УДК 621.391.16

ИССЛЕДОВАНИЕ СЕТИ GSM С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ SDR

© 2018 А. В. Туровский, А. С. Стешковой, Р. С. Милованов

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (ВУНЦ ВВС, г. Воронеж, Россия)

В статье проведено исследование пропускной способности беспроводной сетей GSM (900) с применением программно-определяемого радиоприёмного передающего устройства HackRF One.

Ключевые слова: беспроводная связь, компьютерная сеть.

Территориально распределенные системы на основе беспроводных сетей завоевали широкое применение в быту и служебной деятельности. К ним можно отнести автоматизированные системы контроля, охранно-пожарные сигнализации, системы мониторинга транспортных средств, системы безналичных расчетов и платежей и т. п.

В военно-техническую сферу беспроводные технологии внедряют с целью организации канала связи между образцами военной техники, для передачи данных с робототехнических средств: беспилотных летательных аппаратов, камерам видеонаблюдения и т. д. К используемым для решения таких задач беспроводным сетям можно отнести следующие: Wi-fi, bluetooth, сети GSM и д.р.

Однако, использование общей среды передачи, а также отсутствие четкого периметра сети ведут к росту рисков информационной безопасности. В связи с этим применение беспроводных сетей для передачи критически важных данных определяет дополнительные требования к обеспечению защиты информации. В данной статье описывается использование программно-определяемого радио HackRF One совместно с программными продуктами GNU Radio и Wireshark для перехвата, декодирования и анализа трафика сети GSM.

Программно-определяемое радио (SDR) – радиотехническое устройство цифровой обработки радиосигналов, которое реализует использование программного обеспечения вместо обычных аппаратных средств (смесителей, усилителей, модуляторов). На рисунке 1 представлен внешний вид HackRF One.

В качестве антенны выступает вибратор. Устройство обладает антенным SMA разъемом, что дает возможность установить антенну с более высоким КПД для требуемого диапазона частот. Принятый антенной сигнал поступает на антенный переключатель. Сигнал в зависимости от назначения распределяется между тремя портами. После этого сигнал поступает на усилитель MGA81563, который обеспечивает хороший коэффициент усиления и низкий уровень шума. Усиленный сигнал поступает на широкополосный синтезатор, который является устройством преобразования частоты с фазовой автоматической подстройкой. Синтезатор объединен с внешними контурными фильтрами, которые разбивают рабочий частотный диапазон HackRF One на три диапазона. За синтезатором следует широкополосный передатчик прямого преобразования MAX2837. Этот элемент интегрирует все схемы, необходимые для реализации радиочастотного приёмопередатчика. Следующим элементом блок схемы является микросхема MAX5864. Она содержит в себе двойной 8-битный аналого-цифровой преобразователь и двойной 10-битный цифро-аналоговый преобразователь, обеспечивает высокую динамическую производительность при низком энергопотреблении. Также, MAX5864 содержит в себе аналоговые усилители сигнала. После оцифровки сигнал поступает в микроконтроллер LPC43xx ARM. Данный микроконтроллер разработан для мобильных устройств, работает на частоте до 204 МГц, имеет 32-разрядное процессорное ядро, которое обеспечивает низкое энергопотребле-

Стешковой Анатолий Сергеевич – ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина», сотрудник, tttt_sttesh90@mail.ru.

Туровский Алексей Владимирович – ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина», сотрудник, tttt_turivkiy45@mail.ru.

Милованов Р. С. – ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина», сотрудник, tttt_milovv_yu76@mail.ru.

ние. Далее сигнал передаётся по USB на компьютер. Весь тракт приёма (передачи) от антенны до микросхемы MAX5864 ADC/DAC является трактом обработки основной и промежуточной полосы частот. Цифровым этапом обработки являются микросхема MAX5864 ADC/DAC и микроконтроллер LPC43xx ARM.

Рисунок 1. Внешний вид HackRF One.

