор существующих технических решений по анализу сигналов стандарта LTE

Выполним обзор существующих комплексов радиоконтроля, реализующих анализ сигналов стандарта LTE, основываясь на анализе открытых отечественных источников.

1. Портативный комплекс радиоконтроля «Омега-М5» [15] предназначен для идентификации и фиксации соединений между базовой и мобильной станциями, работающими в сетях стандартов GSM (*аббр. от англ.* Global System for Mobile Communications — глобальная система мобильной связи), UMTS (*аббр. от англ.* Universal Mobile Telecommunications System — универсальная система мобильной связи) и LTE. Применительно к сетям LTE комплекс «Омега-М5» может осуществлять сканирование диапазонов частот 832–862, 880–915, 1710–1785, 1900–1920, 2300–2400, 2500–2570, 2570–2620 МГц, которые соответствуют диапазонам В3, В7, В8, В20, В33, В38, В40 в направлении UL (*аббр. от англ.* Uplink — восходящая линия связи) с частотным дуплексом (FDD, *аббр. от англ.* Frequency Division Duplex), или в направлениях UL и DL (*аббр. от англ.* Downlink — нисходящая линия связи) с временным дуплексом (TDD, *аббр. от англ.* Time Division Duplex) [16]. Также комплекс способен имитировать работу БС для перехвата трафика абонентов.

2. Комплекс радиоконтроля «Призрак» [17] позволяет распознавать и записывать фрагменты радиозэфира в диапазоне частот 0,01–12 000 МГц при анализе сигналов стандартов GSM, EDGE (*аббр. от англ.* Enhanced Data Rates for GSM Evolution — повышенная скорость передачи данных для стандарта GSM), UMTS, HSDPA (*аббр. от англ.* High-Speed Downlink Packet Access — высокоскоростной пакетный доступ в нисходящей линии связи), LTE-A (*аббр. от англ.* LTE Advanced — улучшение стандарта LTE), IS-95 (*аббр. от англ.* Interim Standard 95 — временный стандарт 1995 г.). Комплекс имеет возможность отправки записанных фрагментов радиосигнала по протоколу WAV (*аббр. от англ.* Waveform Audio File Format — формат файла для хранения цифрового сигнала) на автоматизированное рабочее место (АРМ) оператора. В соответствии с распознанными параметрами сигнала (рабочей частотой, видом модуляции, символьной скоростью и др.) комплекс определяет стандарт связи из заранее подготовленной справочной информации.

3. Анализатор спектра «FSH4» [18] создан для проведения контрольно-измерительных работ при обслуживании БС. Кроме того, применение его вместе с измерительным программным комплексом «FSH-K50E» в диапазоне частот 15–4000 МГц позволяет производить измерение параметров сигналов стандарта LTE, в числе которых коэффициент вектора ошибок каждого в отдельности канала управления, отображение на сигнальном созвездии принятых символов, определение физических идентификаторов находящихся поблизости БС.

Несмотря на разные сферы применения описанных комплексов, они имеют схожую функциональность, заключающуюся в обнаружении и записи сигналов LTE из радиоэфира. Также рассмотренные комплексы имеют разделение на аппаратный радиоприемник и программный модуль цифровой обработки сигналов. В отличие от анализатора спектра «FSH4», который используется в сетях связи общего пользования, подробной информации о комплексах «Омега-М5» и «Призрак» в открытом доступе недостаточно. Однако основные особенности работы этих комплексов, отмеченные выше, позволяют сформулировать обобщенные задачи, которые должен решать анализатор сигналов стандарта LTE: 1) запись и последующая отправка фрагментов радиоэфира на АРМ; 2) нахождение в записи радиоэфира сигналов, излучаемых БС стандарта LTE; 3) определение сетевых идентификаторов БС стандарта LTE; 4) запрос в базу данных (БД) на извлечение местоположения БС стандарта LTE.

Обоснование выбора программной среды разработки анализатора сигналов стандарта LTE

На основе сформулированных выше обобщенных задач выполним далее обоснование выбора программной среды разработки анализатора сигналов стандарта LTE применительно к задаче определения местоположения ближайшей БС. Исходными данными для выбора являются следующие факторы: во-первых, в качестве БД местоположений БС будем использовать БД открытого проекта OpenCellID [19]; во-вторых, разработку и экспериментальную апробацию сигналов будем проводить для имеющейся в наличии платы SDR USRP B210 [20] компании Ettus Research.

Компания Ettus Research предоставляет согласно свободной лицензии GPL (*аббр. от англ. General Public License*) драйвер UHD (*аббр. от англ. USRP Hardware Driver*) для работы с платами USRP [21] на языках программирования C, Python, а также интерфейсы для популярных программных сред разработки LabVIEW [22], MATLAB [23] и GNU Radio [24]. Рассмотрим особенности перечисленных программных сред.

Программы в средах разработки GNU Radio и LabVIEW создаются посредством описания их графических блок-схем, которые могут состоять как из готовых блоков, распространяемых вместе со средой, так и определенных пользователем и написанных на языках программирования Python и C++ для GNU Radio, а также MATLAB, C и C# для LabVIEW. В среде MATLAB, в отличие от остальных сред разработки, программа анализа сигналов может быть полностью создана на текстовом языке программирования.

Среда LabVIEW предоставляет средства преобразования созданных блок-схем в отдельные исполняемые файлы, не зависящие от среды и запускаемые вне ее, только с условием установленной на компьютере библиотеки «LabVIEW Runtime Engine» [25]. В среде GNU Radio после описания блок-схемы программы генерируется скрипт на языке программирования Python, а значит созданная программа далее не зависит от используемой при ее написании среды. В MATLAB существует возможность генерации исходного кода на других языках программирования с помощью пакетов «MATLAB Coder» [26] и «HDL Coder» [27].

Рассматривая остальные возможности, кроме автоматической генерации кода, отметим, что при разработке в средах LabVIEW и GNU Radio объем работ увеличивается за счет последующего описания взаимодействия блоков на целевом языке, в случае же среды MATLAB этот этап происходит одновременно с написанием программы, и далее остается только решить задачу переноса алгоритма на синтаксис другого языка программирования.

Рассмотрим языки программирования, использующиеся в этих средах. Все они являются кроссплатформенными: C и C++ — за счет использования компиляторов, написанных для различных аппаратных платформ; C#, Python и MATLAB — за счет использования сред выполнения, написанных для разных операционных систем. Их можно разделить на две группы по виду типизации: 1) статическая: C, C++, C#; 2) динамическая: Python, MATLAB.

Написание и отладка исходного кода на статически типизированных языках требует больше времени, код становится более сложным и объемным. Динамически типизированные языки обладают менее объемным синтаксисом, увеличивают скорость разработки алгоритмов, избавляют пользователя от обязанности вывода типов данных. Но написанные на таких языках программы исполняются медленнее из-за необходимости производить трансляцию кода во время выполнения; помимо этого, также увеличивается вероятность ошибок из-за неправильного вывода типов переменных. Несмотря на описанные недостатки языков с динамической типизацией, выберем их из-за преимуществ в скорости разработки.

Python и MATLAB являются интерпретируемыми языками, поддерживающими множество парадигм программирования. MATLAB имеет объемную стандартную библиотеку, включающую большинство математических функций и операторов, множество функций графического вывода и создания документации, а также множество дополнительных пакетов, призванных решать узкоспециализированные задачи. В отличие от MATLAB, для Python существуют разные интерпретаторы, функциональность языка обеспечивается наличием множества отдельно поставляемых библиотек. Существенное различие между этими языками заключается в том, что MATLAB является проприетарным языком с собственной средой разработки, а Python — свободно распространяемым языком.

Реализация процедур обработки сигналов из примитивных функций как на языке MATLAB, так и Python, позволяет в дальнейшем перейти к их реализации на языке HDL (*аббр. от англ.* Hardware Description Language — язык описания аппаратуры) программируемых логических интегральных схем (ПЛИС). Аргументом в пользу выбора среды разработки MATLAB является наличие встроенных пакетов расширения, в том числе пакета расширения LTE Toolbox: сравнивая самостоятельно реализованные из примитивных функций программные модули со встроенными высокоуровневыми функциями пакета расширения можно верифицировать корректность их реализации.

Формализация процедур обработки широкополосных сигналов стандарта LTE

Для извлечения местоположения БС из БД OpenCellID при отправке запроса следует сообщить следующие идентификаторы, принадлежащие БС: мобильный код страны (MCC, *аббр. от англ.* Mobile Country Code), код мобильной сети (MNC, *аббр. от англ.* Mobile Network Code), код региона местоположения (LAC, *аббр. от англ.* Location Area Code), идентификатор соты (CID, *аббр. от англ.* Cell Identity) [19]. Эти идентификаторы передаются БС в поле cellAccessRelatedInfo блока системной информации SIB1 (*аббр. от англ.* System Information Block Type 1) (таблица 1), который передается в сообщении BCCH-DL-SCH-Message [28] в логическом канале BCCH (*аббр. от англ.* Broadcast Control Channel — широкополосный канал управления) через транспортный канал DL-SCH (*аббр. от англ.* Downlink Shared Channel — транспортный канал с разделением пользователей). Расписание передачи SIB1 определяется системным номером кадра (SFN, *аббр. от англ.* System Frame Number) [28], который передается в блоке MIB (*аббр. от англ.* Master Information Block — блок системной информации) (таблица 2), являющегося частью сообщения BCCH-BCH-Message [28], в канале BCCH через транспортный канал BCH (*аббр. от англ.* Broadcast Channel).

Формализуем далее процедуры формирования, передачи, приема и обработки широкополосных сигналов в транспортных и физических каналах. Данная формализация необходима для последующей программной реализации в среде MATLAB из примитивных функций. После формирования блоков MIB, SIB1 они передаются в транспортные каналы BCH и DL-SCH. Первой процедурой является вычисление и прикрепление CRC-суммы (*аббр. от англ.* Cyclic Redundancy Check — циклический избыточный код). Для канала BCH используется полином генератора g_{CRC16} [29], после вычисления CRC-суммы она дополнительно скремблируется в зависимости от количества используемых БС антенных портов [29]: для одного антенного порта скремблирование отсутствует, для двух портов используется единичная последовательность, для четырех портов — последовательность чередующихся 0 и 1. В канале DL-SCH используется генератор с полиномом g_{CRC24A} [29]. Значения указанных полиномов приводятся ниже [29]:

- 1) $g_{CRC16} = 10001000000100001$;
- 2) $g_{CRC24A} = 1100001100100110011111011$.

Таблица 1. Структура поля cellAccessRelatedInfo сообщения SIB1 [28]

Поле	Описание
plmn-IdentityList	Набор идентификаторов сетей, которым принадлежит БС
trackingAreaCode	Код зоны слежения
cellIdentity	Идентификатор БС
cellBarred	Флаг доступности БС
intraFreqReselection	Флаг доступности реселекции в другие соты, работающие с такой же частотой
csg-Indication	Флаг закрытой абонентской группы
csg-Identity	Идентификатор закрытой абонентской группы

Таблица 2. Структура сообщения MIB [28]

Поле	Описание
dl-Bandwidth	Ширина канала
phich-Config	Конфигурация физического канала PHICH (аббр. от англ. Physical Hybrid ARQ Indicator Channel — физический канал для передачи HARQ-ACK)
System Frame Number	Системный номер кадра
spare	Заполняющие биты

Поскольку в канале DL-SCH передается информация, включающая данные каналов трафика, объем обрабатываемого транспортного блока может достигать больших размеров. Для идентичности дальнейшей обработки вне зависимости от размера транспортного блока его сегментируют на фрагменты длиной 6144 бит [29]. Поскольку максимальный размер блока системной информации ограничен величиной 2216 бит, то процессом сегментирования можно пренебречь. Причиной такого ограничения служит максимальный размер транспортного блока (TBS, аббр. от англ. Transport Block Size), который может быть передан в блоках DCI (аббр. от англ. Downlink Control Information — управляющая информация для нисходящей линии связи), которые будут рассмотрены далее.

Следующим этапом обработки является канальное кодирование. Для канала BCH применяется сверточный кодер, для канала DL-SCH — турбокодер [29]; скорости обоих кодеров равны 1/3.

Перед началом обработки сдвиговый регистр сверточного кодера инициализируется значениями последних шести бит кодового блока. Размер регистра составляет 7 бит. Структурная схема кодера представлена на рисунке 1. Значения полиномов сумматоров кодера:

- 1) $G_0 = 1011011$;
- 2) $G_1 = 1111001$;
- 3) $G_2 = 1110101$.

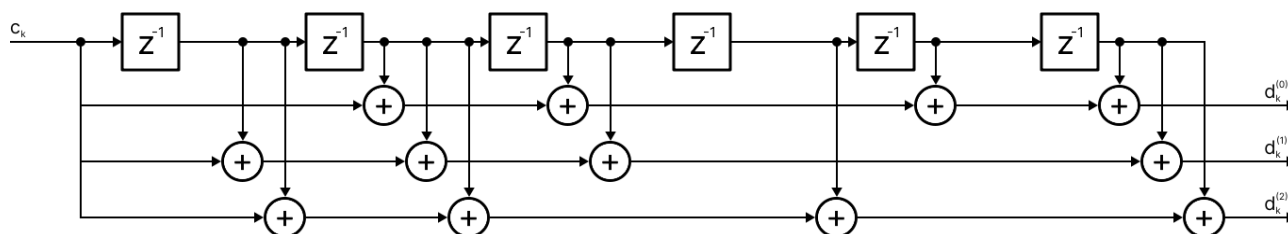


Рис. 1. Структурная схема сверточного кодера [29]

Турбокодер (рисунок 2) состоит из двух рекурсивных сверточных кодеров, включенных параллельно, перед вторым кодером используется внутренний перемежитель. Код генерируется согласно следующим полиномам:

- 1) прямой ветви: $g_1 = 1101$;
- 2) обратной ветви: $g_0 = 1011$.

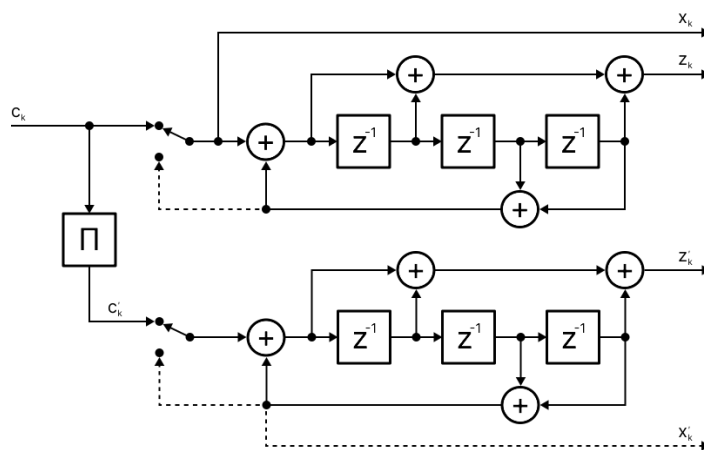


Рис. 2. Структурная схема турбокодера [29]

Сдвиговой регистр в начальный и конечный моменты времени заполнен нулевой последовательностью. Это сделано для обеспечения работоспособности декодера, поскольку для работы ему необходимо знать начальное и конечное состояние кодера. Чтобы обеспечить обнуление регистров после окончания кодирования, на их входы подаются последние три выходных бита.

Внутренний перемежитель перед вторым элементарным кодером вычисляет номер выходного бита $\Pi(i)$ по номеру входного бита i согласно выражению:

$$\Pi(i) = (f_1 i + f_2 i^2) \bmod K, \quad (1)$$

где параметры f_1 и f_2 зависят от длины блока информации K и определяются в соответствии с [29].

Завершающий этап обработки блоков информации в транспортных каналах производит модуль задания скорости. Он состоит из блоковых перемежителей, блока преобразования параллельного кода в последовательный и циклического буфера.

Блоковыми перемежителями обрабатываются все три выходные последовательности кодера вне зависимости от его типа. Перемежитель представляется в виде матрицы с 32 столбцами и изменяемым количеством строк $R_{subblock}^{TC}$ в зависимости от длины входной последовательности. Входная последовательность записывается в перемежитель по строкам и дополняется пустыми битами в случае, если ее длина не совпадает с количеством элементов матрицы. Далее перемежитель выполняет перестановку столбцов по правилам сортировки, определенным в [29] для турбокодера и сверточного кодера. Чтение данных на выходе перемежителя осуществляется по столбцам.

После блоковых перемежителей данные поступают на вход блока преобразования параллельного кода в последовательный, который в случае использования сверточного кодера отправляет далее полученные битовые потоки без их изменения, а в случае использования турбокодера дополнительно прореживает второй поток элементами третьего.

Циклический буфер задает скорость кодового слова, выкалывая пустые биты, которые появились в блоковых перемежителях, и повторяя получившийся блок данных, пока длина кодового слова не достигнет требуемого размера. В случае использования турбокодера номер первого символа k_0 , с которого начинается формирование кодового слова, вычисляется по формуле [29]:

$$k_0 = R_{subblock}^{TC} \left(2 \left\lceil \frac{N_{cb}}{8R_{subblock}^{TC}} \right\rceil rv_{idx} + 2 \right), \quad (2)$$

где N_{cb} — размер буфера, выделенного для хранения сегмента блока информации; rv_{idx} — индекс номера повтора передачи сообщения.

Сформированные в транспортных каналах кодовые слова передаются в физические каналы. Канал BCH передается в канал PBCH (аббр. от англ. Physical Broadcast Channel — физический широковещательный канал), канал DL-SCH — в канал PDSCH (аббр. от англ. Physical Downlink Shared Channel — физический канал с разделением пользователей) [29].

размещаются в первых четырех символах 1-го слота каждого из четырех последовательных кадров в шести центральных ресурсных блоках (РБ), игнорируя поднесущие, которые могут быть отданы опорным сигналам CRS (*аббр. от англ. Cell-Specific Reference Signal* — опорные сигналы, уникальные для соты) при использовании четырех антенных портов [30].

Последней процедурой, выполняемой в физических каналах перед переносом сигнала на радиочастоту, является генерация OFDM-символов (*аббр. от англ. Orthogonal Frequency-Division Multiplexing* — мультиплексирование с ортогональным частотным разделением каналов). Для расстояния между поднесущими $\Delta f = 15$ кГц длина символа составляет 2048 временных интервалов T_s , длина нормального циклического префикса — $160 T_s$ для 1-го символа слота и $144 T_s$ для остальных символов, расширенного — $512 T_s$ для всех символов слота [30]. Генерация OFDM-символов осуществляется для всех поднесущих, кроме центральной ($k \neq 0$) по формуле:

$$s_l^{(p)}(t) = \sum_{k=-\lfloor N_{RB}^{DL} N_{SC}^{RB} / 2 \rfloor}^{\lfloor N_{RB}^{DL} N_{SC}^{RB} / 2 \rfloor} a_{k,l}^{(p)} e^{j2\pi k \Delta f (t - N_{CP,l} T_s)}, \quad (4)$$

где p — номер антенного порта; l — номер символа в слоте; k — номер поднесущей; N_{RB}^{DL} — ширина канала, выраженная в количестве используемых РБ; N_{SC}^{RB} — количество поднесущих в одном РБ.

Для возможности подключения и работы пользователей в радиосети БС передает дополнительные сообщения и сигналы: опорные сигналы PSS (*аббр. от англ. Primary Synchronization Signal* — первичный сигнал синхронизации), SSS (*аббр. от англ. Secondary Synchronization Signal* — вторичный сигнал синхронизации), а также специальные блоки данных управляющей информации CFI (*аббр. от англ. Control Format Indicator* — индикатор формата управляющей информации), HI (*аббр. от англ. Hybrid Automatic Repeat Request Indicator* — индикатор автоматического запроса повтора передачи), DCI, CRS. Рассмотрим далее особенности их формирования, передачи, приема и обработки.

DCI — блок управляющей информации, в котором передаются параметры, требуемые для обработки каналов PDSCH и DL-SCH. Поскольку из всех типов информации, которые могут передаваться по каналам данных, интерес представляет только системная, передаваемая с SI-RNTI (*аббр. от англ. System Information Radio Network Temporary Identifier* — идентификатор радиосоединения для передачи системной информации), то достаточно рассмотреть форматы 1A и 1C (таблицы 3 и 4).