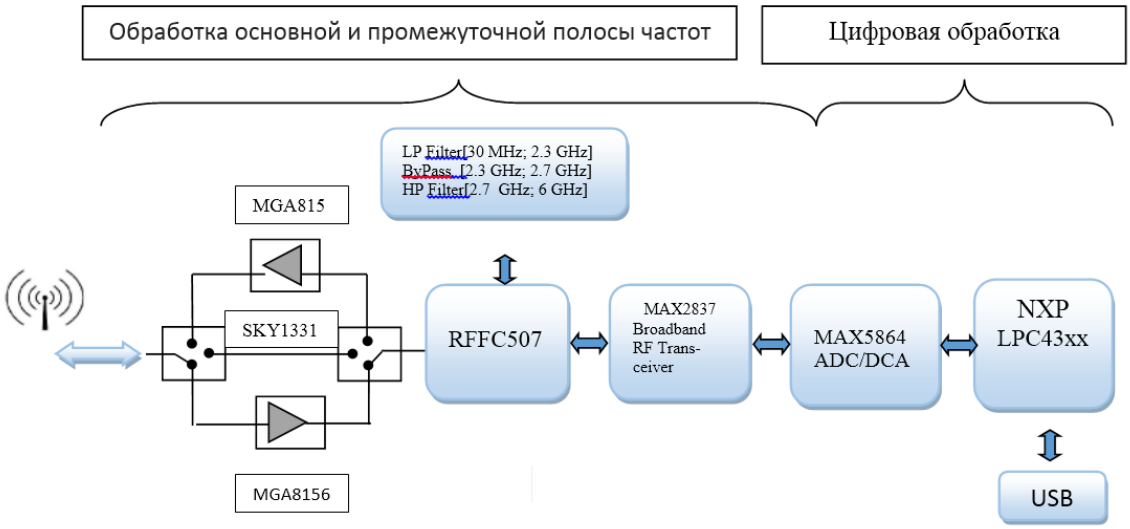

Рисунок 2. Основные элементы структурной схемы устройства HackRF One.

Основные элементы структурной схемы устройства изображены на рисунке 2.Данное устройство обладает следующими основными техническими характеристиками: диапазон рабочих частот от 30 МГц до 6 ГГц, частота дискретизации до 20 МГц, полудуплексный режим работы, питание по шине USB, программное управление мощности порта антенны (max 50 мА при напряжении 3,3 В).

Устройство HackRF One предоставляет широкий набор программного обеспеченья для работы с радиоустройствами, а также поддержку программы gr-osmosdr, которая позволяет использовать HackRF One в связке с многофункциональным обработчиком сигналов GNURadio. В поддерживаемые диапазоны частот попадает практически всё многообразие используемых технологий беспроводной передачи данных, от обычного FM-радио до Wi-Fi и популярного в настоящее время LTE. Формально устройство HackRF One может передать любые сигналы в пределах своей полосы пропускания, например, зная протокол передачи данных, можно управлять радиоуправляемой машиной.

Для обработки принятого сигнала используется программа GNU Radio. GNU Radio — это открытый и бесплатный пакет программ, предназначенный для цифровой обработки сигналов. Система состоит из большого числа готовых блоков, имеющих интерфейс на языке Питон, сами блоки написаны на C++. В GNU Radio входит также визуальный редактор GNURadio Companion, позволяющий визуально соединять блоки в готовое “устройство”, вообще не используя

язык программирования. Пакет программы GNU Radio предназначен для обработки данных, полученных от радиоприемника, в реальном времени. Являющаяся стандартом де-факто для всех профессиональных экспериментов в области радиотехники, программа построена на модульной основе с учетом парадигмы объектно-ориентированного программирования. Это настоящий радиоконструктор, в котором роль элементов отведена функциональным блокам: фильтрам, модуляторам/демодуляторам и множеству других примитивов обработки сигналов. Таким образом, имеется возможность составить из них практически любой тракт обработки. Программный продукт может быть использован совместно с другими программными пакетами, такими как AirProbe для выполнения низкоуровневых функций GSM, таких как приём и демодуляция трафика [1].