Таблица 3. Структура блока DCI формата 1A для SI-RNTI [29]

Поле	Размер поля, бит
Carrier Indicator (Индикатор несущей)	0
Differentiation Flag (Флаг различения форматов)	1
Localized / Distributed VRB Assignment Flag (Флаг типа распределения РБ)	1
Resource Block Assignment (Размещение РБ)	$\left\lceil \log_2 \left(\frac{N_{RB}^{DL}}{2} (N_{RB}^{DL} + 1) \right) \right\rceil$
Modulation and Coding Scheme (Индекс модуляционных и кодирующих схем)	5
HARQ Process Number (Номер передачи)	3 (FDD) / 4 (TDD)
New Data Indicator (Индикатор новой передачи)	1
Redundancy Version (Версия передачи)	2
TPC Command for PUSCH (Команда управления мощностью)	2
Downlink Assignment Index (Индекс передачи)	0 (FDD) / 2 (TDD)

Размер поля «Carrier Indicator» равен 0 бит согласно [32]. Если поле «Differentiation Flag» равно 0, то данный блок имеет формат 0, иначе — 1A. Поле «Localized / Distributed VRB Assignment Flag» является индикатором используемого типа размещения виртуальных РБ (VRB, *аббр. от англ. Virtual Resource Block*): 0 — локализованное, 1 — распределенное. При использовании распределенного размещения VRB и ширине канала $N_{RB}^{DL} \geq 50$ в старшем бите поля «Resource Block Assignment» указывается используемое значение разнесения РБ N_{gap} : 0 — $N_{gap} = N_{gap,1}$, 1 — $N_{gap} = N_{gap,2}$. В поле

«Modulation and Coding Scheme» указывается индекс MCS, который используется для определения порядка модуляционной схемы и индекса TBS [32]. Размер поля «HARQ Process Number» зависит от используемого типа дуплекса: 3 бит для FDD, 4 бит — TDD. Старший бит поля «TPC Command for PUCCH» зарезервирован, а в младшем бите указывается количество физических РБ (PRB, *аббр. от англ.* Physical Resource Block) N_{PRB} для определения размера информационного блока TBS, для которого формируется этот DCI, по [32]: 0 — $N_{PRB} = 2$, 1 — $N_{PRB} = 3$. Размер поля «Downlink Assignment Index» зависит от используемого типа дуплекса [29]: 0 бит при FDD, 2 бит при TDD.

Если размер сформированного блока DCI формата 1A равен одному из размеров, указанных в [29], то он дополняется одним заполняющим битом. Если размер с учетом дополнительного бита меньше размера блока DCI формата 0, который определяется по [29], то блок дополняется заполняющими битами, пока размеры блоков DCI обоих форматов не совпадут [29].

Таблица 4. Структура блока DCI формата 1C для SI-RNTI [29]

Поле	Размер поля, бит
N_{gap} (Номер набора величин разнесения РБ)	1
Localized / Distributed VRB Assignment Flag (Флаг типа распределения РБ)	$\left\lceil \log_2 \left(\left\lfloor \frac{N_{VRB, gap1}^{DL}}{N_{RB}^{step}} \right\rfloor \times \left(\left\lfloor \frac{N_{VRB, gap1}^{DL}}{N_{RB}^{step}} \right\rfloor + 1 \right) / 2 \right) \right\rceil$
Modulation and Coding Scheme (Индекс модуляционных и кодирующих схем)	5

В DCI формата 1C передается информация только о распределенном размещении VRB. Поле « N_{gap} » при ширине канала $N_{RB}^{DL} < 50$ отсутствует. Размер поля «Localized / Distributed VRB Assignment Flag» зависит от шага между РБ N_{RB}^{step} , который равен 4 при $N_{RB}^{DL} \geq 50$ и 2 в остальных случаях [32]. По индексу MCS аналогично DCI формата 1A находится индекс TBS, но TBS определяется по [32].

В обоих форматах DCI используется тип размещения ресурсов 2 [32], в котором набор виртуальных РБ VRB передается с помощью индикатора ресурсов (RIV, *аббр. от англ.* Resource Indication Value), который формируется из значений номера первого VRB RB_{start} и количества выделяемых последовательных VRB L_{CRBs} :

- 1) при $(L_{CRBs} - 1) \leq \left\lfloor \frac{N_{RB}^{DL}}{2} \right\rfloor$: $RIV = N_{RB}^{DL} (L_{CRBs} - 1) + RB_{start}$;
- 2) при $(L_{CRBs} - 1) > \left\lfloor \frac{N_{RB}^{DL}}{2} \right\rfloor$: $RIV = N_{RB}^{DL} (N_{RB}^{DL} - L_{CRBs} + 1) + (N_{RB}^{DL} - 1 - RB_{start})$.

Для DCI формата 1C параметры L_{CRBs} , RB_{start} и N_{RB}^{DL} дополнительно делятся на N_{RB}^{step} .

После формирования блока информации к нему прикрепляется сумма CRC-16, которая дополнительно скремблируется значением выбранного RNTI. При кодировании используется сверточный код [29]. Поскольку DCI форматов 1A и 1C размещаются в общем пространстве поиска [32], то для них используется 4-й или 8-й уровень агрегации [32], другими словами, размер их кодового слова составляет 4 или 8 CCE (*аббр. от англ.* Control Channel Element — элемент канала управления), что означает 288 или 576 бит [30]. Согласно [29] DCI передаются по физическому каналу PDCCH (*аббр. от англ.* Physical Downlink Control Channel — физический канал управления в нисходящей линии связи).

В канале PDCCH набор кодовых слов мультиплексируется, после чего скремблируется. Для запуска генератора используется $c_{init} = \left\lfloor \frac{n_s}{2} \right\rfloor \times 2^9 + N_{ID}^{cell}$.

Для модуляции используется QPSK [30]. Для прекодирования используется такое же количество антенных портов, как и для передачи PBCH. Для размещения канала PDCCH в ресурсной сетке используются все группы ресурсных элементов (REG, *аббр. от англ.* Resource Element Group), оставшиеся после размещения каналов PCFICH (*аббр. от англ.* Physical Control Format Indicator Channel — физический канал для передачи индикатора CFI) и PHICH в пространстве управления. Перед размещением элементы REG перемежаются, используя блочный перемежитель для сверточного кода, на вход которого вместо битовой последовательности подаются номера REG. После перемежения и удаления пустых элементов REG циклически сдвигаются на величину N_{ID}^{cell} .

CFI — индикатор, указывающий размер пространства управления: количество символов в подкадре, которые выделены для передачи канала PDCCH. CFI может принимать значения 1, 2 и 3, для

канала шириной 6 РБ все значения увеличены на 1. Кодовые слова определяются блочным кодом длиной 32 бита и указаны в таблице 5.

Таблица 5. Кодовые слова для CFI [29]

CFI	Кодовое слово
1	01101101101101101101101101101101
2	10110110110110110110110110110110
3	11011011011011011011011011011011

Кодовые слова передаются в физический канал PCFICH [29]. Для инициализации генератора скремблирующей последовательности используется значение $c_{init} = \left(\left\lfloor \frac{n_s}{2} \right\rfloor + 1\right) (2N_{ID}^{cell} + 1)2^9 + N_{ID}^{cell}$.

Используется модуляционная схема QPSK [30]. Для прекодирования используется такое же количество антенных портов, как и для передачи PBCH. Символы размещаются в четырех REG. Номер первой поднесущей k REG номер n вычисляется согласно:

$$k(n) = \left(\frac{N_{sc}^{RB}}{2} (N_{ID}^{cell} \bmod 2N_{RB}^{DL}) + \left\lfloor \frac{nN_{RB}^{DL}}{2} \right\rfloor \frac{N_{sc}^{RB}}{2}\right) \bmod N_{RB}^{DL} N_{sc}^{RB}. \quad (5)$$

HI – индикатор HARQ-подтверждений. Поскольку в разрабатываемом анализаторе взаимодействия с БС на передачу и прием пользовательских данных производиться не будет, то обработку HI можно далее не рассматривать. Однако количество и расположение ресурсных элементов (РЭ), выделяемых для передач PDCCH, зависят от размещения канала PHICH, в котором передается HI. Поэтому далее необходимо рассмотреть особенности размещения символов PHICH в ресурсной сетке.

Каналы PHICH передаются группами. При использовании типа дуплекса TDD из-за различного расписания DL и UL передач в кадре типа структуры 2 [30] количество групп PHICH N_{PHICH}^{group} зависит от коэффициента масштабирования m_i для номера подкадра i [30], для типа дуплекса FDD m_i равен 1 для всех подкадров при использовании нормального циклического префикса и 2 при использовании расширенного префикса. N_{PHICH}^{group} также зависит от количества, выделяемых для передачи PHICH, ресурсов N_g , которое передается в блоке MIB в поле phich-Resource структуры PHICH-Config [28], и вычисляется согласно выражению:

$$N_{PHICH}^{group} = m_i \left\lfloor N_g \frac{N_{RB}^{DL}}{8} \right\rfloor. \quad (6)$$

Всего в одном подкадре есть три блока PHICH, в каждом из которых содержится N_{PHICH}^{group} групп. Номер символа l'_i , в котором размещается блок номер i , зависит от продолжительности передачи PHICH, передаваемой в PHICH-Config в поле PHICH-Duration: для нормальной продолжительности все блоки передаются в первом символе подкадра; для расширенной продолжительности существует несколько вариантов, но, учитывая, что SIB1 передается только в 5-м подкадре [28], i и l'_i совпадают. Символы PHICH размещаются только в REG, оставшихся после размещения канала PCFICH в ресурсной сетке. Номер REG \bar{n}_i вычисляется по следующей формуле:

$$\bar{n}_i = \left\lfloor N_{ID}^{cell} \frac{n_{l'_i}}{n_1} \right\rfloor + m' + \left\lfloor i \frac{n_{l'_i}}{3} \right\rfloor, \quad (7)$$

где $n_{l'_i}$ – количество доступных REG в символе l'_i ; n_1 – количество доступных REG в 1-м символе подкадра; m' – номер группы PHICH.

Опорные сигналы CRS предназначены для выравнивания характеристики (реакции) канала при его обработке в приемнике. Поскольку требуется прочитать системную информацию, которая передается в направлении DL, то из всех типов опорных сигналов достаточно рассмотреть CRS.

CRS состоит из элементов псевдослучайной последовательности Голда, которая инициализируется значением c_{init} [30]:

$$c_{init} = (7(n_s + 1) + l + 1)(2N_{ID}^{cell} + 1)2^{10} + 2N_{ID}^{cell} + N_{CP}, \quad (8)$$

где N_{CP} — индикатор циклического префикса, который равен 1 для нормального префикса и 0 для расширенного.

Последовательность Голда модулируется с QPSK: ее четные элементы передаются в синфазной, а нечетные — в квадратурной составляющей сигнала. CRS может одновременно передаваться по одному, двум или четырем антенным портам. Размещение модулированной последовательности в ресурсной сетке и инициализирующее значение для ее генерации зависят от номера символа l , который, в свою очередь, зависит от номера антенного порта p :

$$l = \begin{cases} 0, N_{symb}^{DL} - 3 & \text{при } p \in \{0,1\} \\ 1 & \text{при } p \in \{2,3\} \end{cases}, \quad (9)$$

где N_{symb}^{DL} — количество символов в слоте: для нормального циклического префикса — 7 символов, для расширенного — 6 [30]; p — номер антенного порта.

Номер поднесущей k для элемента m определяется согласно выражению:

$$k = 6m + (v + v_{shift}) \bmod 6, \quad (10)$$

где v и v_{shift} — частотные сдвиги, которые равны:

$$v = \begin{cases} 0 & \text{при } p = 0 \text{ и } l = 0 \\ 3 & \text{при } p = 0 \text{ и } l \neq 0 \\ 3 & \text{при } p = 1 \text{ и } l = 0 \\ 0 & \text{при } p = 1 \text{ и } l \neq 0 \\ 3(n_s \bmod 2) & \text{при } p = 2 \\ 3 + 3(n_s \bmod 2) & \text{при } p = 3 \end{cases}, \quad (11)$$

$$v_{shift} = N_{ID}^{cell} \bmod 6.$$

Пример размещения CRS в ресурсной сетке одного РБ, передаваемых по четырем антенным портам, для нормального циклического префикса и $N_{ID}^{cell} = 5$ приведен на рисунке 4.

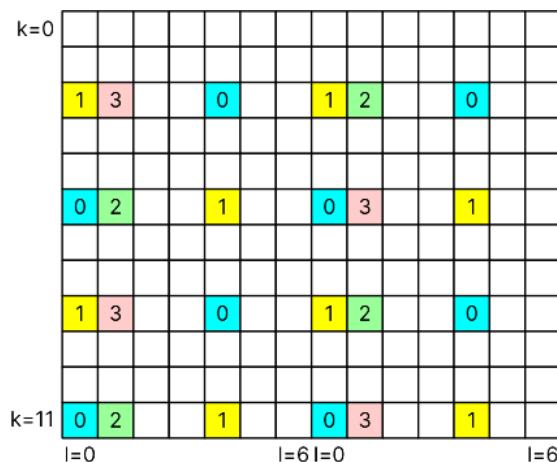


Рис. 4. Размещение CRS в ресурсной сетке [30]

Сигналы PSS и SSS предназначены для обеспечения синхронизации передач БС и UE, с их помощью находится PCI, который используется в том числе для инициализации генератора последовательностей Голда и отыскания частотных сдвигов различных физических каналов.

Первичный сигнал синхронизации PSS представляет собой последовательность Задова – Чу $d_u(n)$ длиной 62 символа, которая равна:

$$d_u(n) = \begin{cases} e^{-j\frac{\pi u n(n+1)}{63}} & \text{при } 0 < n \leq 30 \\ e^{-j\frac{\pi u (n+1)(n+2)}{63}} & \text{при } 31 < n \leq 61 \end{cases}, \quad (12)$$

где u – корень последовательности, определяемый физическим идентификатором соты внутри группы сот $N_{ID}^{(2)}$ (таблица 6).

Таблица 6. Корни последовательности Задова – Чу [30]

$N_{ID}^{(2)}$	Корень u
0	25
1	29
2	34

При использовании типа дуплекса FDD PSS передается в последнем символе 0-го и 10-го слотов каждого кадра на 62 центральных поднесущих. При использовании типа дуплекса TDD PSS размещается в третьем символе 2-го и 12-го слотов.

SSS является скремблированной последовательностью $d(n)$, состоящей из двух перемеженных между собой последовательностей длиной 31 символ):

$$d(2n) = \begin{cases} s_0^{(m_0)}(n)c_0(n) & \text{в подкадрах 0,1} \\ s_1^{(m_1)}(n)c_0(n) & \text{в подкадрах 5,6} \end{cases}, \quad (13)$$

$$d(2n + 1) = \begin{cases} s_1^{(m_1)}(n)c_1(n)z_1^{(m_0)} & \text{в подкадрах 0,1} \\ s_0^{(m_0)}(n)c_1(n)z_1^{(m_1)} & \text{в подкадрах 5,6} \end{cases}.$$

Эти последовательности состоят из комбинации модулированных BPSK M-последовательностей 5-го порядка, задающие полиномы и циклические сдвиги которых указаны в таблице 7. Величины сдвигов зависят от индексов m_0 и m_1 , значения которых приведены в [30] и зависят от физического идентификатора группы сот $N_{ID}^{(1)}$. Сдвиговые регистры генераторов M-последовательностей инициализируются цифровым импульсом.

Таблица 7. Параметры M-последовательностей

M-последовательность	Полином	Сдвиг
$s_0^{(m_0)}(n)$	100101	m_0
$s_1^{(m_1)}(n)$		m_1
$c_0(n)$	101001	$N_{ID}^{(2)}$
$c_1(n)$		$N_{ID}^{(2)} + 3$
$z_1^{(m_0)}(n)$	110111	$m_0 \bmod 8$
$z_1^{(m_1)}(n)$		$m_1 \bmod 8$

При использовании типа дуплекса FDD SSS передается в предпоследнем символе 0-го и 10-го слотов каждого кадра на 62 центральных поднесущих, для TDD SSS передается в последнем символе 1-го и 11-го слотов.

Для передачи сигналов синхронизации выделяются 6 центральных РБ, но, исходя из размеров этих сигналов, 10 крайних поднесущих не используются и также запрещены к использованию другими каналами.

PCI вычисляется согласно выражению [30]:

$$N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}. \quad (14)$$

Далее опишем особенности программной реализации и экспериментальной апробации рассмотренных выше процедур.

Особенности программной реализации анализатора сигналов стандарта LTE

Блок-схема программной реализации анализатора сигналов стандарта LTE, выполняющего определение местоположения ближайшей БС, представлена на рисунке 5.

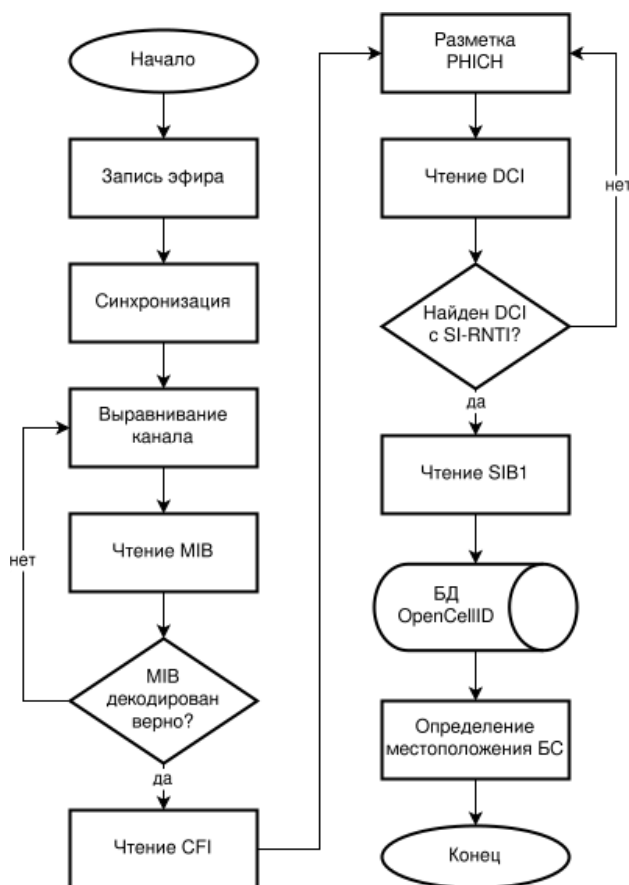


Рис. 5. Блок-схема алгоритма определения местоположения БС

Первым этапом программной реализации анализа сигналов стандарта LTE является конфигурация платы USRP B210 и запись радиоэфира. Поскольку распределение частотных каналов сетей LTE, принадлежащих операторам сотовой связи, заранее неизвестно, то номер частоты канала EARFCN (аббр. от англ. E-UTRA Absolute Radio Frequency Channel Number – номер радиочастотного канала в сети E-UTRA) будем получать с помощью внешних программ, таких как G-NetTrack [33]. Преобразование значения EARFCN в абсолютное значение частоты F_{DL} будем осуществлять согласно выражению [16]:

$$F_{DL} = F_{DL_{low}} + 0,1(N_{DL} - N_{Offs-DL}), \quad (15)$$

где F_{DL_low} — нижняя частота диапазона; N_{DL} — номер частоты канала EARFCN; $N_{offs-DL}$ — смещение номера частоты канала N_{DL} .

Поскольку размещение сигналов синхронизации PSS и SSS канала PICH зависит от типа дуплекса, то будем определять его по номеру диапазона в соответствии с [16]. Для корректной записи эфира частота дискретизации f_d должна соответствовать временной единице T_s [30]:

$$f_d = \frac{1}{T_s} = 15000 \times 2048 = 30,72 \text{ МГц.} \quad (16)$$

Поскольку уменьшать частоту дискретизации не требуется, то коэффициент децимации примем равным 1. Для экономии объема памяти компьютера, выделяемой для хранения записи, примем длительность записи равной 20 кадрам: 0,2 с. Параметры записи представлены в таблице 8.

Таблица 8. Параметры записи эфира

Параметр	Значение
Частота дискретизации, МГц	30,72
Коэффициент децимации	1
Количество отсчетов в 1 кадре	2048
Длительность записи, с	0,2

Первым этапом подключения устройства UE к БС сети является синхронизация с ней — нахождение сигналов синхронизации в эфире и вычисление по ним PCI.

Для поиска PSS из всей записи эфира будем обрабатывать фрагмент длительностью 10 кадров, в течение которого состояние среды передачи может множество раз изменяться, а значит, шанс удачного нахождения истинного сигнала PSS будет высок. Вычисляя взаимную корреляционную функцию (ВКФ) этого промежутка с OFDM-символами, сгенерированными со всеми возможными корнями последовательностей Задова — Чу, по ее максимуму найдем физический идентификатор соты внутри группы сот $N_{ID}^{(2)}$ и сдвиг от начала записи до начала символа слота, в котором передавался PSS. Для того, чтобы быть уверенными в том, что в выбранном отсчете действительно находится PSS, примем минимум пик-фактора ВКФ равным 2.

Как видно из таблицы 7, M-последовательность $s(n)$, из которой состоит сигнал SSS, поочередно сдвигается на величину индексов m_0 и m_1 . По этим индексам находится физический идентификатор группы сот $N_{ID}^{(1)}$.

Для этого нужно OFDM-символ принятого сигнала демодулировать и разделить на последовательности четных и нечетных элементов. Затем вычислить ВКФ $s(n)$ и последовательности нечетных элементов, умноженной на $c_0(n)$. По положению максимума ВКФ найти индекс m_0 . Последовательность четных элементов, умноженная на $c_1(n)$ и $z_1^{(m_0)}(n)$, коррелируется с $s(n)$. По положению максимума ВКФ находится индекс m_1 . Во избежание ошибок при нахождении индекса m_1 ограничим зону, в которой будет происходить поиск максимума ВКФ диапазоном $m_0 \pm 7$.