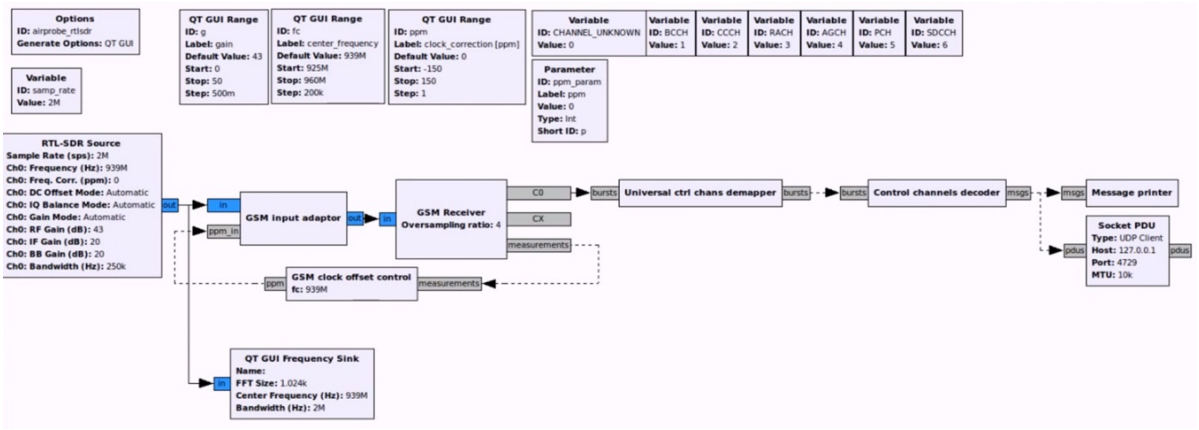

Рисунок 3. Окно программы GNU Radio.

Для мониторинга и анализа трафика GSM используется проект GR-GSM, которая расширяет GNU Radio и использует AirProbe в качестве модуля для работы с GSM. Также понадобится программа анализатор протокола для компьютерных сетей – Wireshark. Программа Wireshark определяет структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

В окне программы GNU Radio Companion приведена схема, которая декодирует принятый от HackRF One сигнал и передаёт его в анализатор трафика Wireshark. Окно программы представлено на рисунке 3. Здесь основными блоками являются: GSM приёмник, понижающий блок частоты дискретизации, канал обратного преобразования [2].

В среде интернет-сообществ, популярных научно-технических изданиях, а также разговорной речи профессиональных работников можно встретить выражения «*3D*-печать», «*3D*-принтер» или «*3D*-принтинг», их тоже можно рассматривать как синонимы.

Основная идея AF-технологий заключается в том, что происходит послойное построение (синтез) изделий – модели, формы, мастер-модели и др. на основе того, что фиксируются слои модельных материалов и осуществляется их последовательное соединение между собой при помощи разных способов: спекание, сплавление, склеивание, полимеризация, в зависимости от особенностей конкретных технологий.

Помимо того, что есть очевидные преимущества в скорости, а часто, в стоимости формирования изделий, такие технологии характеризуются важным достоинством при охране окружающей среды, например, в задачах эмиссии парниковых газов и «тепловом» загрязнении.

На начальном этапе декодирования GSM сигналов формируется график спектра мощности сигнала, по графику необходимо найти постоянные каналы передачи GSM трафика. Вид спектра мощности сигнала представлен на рисунке 4.

В процессе декодирования в нижней части интерфейса программы GNU Radio отображаются символы сигнала GSM. Процесс декодирования представлен на рисунке 5.

Для анализа декодированного сигнала запускается программа Wireshark. Эта программа позволяет представить в доступном для пользователя виде полученные пакеты сети GSM, содержащие следующую инфор-

мацию: размер пакета в битах, версию протокола, время начала следования кадра и др. Стоит отметить, что в процессе перехвата и декодирования трафика GSM, была получена только служебная информация о структуре пакета, их количестве и длительности. Окно программы Wireshark представлено на рисунке 6.