На следующем этапе приемник анализатора сигналов выполняет выравнивание канала с помощью опорных сигналов CRS, передаваемых БС.

Поскольку изначально количество антенных портов неизвестно, то необходимо произвести перебор доступных значений: 1, 2 или 4 порта. Проверку правильности выбора значения будем осуществлять на этапе чтения блока MIB: если его удалось правильно декодировать, что подтверждается с помощью CRC-суммы, то и количество антенных портов подобрано верно, иначе обработка повторяется со следующим значением.

Умножив принятые CRS на комплексно-сопряженные значения сгенерированных символов, получим реакцию канала в РЭ, в которых они были размещены. Интерполировав значения по частоте на всю ширину канала и по времени на все символы, получим реакцию канала на всей ресурсной сетке. Для уменьшения количества вычислений будем считать ширину канала равной 6 РБ, поскольку именно

столько РБ отводится для размещения символов канала РВСН. Разделив принятые символы на реакцию канала, вычтем ее из принятого сигнала.

Поскольку размещение канала РВСН фиксировано, то для поиска блока МІВ будем считать РЭ первого подкадра. Так как блок МІВ занимает 4 последовательные передачи канала РВСН, для его поиска требуется обработать, как минимум, 7 передач.

После выделения требуемых РЭ, осуществляется их депрекодирование. Для одного антенного порта процедура игнорируется, при использовании двух или четырех антенных портов каждая пара соседних символов преобразовывается согласно следующей формуле:

$$\begin{aligned} x^{(0)}(i) &= \frac{\operatorname{Re}(y(2i)+y(2i+1))}{2} + j \times \frac{\operatorname{Im}(y(2i)-y(2i+1))}{2}, \\ x^{(1)}(i) &= \frac{\operatorname{Re}(y(2i+1)-y(2i))}{2} + j \times \frac{\operatorname{Im}(y(2i)+y(2i+1))}{2}. \end{aligned} \quad (17)$$

Поскольку количество слоев, используемых при передаче канала РВСН, равно количеству антенных портов, то дополнительной обработки на данном этапе не происходит и символы передаются в демодулятор в том же порядке, в котором они считывались из ресурсной сетки.

Для демодуляции будем использовать алгоритм принятия мягких решений в логарифмическом масштабе. Таким образом увеличим точность вычислений за счет того, что в отличие от жестких решений станет доступна для анализа мера надежности принятия решения. Демодулятор принимает решения согласно выражению [34]:

$$LLR(c_i) = \frac{1}{2\sigma_N^2} \left[\min_{U \in C_i^1} |y - U| - \min_{U \in C_i^0} |y - U| \right], \quad (18)$$

где c_i — бит i текущего символа; $LLR(c_i)$ — принятое решение для бита c_i ; σ_N — среднеквадратическое отклонение белого Гауссовского шума; y — принятый символ; U — символ выбранной модуляционной схемы; C_i^j — множество символов модуляционной схемы, в которых бит c_i принимает значение j .

Далее происходит поиск блока информации МІВ. Поскольку для всех четырех последовательных передач канала РВСН применяются одна скремблирующая последовательность, то процедура поиска будет заключаться в объединении мягких бит четырех соседних передач и попытке их декодирования. Если попытка декодирования окажется неудачной, то со сдвигом, равным одной передаче, процесс будет повторяться.

После осуществления дескремблирования произведем восстановление скорости кодового слова: сложив значения каждого k бита кодового слова, где k — 3 размера кодированного блока информации. Промоделировав процесс задания скорости для последовательности номеров элементов и произведя сортировку результата, найдем паттерн перестановок элементов кодированной последовательности.

Следующим этапом является декодирование по алгоритму Витерби [35]. Задачей декодера является вычисление метрик путей как Евклидова расстояния между мягкими входными битами и 2^k возможными состояниями кодера (для используемого в стандарте LTE кодера $k = 6$). В процессе работы декодер формирует 2^k путей между различными состояниями. На каждом шаге путь с наибольшей метрикой последнего перехода из всех путей, перешедших в одно состояние, удаляется. В случае равенства метрик последнего перехода удаляется путь с наибольшей метрикой на всем пути. В случае равенства метрик путей удаляется путь с наибольшим значением последнего состояния. Если на промежутке, длина которого составляет длину кодового блока, все пути эквивалентны, то работа декодера считается завершенной и принимаются решения о значении принятых бит как выходных бит кодера при переходе им между установленными состояниями.

После декодирования кодового блока проверяется прикрепленная к нему CRC-сумма, при этом, в зависимости от количества используемых антенных портов, выбирается маска, которой она была скремблирована.

Из всей принятой ресурсной сетки выделим 5-й подкадр каждого 2-го кадра, поскольку только в нем может передаваться канал PDSCH для системной информации. Выделив из первого символа каждого подкадра РЭ, передаваемые по каналу PCFICH, произведя демодуляцию и дескремблирование бит, найдем расстояние Хэмминга между принятым кодовым словом и тремя его возможными значениями. Значением сообщения CFI будем считать то, расстояние до кодового слова которого оказалось наименьшим, но не более 8.

Поскольку размещение канала PDCCH зависит от размещения канала PHICH, то перед чтением DCI определим РЭ, выделенные для канала PHICH, по данным, полученным из блока MIB, и типу дуплекса. Если поиск DCI завершится неудачей, и при этом используется тип дуплекса TDD, то процесс будет перезапущен со следующим номером конфигурации TDD.

Выделив все РЭ в первых символах подкадра, чье количество определяется значением сообщения CFI, и исключив РЭ, занятые сигналами CRS и каналами PCFICH и PHICH, произведем перемежение REG, депрекодирование, демодуляцию и дескремблирование полученных символов. Далее вычислим предполагаемые размеры DCI форматов 1A и 1C, и, поскольку перед скремблированием все блоки DCI были мультиплексированы, будем последовательно производить перебор кандидатов на всех возможных уровнях агрегации в общем пространстве поиска, начинающегося с первого CCE в пространстве управления [32]: для каждого кандидата на роль DCI, переданного с SI-RNTI, восстанавливать скорость кодового слова, декодировать и проверять CRC-сумму полученной битовой последовательности, дескремблировав ее значением SI-RNTI: 0xFFFF [31]. После успешной проверки CRC-суммы по размеру блока информации определим формат блока DCI и произведем его чтение.

Номер первого VRB RB_{start} и количество выделяемых последовательных VRB L_{CRBs} , передаваемых с помощью индикатора RIV, найдем их последовательным перебором: значение L_{CRBs} изменяется в диапазоне от 1 до количества РБ в канале N_{RB}^{DL} , значение RB_{start} изменяется в диапазоне от 0 до $N_{RB}^{DL} - 1$.

При использовании распределенного размещения VRB вычислим номера PRB. Значение разнесения РБ N_{gap} определяется шириной канала согласно [30]. Количество VRB N_{VRB}^{DL} определяется выбранным значением N_{gap} :

- 1) при $N_{gap} = N_{gap,1}$: $N_{VRB}^{DL} = 2\min(N_{gap}, N_{RB}^{DL} - N_{gap})$;
- 2) при $N_{gap} = N_{gap,2}$: $N_{VRB}^{DL} = 2N_{gap} \times \left\lfloor \frac{N_{RB}^{DL}}{2N_{gap}} \right\rfloor$.

Количество последовательных VRB \tilde{N}_{VRB}^{DL} , готовящихся к перемежению, определяется значением N_{gap} . При $N_{gap} = N_{gap,1}$: $\tilde{N}_{VRB}^{DL} = N_{VRB}^{DL}$, при $N_{gap} = N_{gap,2}$: $\tilde{N}_{VRB}^{DL} = 2N_{gap}$. Перемежитель представляется в виде матрицы с четырьмя столбцами и N_{row} строками, при $N_{row} = P \left\lceil \frac{\tilde{N}_{VRB}^{DL}}{4P} \right\rceil$, где P — размер группы РБ согласно [32]. Запись номеров VRB в матрицу производится по строкам, чтение — по столбцам. N_{null} пустых элементов записывается в $\frac{N_{null}}{2}$ последних строк 2-го и 4-го столбцов, где $N_{null} = 4N_{row} - \tilde{N}_{VRB}^{DL}$. Номера PRB n_{PRB} вычисляются согласно формуле:

$$n_{PRB}(n_s) = \begin{cases} \tilde{n}_{PRB}(n_s) & \text{при } \tilde{n}_{PRB} < \frac{\tilde{N}_{VRB}^{DL}}{2} \\ \tilde{n}_{PRB}(n_s) + N_{gap} - \frac{\tilde{N}_{VRB}^{DL}}{2} & \text{при } \tilde{n}_{PRB} \geq \frac{\tilde{N}_{VRB}^{DL}}{2} \end{cases} \quad (19)$$

где \tilde{n}_{PRB} зависит от номера слота в подкадре n_s :
— для 1-го слота подкадра ($n_s = 0$):

$$\tilde{n}_{PRB} = \begin{cases} \tilde{n}'_{PRB} - N_{row} & \text{при } N_{null} \neq 0, \tilde{n}_{VRB} \geq \tilde{N}_{VRB}^{DL} - N_{null}, \tilde{n}_{VRB} \bmod 2 = 1 \\ \tilde{n}'_{PRB} - N_{row} + \frac{N_{null}}{2} & \text{при } N_{null} \neq 0, \tilde{n}_{VRB} \geq \tilde{N}_{VRB}^{DL} - N_{null}, \tilde{n}_{VRB} \bmod 2 = 0 \\ \tilde{n}''_{PRB} - \frac{N_{null}}{2} & \text{при } N_{null} \neq 0, \tilde{n}_{VRB} < \tilde{N}_{VRB}^{DL} - N_{null}, \tilde{n}_{VRB} \bmod 4 \geq 2 \\ \tilde{n}''_{PRB} & \text{в остальных случаях} \end{cases} \quad (20)$$

где промежуточные номера PRB \tilde{n}'_{PRB} и \tilde{n}''_{PRB} равны:

$$\begin{aligned}\tilde{n}'_{PRB} &= 2N_{row}(\tilde{n}_{VRB} \bmod 2) + \left\lfloor \frac{\tilde{n}_{VRB}}{2} \right\rfloor + \tilde{N}_{VRB}^{DL} \left\lfloor \frac{n_{VRB}}{\tilde{N}_{VRB}^{DL}} \right\rfloor, \\ \tilde{n}''_{PRB} &= 2N_{row}(\tilde{n}_{VRB} \bmod 4) + \left\lfloor \frac{\tilde{n}_{VRB}}{4} \right\rfloor + \tilde{N}_{VRB}^{DL} \left\lfloor \frac{n_{VRB}}{\tilde{N}_{VRB}^{DL}} \right\rfloor,\end{aligned}\quad (21)$$

где \tilde{n}_{VRB} – промежуточный номер VRB, вычисляется как модуль номера VRB по количеству последовательных VRB \tilde{N}_{VRB}^{DL} ;
– для 2-го слота подкадра ($n_s = 1$):

$$\tilde{n}_{PRB} = \left(\tilde{n}_{PRB}(n_s - 1) + \frac{\tilde{N}_{VRB}^{DL}}{2} \right) \bmod \tilde{N}_{VRB}^{DL} + \tilde{N}_{VRB}^{DL} \left\lfloor \frac{n_{VRB}}{\tilde{N}_{VRB}^{DL}} \right\rfloor. \quad (22)$$

Получив из блока DCI следующую информацию: набор номеров РБ, в которых размещается канал PDSCH, выбранная для его передачи модуляционная схема, размер транспортного блока TBS и индекс повторной передачи rv_{idx} , произведем по ней чтение блока SIB1.

Обработку физического канала PDSCH произведем аналогично ранее рассмотренным каналам. Восстановление скорости кодовых слов канала DL-SCH произведем по такому же алгоритму, который рассматривался для канала BCH, но с тем отличием, что для задания скорости будем использовать алгоритм для данных, кодированных турбокодером. Считая, что требуемая информация, передаваемая в блоке SIB1, изменяется очень редко, будем усреднять кодированные последовательности, полученные от нескольких передач PDSCH. Турбодекодер реализуем по алгоритму итеративного декодирования.

При итеративном декодировании мягкие решения принятых систематических y^s и проверочных бит y^p от 2 элементарных кодеров циклически обрабатываются двумя SISO-декодерами с мягкими входами и выходами (рисунок 6). Каждый декодер вычисляет и уточняет внешнюю информацию $L^{(e)}(u_i)$ о принятых битах u_i . Между 1-м и 2-м декодерами установлен перемежитель Π , между 2-м и 1-м – деперемежитель Π^{-1} , требующиеся для восстановления порядка систематических бит, которые поступали на входы элементарных кодеров. На каждой итерации вычисляется жесткое решение суммы решений $L(u_i)$, полученных от обоих декодеров, и систематических бит. Если CRC-сумма последовательности жестких бит проходит проверку, то работа декодера считается завершенной, иначе декодер переходит на следующую итерацию. Поскольку при изначально неверных данных декодер никогда не сможет завершить свою работу, ограничим количество итераций пятью.

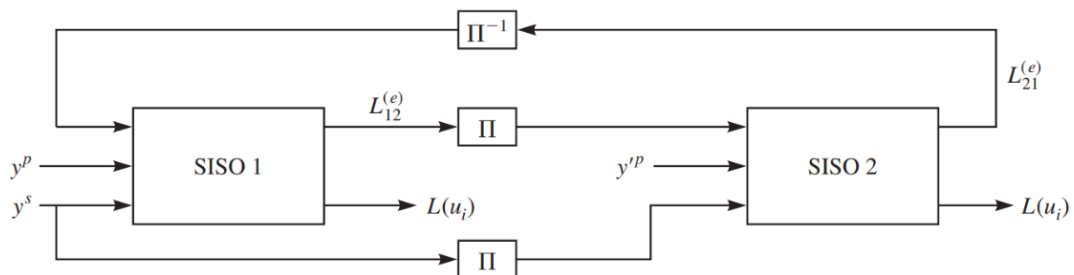


Рис. 6. Структура итеративного турбодекодера [35]

Перед началом процесса декодирования учтем влияние среды передачи в коэффициенте надежности решений, принятых демодулятором, и умножим все входные мягкие биты на него. Коэффициент надежности вычислим как среднеквадратическое отклонение закодированной последовательности от нулевой. Элементарные SISO-декодеры реализуем по алгоритму MAP (аббр. от англ. Maximum A-posteriori Probability – максимум апостериорной вероятности) в логарифмическом масштабе, который является усовершенствованием алгоритма BCJR (от первых букв фамилий его изобретателей Bahl, Cocke, Jelinek and Raviv).

Поскольку начальное и конечное состояния кодера известны, то в отличие от декодера Витерби, который вычисляет только метрики текущих переходов $\Gamma_k(x)$, в этом алгоритме также вычисляются метрики переходов в предыдущие $B_k(S_i)$ и будущие $A_k(S_i)$ состояния [36]:

$$\begin{aligned} A_k(S_i) &= \max_u [A_{k-1}(S_i^-(u)) + \Gamma_k(x(u, S_i))], \\ B_k(S_i) &= \max_u [B_{k+1}(S_i^+(u)) + \Gamma_{k+1}(x(S_i, u))], \end{aligned} \quad (23)$$

где i — номер состояния; k — номер перехода; u — мягкий бит; $S_i^-(u)$ — предыдущее состояние для бита u ; $S_i^+(u)$ — будущее состояние для бита u ; $x(u, S_i)$ — набор бит для принятого бита u , который кодер мог бы сгенерировать при переходе в состояние S_i .

Пояснение к алгоритму расчета метрик представлено на рисунке 7. Вычисление итоговых метрик $\Sigma_k(S_i, u)$ производится согласно формуле:

$$\Sigma_k(S_i, u) = A_{k-1}(S_i^-(u)) + \Gamma_k(x(u, S_i)) + B_{k+1}(S_i^+(u)). \quad (24)$$

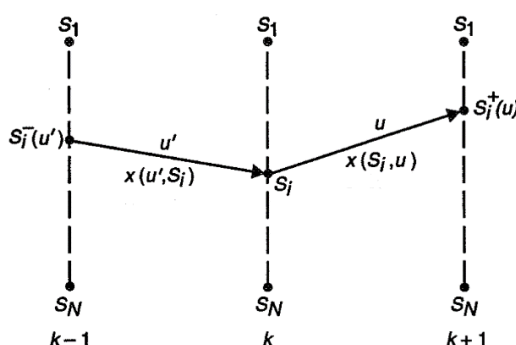


Рис. 7. Решетчатая диаграмма BCJR-декодера [36]

Декодер принимает решение о значении полученного бита как разности итоговых метрик $\Sigma_k(S_i, u)$ для переданных бит $u = 1$ и $u = 0$.

После чтения полей plmn-IdentityList, trackingAreaCode и cellIdentity блока SIB1 произведем запрос к БД OpenCellID, заранее получив ключ для доступа к сервису apiKey и сформировав HTTP-запрос, имеющий следующую структуру [19]: <http://www.opencellid.org/cell/get?key=<apiKey>&mcc=<mcc>&mnc=<mnc>&lac=<lac>&cellid=<cellid>&format=at>. В ответ от БД получим текстовую строку, в которой последовательно будут указаны широта и долгота местоположения БС, например: «+Location: 52.231644,21.011933,1713106250», в случае отсутствия записей о БС в БД: «+Error:Cell not found».

Для определения местоположения пользователя необходимо оценить координаты хотя бы трех соседних БС. После этого в первом приближении можно оценить расстояния до каждой из БС через нормирование значений средней мощности принятых сигналов.

Особенности экспериментальной апробации анализатора сигналов стандарта LTE

Рассмотрим особенности экспериментальной апробации анализатора сигналов стандарта LTE. Успешность обнаружения сигналов стандарта LTE на начальном этапе обусловлена, в первую очередь, извлечением сигналов синхронизации.

На рисунке 8 показана спектрограмма частотно-временной ресурсной сетки подкадра стандарта LTE до и после работы функции выравнивания канала (эквалайзера) «equalize»; по одной из осей ресурсной сетки отложены номера поднесущих, а по другой — номера OFDM-символов.

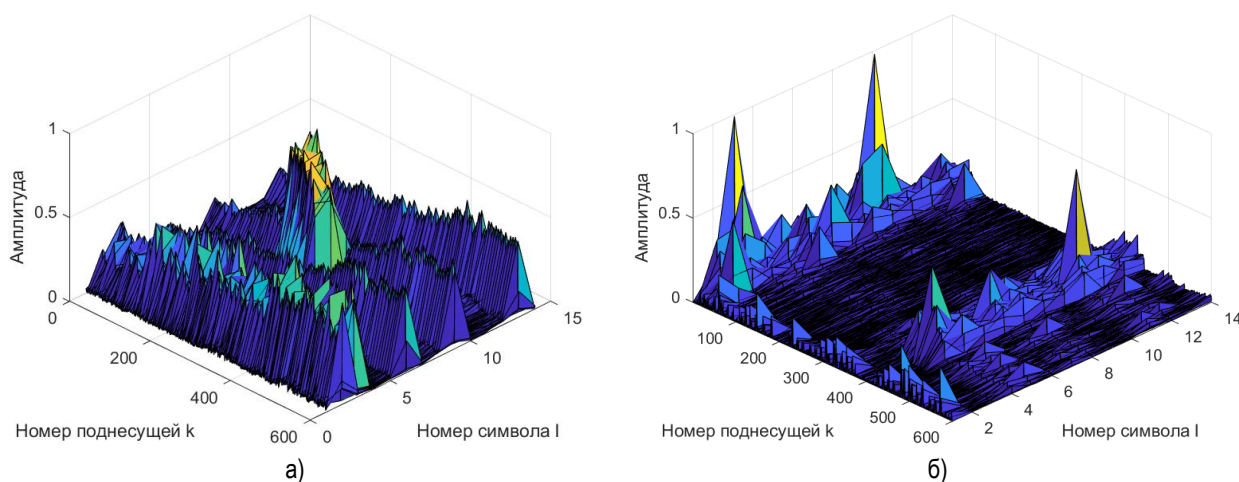


Рис. 8. Результат работы функции «equalize»: а) входные данные; б) выходные данные

Из анализа спектрограмм на рисунке 8 следует, что после обработки на ресурсной частотно-временной сетке пропали волнообразные всплески амплитуды сигнала на временной оси и ее нарастание вдоль оси частот, однако появились выделяющиеся относительно остальных РЭ пики сигналов синхронизации, а также стали визуально различимы основные элементы ресурсной сетки подкадра, включающие данные канала PDCCH в первых символах подкадра.

Оценку эффективности работы декодеров произведем имитационным моделированием с помощью случайной последовательности бит, модуляции закодированных данных и сложения полученного сигнала с шумом различной мощности. Для генерации проверочных данных были выбраны следующие параметры: длина кодируемой последовательности — 40 бит, модуляционная схема — QPSK, тип решений на выходе демодулятора — мягкие. Сравнение реализованного из примитивных функций алгоритма декодирования с работой функций, встроенных в MATLAB, выполнено по критерию коэффициента битовых ошибок BER (аббр. от англ. Bit Error Rate); результаты имитационного моделирования показаны на рисунке 9.