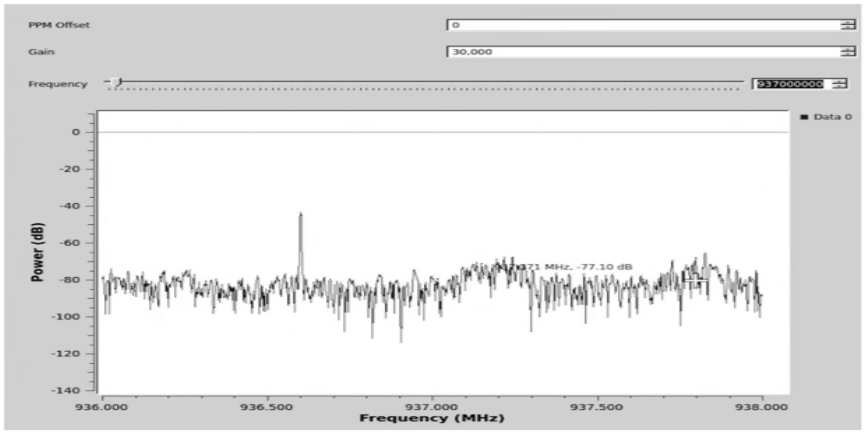

Рисунок 4. Спектр мощности сигнала.

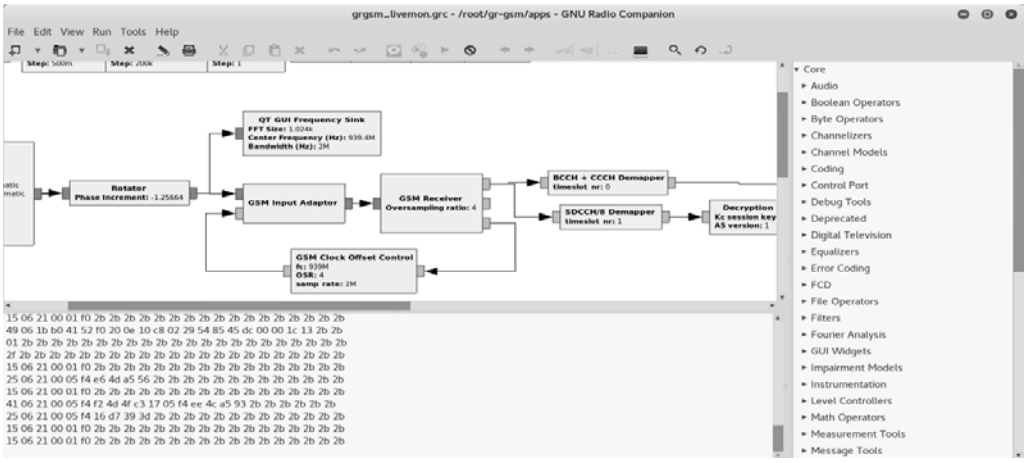

Рисунок 5. Процесс декодирования сигнала.