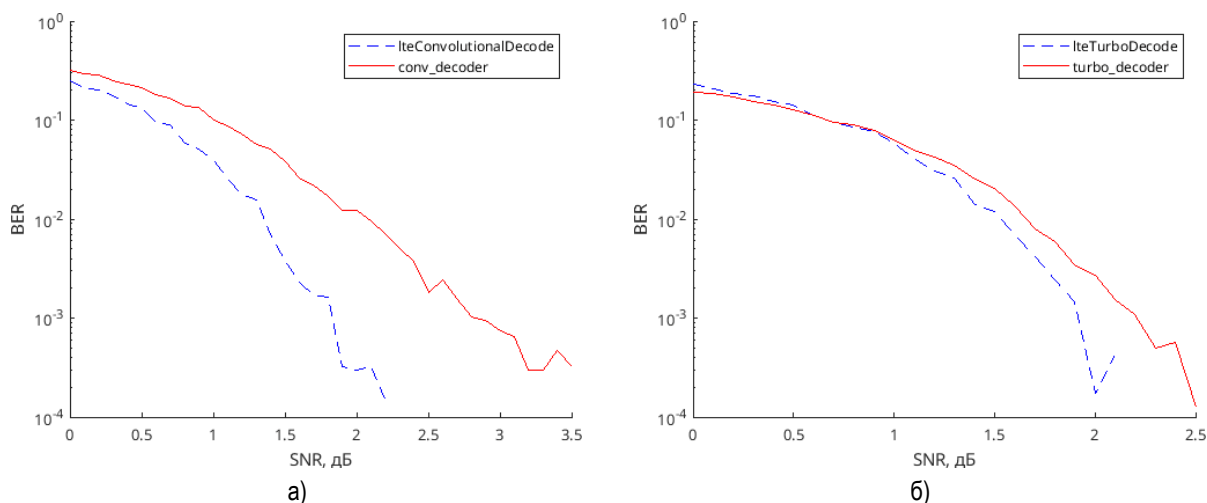


Рис. 9. График зависимости BER декодеров от отношения сигнал/шум: а) сверточных декодеров; б) турбодекодеров

Из графиков зависимости BER от отношения сигнал/шум на рисунке 9 следует, что функционирование самостоятельно реализованного (красная кривая) сверточного и турбодекодера соответствует работе встроенной функции MATLAB (синяя кривая) при отношении сигнал/шум не менее 3,5 и 2,5 дБ, соответственно.

Взаимосвязь составных программных модулей разработанного анализатора широкополосных сигналов стандарта LTE показана на рисунке 10. Структурная схема экспериментальной апробации приводится на рисунке 11.

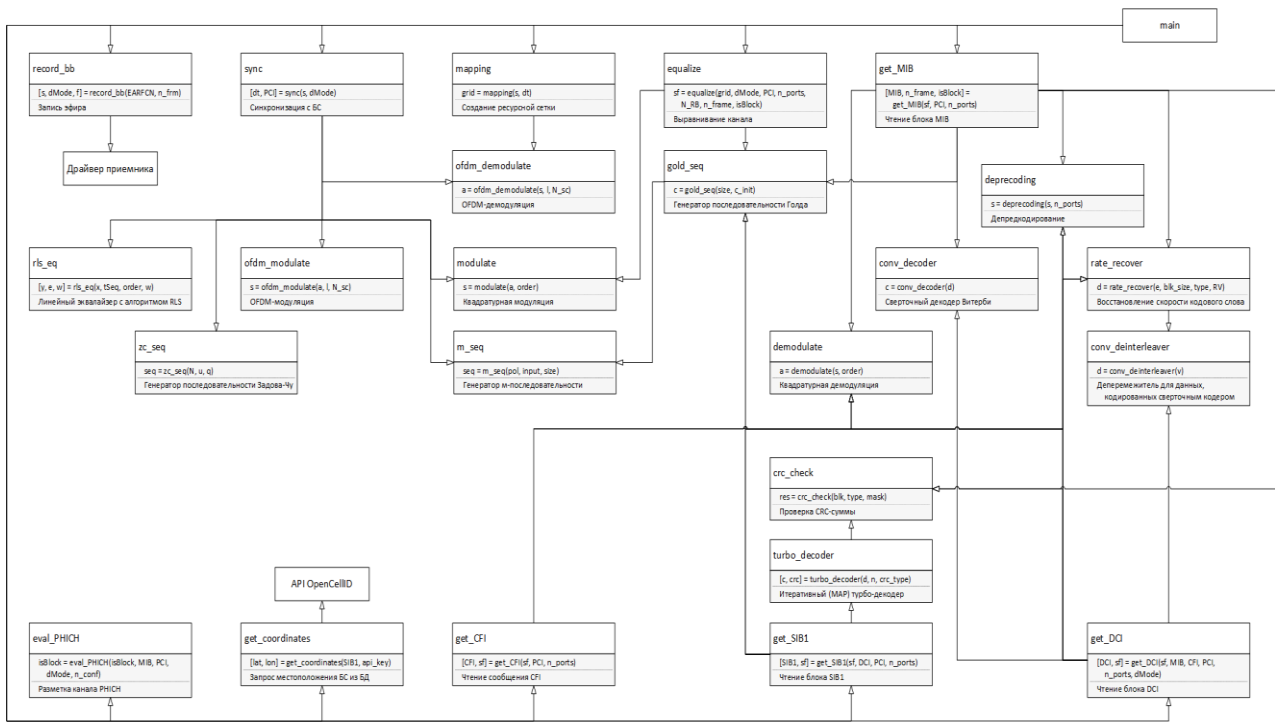


Рис. 10. Взаимосвязь составных программных модулей анализатора сигналов стандарта LTE

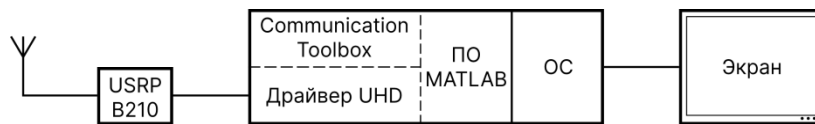


Рис. 11. Структурная схема экспериментальной апробации

Результаты профилирования программных модулей анализатора сигналов стандарта LTE по времени выполнения для одной заранее подготовленной и загруженной в АРМ записи радиоэфира длительностью 20 кадров с принятыми сигналами от БС, работающей с частотным дуплексом и двумя антенными портами, указаны в таблице 9 и на рисунке 12.

Таблица 9. Результаты профилирования программы приемника

Название функции	Количество вызовов	Время выполнения, мс	Относительное время выполнения, %
sync	1	2182	34,34
get_MIB	2	1624	25,56
get_coordinates	1	923	14,53
get_DCI	1	654	10,29
equalize	3	420	6,61
mapping	1	376	5,92
get_SIB1	1	95	1,49
get_CFI	1	11	0,17
eval_PHICH	1	10	0,16
остальное	—	59	0,93



Рис. 12. Flame-граф вызовов программы приемника

По приведенным выше данным видно, что функциями с наибольшим временем выполнения оказались: «sync» из-за вычисления ВКФ сигнала длительностью 10 кадров и сгенерированных сигналов PSS, «get_MIB» и «get_DCI» из-за большого количества вызовов сверточного декодера при поиске передач соответствующих сообщений, «get_coordinates» из-за обращения программы к БД через сеть «Интернет». Чрезмерно большое время выполнения программы объясняется недостатками режима интерпретации языка MATLAB, описанными при выборе средства разработки.

Комплексную проверку программы приемника проведем с помощью приема сигналов нескольких БС. Для каждой БС запишем полученный от приемника USRP набор отсчетов в файл. Результат обработки трех таких файлов программой анализа широкополосных сигналов стандарта LTE приведен на рисунке 13.

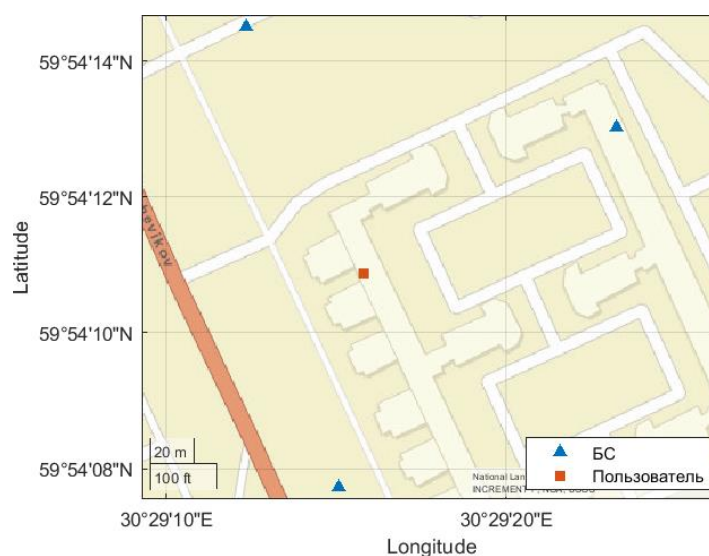


Рис. 13. Результат выполнения программы приемника

Данные на рисунке 13 позволяют сделать вывод о том, что разработанный анализатор сигналов стандарта LTE решает поставленную задачу корректно, что подтверждается отображением координат трех ближайших БС стандарта LTE на карте.

Заключение

Описанная в настоящем исследовании разработка и апробация анализатора сигналов стандарта LTE средствами SDR является первой отечественной работой, в которой детально описан порядок анализа широкополосных сигналов стандарта LTE для определения местоположения SDR-устройства, не являющегося абонентом какой-либо сети. Разработанный из примитивных функций набор программных модулей на языке MATLAB решает задачу анализа сигналов стандарта LTE от одной БС за несколько секунд по предварительной записи радиозэфира в режиме офлайн. Для анализа сигналов стандарта LTE синхронно с записью фрагмента радиозэфира в режиме онлайн параллельно от нескольких БС необходима программная реализация описанных процедур на языке HDL ПЛИС, что является предметом дальнейших исследований и разработок.

Практическая ценность исследования заключается в экспериментальном подтверждении возможности решения навигационной задачи с точностью до принадлежности к ближайшим БС сотовых сетей стандарта LTE в условиях ненадежного приема сигналов ГНСС.

Литература

1. ITU-D. Measuring Digital Development: Facts and Figures. 2022. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICT_MDD-2022-PDF-E.pdf (дата обращения 23.04.2024)

2. Ukraine: EU Agrees on Eighth Package of Sanctions against Russia. European Commission — Press Release. Brussels, 6 October 2022. URL: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_5989 (дата обращения 23.04.2024)
3. Collins T. F., Getz R., Pu D., Wyglinski A. M. Software-Defined Radio for Engineers. Norwood: Artech House, 2018. URL: <https://www.analog.com/media/en/training-seminars/design-handbooks/Software-Defined-Radio-for-Engineers-2018/SDR4Engineers.pdf> (дата обращения 23.04.2024)
4. Фокин Г. А. Технологии программно-конфигурируемого радио. М.: Горячая Линия — Телеком, 2019. 316 с. EDN: TMJLHA
5. Фокин Г. А. Современные тенденции в области программно-конфигурируемого радио // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции: в 4-х тт. (Санкт-Петербург, 01–02 марта 2017 г.). 2017. Т. 1. С. 271–276. EDN: ZECFGR
6. Фокин Г. А. Принципы и технологии цифровой связи на основе программно-конфигурируемого радио: обзор современных тенденций в области создания комплекса подготовки специалистов // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 78–94. DOI:10.31854/1813-324X-2019-5-1-78-94. EDN: ZEFYQH
7. Фокин Г. А., Лаврухин В. А., Волгушев Д. А., Киреев А. В. Модельно-ориентированное проектирование на основе SDR // Системы управления и информационные технологии. 2015. № 2 (60). С. 94–99. EDN: TWKVQB
8. Фокин Г. А., Буланов Д. В., Волгушев Д. Б. Модельно-ориентированное проектирование систем радиосвязи на основе ПКР // Вестник связи. 2015. № 6. С. 26–30. EDN: XDCTPR
9. Лаврухин В. А., Фокин Г. А. Разработка LPD-приемопередатчика с поддержкой MIMO на основе программно-конфигурируемого радио в приложении к управлению роботом // Extreme Robotics. 2016. Т. 1. № 1. С. 119–128. EDN: XERWIZ
10. Волгушев Д. Б., Киреев А. В., Фокин Г. А. Модельно-ориентированный синтез систем радиосвязи на основе программно-конфигурируемого радио // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2015, Санкт-Петербург, 03–04 марта 2015 г.). Сборник научных статей IV Международной научно-технической и научно-методической конференции. СПб.: СПбГУТ, 2015. Т. 1. С. 50–53. EDN: UNVNCF
11. Борисов Е. Г., Машков Г. М., Фокин Г. А. Экспериментальный стенд оценки точности позиционирования на основе программно-конфигурируемого радио // Актуальные проблемы инфотелекоммуникаций в науке и образовании. (АПИНО 2016? Санкт-Петербург, 10–11 марта 2016 г.). Сборник научных статей V Международной научно-технической и научно-методической конференции. СПб.: СПбГУТ, 2016. Т. 1. С. 120–125. EDN: WZINRT
12. Фокин Г. А. Комплекс моделей и методов позиционирования устройств в сетях пятого поколения. Дисс. ... д-ра тех. наук: 05.12.13. СПб.: СПбГУТ, 2021. 499 с. EDN: PQMSQX
13. Фокин Г. А., Волгушев Д. Б., Григорьев В. А. Способ позиционирования в сетях связи с использованием технологии программно-конфигурируемого радио. Патент на изобретение № 2817862 С1. Публикация 22.04.2024. Заявка от 18.09.2023.
14. КОНСУЛ сориентируется на местности // Коммерсантъ. 2021. № 76. URL: <https://www.kommersant.ru/doc/4793821> (дата обращения 23.04.2024)
15. Комплекс радиоконтроля ОМЕГА-М5 // ООО «Приборэлектро». URL: <https://www.priborelektro.ru/product/price/programmno-apparatnye-kompleksy-256/16057.html> (дата обращения 23.04.2024)
16. ETSI TS 136 101 V15.14.0: User Equipment (UE) Radio Transmission and Reception, 2021. URL: https://www.etsi.org/deliver/etsi_ts/136100_136199/136101/15.14.00_60/ts_136101v151400p.pdf (дата обращения 23.04.2024)
17. Комплекс выявления каналов утечки информации и электронных устройств негласного получения информации (ЭУНПИ) «Призрак» // ЗАО НПЦ Фирма «НЕЛК». URL: https://nelk.ru/catalog/tekhnicheskie_sredstva_poiska_kanalov_utechki_informatsii/kompleksy_vyuavleniya_radioperedayushchikh_tekhnicheskikh_sredstv_razvedki/prizrak (дата обращения 23.04.2024)
18. Data Sheet Version 32.00: FSH handheld analyzer specifications // Rohde & Schwarz: Munich, 2022. URL: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/FSH_dat-sw_en_5214-0482-22_v3200.pdf (дата обращения 23.04.2024)
19. OpenCellID wiki: API, 2024. URL: <https://wiki.opencellid.org/wiki/API> (дата обращения 30.04.2024)

20. USRP Hardware Driver and USRP Manual: USRP B2x0 Series // Ettus Research. 2024. URL: https://files.ettus.com/manual/page_usrp_b200.html (дата обращения 30.04.2024)
21. USRP Hardware Driver and USRP Manual: UHD Development Manual // Ettus Research. 2024. URL: https://files.ettus.com/manual/page_uhd.html (дата обращения 30.04.2024)
22. LabVIEW: Using NI-USRP in LabVIEW // National Instruments. 2024. URL: <https://www.ni.com/docs/en-US/bundle/ni-usrp/page/using-usrp-labview.html> (дата обращения 30.04.2024)
23. MATLAB: USRP Support from Communications Toolbox // MathWorks. 2024. URL: <https://www.mathworks.com/hardware-support/usrp.html> (дата обращения 30.04.2024)
24. GNU Radio: USRP Source, 2024. URL: https://wiki.gnuradio.org/index.php/USRP_Source (дата обращения 30.04.2024)
25. LabVIEW: What Are the Differences Between a LabVIEW Executable and an Installer // National Instruments. 2024. URL: <https://knowledge.ni.com/KnowledgeArticleDetails?id=kA00Z0000019YLjSAM> (дата обращения 30.04.2024)
26. MATLAB Coder: Generate C and C++ code from MATLAB code // MathWorks. 2024. URL: <https://www.mathworks.com/products/matlab-coder.html> (дата обращения 30.04.2024)
27. HDL Coder: Generate Verilog, System Verilog, and VHDL code for FPGA and ASIC designs // MathWorks. 2024. URL: <https://www.mathworks.com/products/hdl-coder.html> (дата обращения 30.04.2024)
28. ETSI TS 136 331 V15.14.0: Radio Resource Control (RRC); Protocol Specification. 2021. URL: https://www.etsi.org/deliver/etsi_ts/136300_136399/136331/15.14.00_60/ts_136331v151400p.pdf (дата обращения 10.05.2024)
29. ETSI TS 136 212 V15.14.0: Multiplexing and Channel Coding. 2021. URL: https://www.etsi.org/deliver/etsi_ts/136200_136299/136212/15.14.00_60/ts_136212v151400p.pdf (дата обращения 10.05.2024)
30. ETSI TS 136 211 V15.14.0: Physical channels and modulation, 2021. URL: https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/15.14.00_60/ts_136211v151400p.pdf (дата обращения 10.05.2024)
31. ETSI TS 136 321 V15.11.0: Medium Access Control (MAC) protocol specification. 2021. URL: https://www.etsi.org/deliver/etsi_ts/136300_136399/136321/15.11.00_60/ts_136321v151100p.pdf (дата обращения 10.05.2024)
32. ETSI TS 136 213 V15.14.0: Physical layer procedures, 2021. URL: https://www.etsi.org/deliver/etsi_ts/136200_136299/136213/15.14.00_60/ts_136213v151400p.pdf (дата обращения 10.05.2024)
33. G-NetTrack Manual // Gyokov Solutions, 2024. URL: <https://gyokovsolutions.com/manual-g-nettrack> (дата обращения 15.05.2024)
34. Yang W., Yang Z., Xu C. A Soft Demodulation Algorithm with Low Complexity for One-Dimensional DPC System // Wireless Personal Communication. 2013. № 69. PP. 1183–1195. DOI: 10.1007/s11277-012-0627-1
35. Proakis J. G., Salehi M. Digital Communications. Boston: McGraw Hill, 2008. URL: https://edisciplinas.usp.br/pluginfile.php/5636847/mod_resource/content/1/digital%20commun%205th%20-%20proakis%2C%20salehi.pdf (дата обращения 15.05.2024)
36. Benedetto S., Montorsi G., Divasalar D., Pollara F. Soft-Output Decoding Algorithms in Iterative Decoding of Turbo Codes // TDA Progress Report 42–124. Jet Propulsion Laboratory, NASA. 15 February 1996. PP. 63–87. URL: <https://ntrs.nasa.gov/api/citations/19960022223/downloads/19960022223.pdf> (дата обращения 17.05.2024)

Статья поступила 06 июля 2024 г.
Одобрена после рецензирования 16 июля 2024 г.
Принята к публикации 22 июля 2024 г.

Информация об авторах

Цап Всеволод Владимирович — студент 4-го курса факультета радиотехнологий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.
E-mail: vsevolodcap@gmail.com

Фокин Григорий Алексеевич — доктор технических наук, доцент, профессор кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. E-mail: fokin.ga@sut.ru

Development and Testing of LTE Signal Analyzer Using Software-Defined Radio

V. Tsap ✉, G. Fokin

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

The purpose of the work is software implementation and experimental testing of an LTE standard signal analyzer using a software-defined radio for positioning with the accuracy of cell coverage. **Result:** software has been developed for a signal analyzer of the LTE standard in MATLAB, which implements the reception, processing and extraction of the necessary blocks of system information that is transmitted by base stations of the LTE standard via broadcast channels; the interface is configured to work with the USRP B210 board; during experimental testing, system information blocks were received and processed from the radio air, extracting identifiers of operator base stations and then accessing the OpenCellID open database to obtain global coordinates. **Novelty:** from the analysis of open Russian sources, it follows that this study is the first work that describes in detail the procedure for analyzing broadcast signals of the LTE standard to determine the location of an SDR device that is not a network subscriber. **Practical significance:** a software implemented and experimentally tested signal analyzer of the LTE standard allows to determine the location of a user who is not a subscriber to any network, accurate to belonging to the nearest cell in conditions of inaccessibility of global navigation satellite systems.

Key words: LTE standard, software defined radio, integrated development environment MATLAB, system information, positioning

Information about Authors

Tsap Vsevolod — a 4th Year Student of Faculty of Radio Communication Technologies (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E-mail: vsevolodcap@gmail.com

Fokin Grigoriy — Doctor of Engineering Sciences, Associate Professor, Professor of the Department of Radio Communications and Broadcasting (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E-mail: fokin.ga@sut.ru