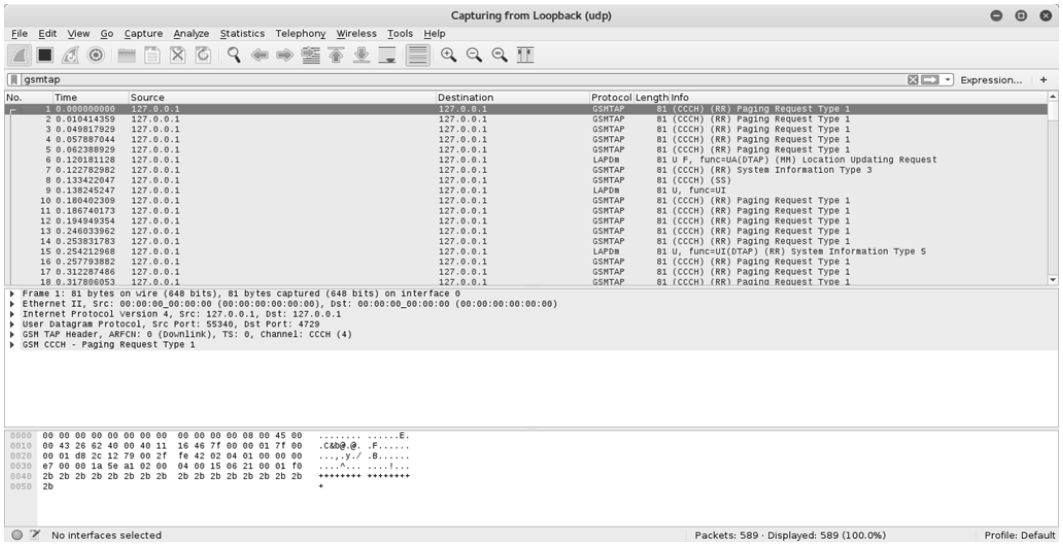

Рисунок 6. Декодированный сигнал GSM в Wireshark.

Таким образом, используя программно-определяемое радио – устройство HackRF One совместно с программными продуктами GNU Radio и Wireshark, был исследован трафик сети GSM. Была получена вся служебная информация о передаваемых данных, такая как: размер пакета в битах, версия протокола, канал передачи и т. д. Полу-

ченная информация может служить для исследования возможных уязвимостей сети GSM.

ЛИТЕРАТУРА

1. Головинов С. О. Разработка имитатора тракта передачи данных спутникового диапазона / С. О. Головинов, И. Я. Львович, А. П. Преображенский // Вестник Воронежского государственного технического университета. – 2009. – Т. 5. – № 4. – С. 214-217.

2. Головинов С. О. Моделирование распространения миллиметровых волн в городской застройке на основе комбинированного алгоритма / С. О. Головинов, А. П. Преображенский, И. Я. Львович // Телекоммуникации. – 2010. – № 7. – С. 20-23.

3. Головинов С. О. Цифровая обработка сигналов / С. О. Головинов, С. Г. Мирончено, Е. В. Щепилов, А. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 4. – С. 064-065.

4. Закиров Г. Сотовая связь стандарта GSM. Современное состояние, переход к сетям третьего поколения. / Г. Закиров, А. Ф. Надеев, Р. Р. Файзуллин. // Издательство: Эко-Трендз, 2004. – 264 с.

5. Кульнева Е. Ю. О характеристиках, влияющих на моделирование радиотехнических устройств / Е. Ю. Кульнева, И. А. Гащенко // Современные наукоемкие технологии. – 2014. – № 5-2. – С. 50.

6. Преображенский А. П. САПР современных радиоэлектронных устройств и систем / А. П. Преображенский, Р. П. Юров // Вестник Воронежского государственного технического университета. – 2006. – Т. 2. – № 3. – С. 35-37.

7. Милошенко О. В. Методы оценки характеристик распространения радиоволн в системах подвижной радиосвязи / О. В. Милошенко // Вестник Воронежского института высоких технологий. – 2012. – № 9. – С. 60-62.

8. Мишин Я. А. О системах автоматизированного проектирования в беспроводных сетях / Я. А. Мишин // Вестник Воронежского института высоких технологий. – 2013. – № 10. – С. 153-156.

9. SDR с GNU Radio [Электронный ресурс] // URL: http:// http://gnuradio.ru/ru/ (Дата обращения: 0.02.2018).

THE INVESTIGATION OF GSM USING THE TECHNOLOGY OF SDR

© 2018 A. V. Turovskiy, A. S. Steshkovoy, R. S. Milovanov

Military training and research center of the air Force «Air force Academy prof. E. Zhukovsky and Y. Gagarin» (VUNTS VVS VVA, Voronezh, Russia))

The investigation of the wireless network bandwidth GSM (900) with the use of software-defined radio-transmitting device HackRF one.

Key words: wireless communication, computer network.