КР "Анализ проектов построения базовых станций стандартов GSM/UMTS с открытым кодом". Часть 3

Симонова Юлия, 14 апреля 2016г.

В третьей части курсовой работы будет рассмотрено назначение модуля Airprobe, его настройка и работа программного модуля в связке с приёмником RTL-SDR. Стоит отметить, что все действия будут производиться в операционной системе Linux xubuntu (для этого можно воспользоваться программой VMware Workstation - она позволит установить на ПК виртуальную машину).

Airprobe - программное обеспечение для декодирования сигналов GSM. Для его установки необходимо открыть окно терминала и набрать следующие команды:

```
git clone git://git.gnumonks.org/airprobe.git;
cd airprobe/gsmdecode;
./bootstrap;
./configure;
make;

cd airprobe/gsm-receiver;
./bootstrap;
./configure;
make;
```

При наличии программы Wareshark и приёмника RTL-SDR можно "поймать" сигнал на частотах GSM 900.

Рисунок 8 - Приёмник RTL-SDR

Для начала следует определить наиболее устойчивый сигнал от ближайших базовых станций. Это можно сделать двумя способами: перебирая частоты вручную, либо воспользоваться модулем kalibrate-rtl. Для его установки в окне терминала потребуется набрать следующие команды:

```
./sdr git clone https://github.com/steve-m/kalibrate-rtl;
./bootstrap && CXXFLAGS='-W –Wall-O3';
```

./configure;
make;
make install;

Затем, используя команду

kal -s 900

приёмник просканирует все частоты стандарта GSM 900, после чего выведет на экран их частоту и мощность.

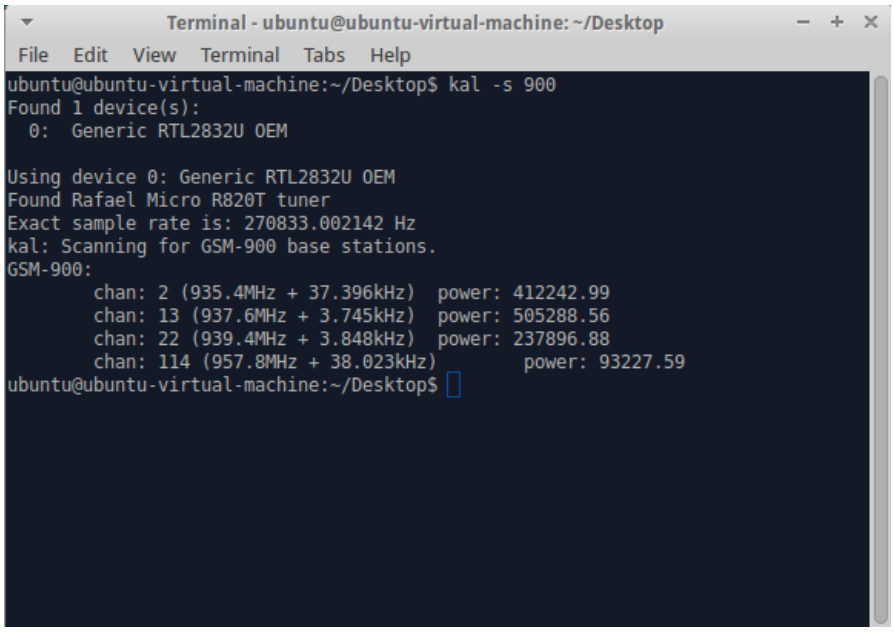

Рисунок 9 - Сигналы GSM 900

Далее следует выбрать подходящую частоту - канал с максимальной мощностью (параметр "power'). Этот модуль также поможет откалибровать приёмник: для этого необходимо в окне терминала прописать команду

kal -c N

где N - номер выбранного канала (параметр "chan").

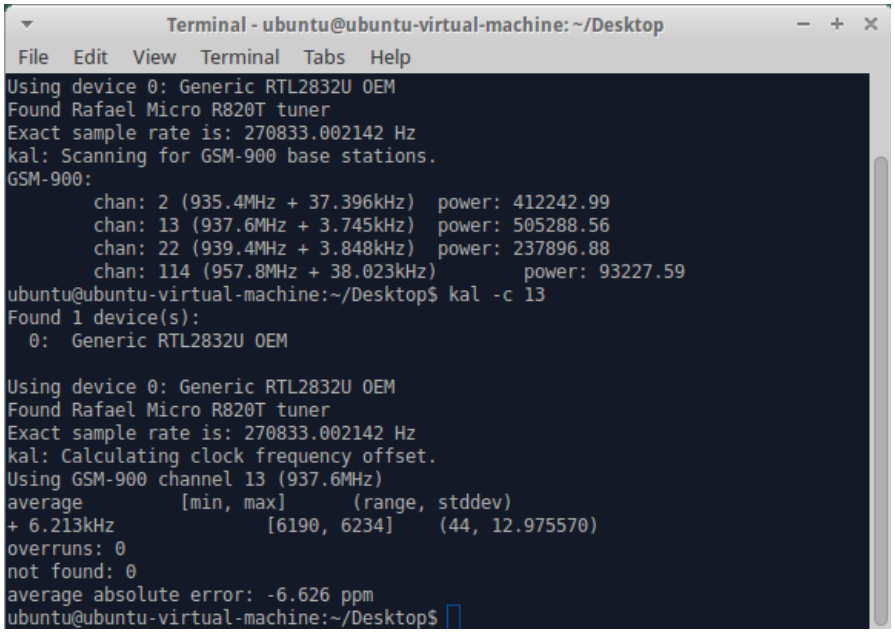

Рисунок 10 - Калибровка 13-го канала

После выполнения этой команды в окно терминала будет выведена оценка рассогласования приёмника по частоте в ppm (Part Per Million или единица на миллион).

Следующим этапом будет получение канала в реальном масштабе времени. Запустим Wareshark с

правами администратора командой

sudo wareshark

После этого откроется соответствующая программа, которую будет необходимо настроить: выбрать интерфейс Loopback: lo и запустить, а затем в открывшемся окне в поле фильтра прописать !icmp && gsmtap - это позволит отображать только данные GSM.

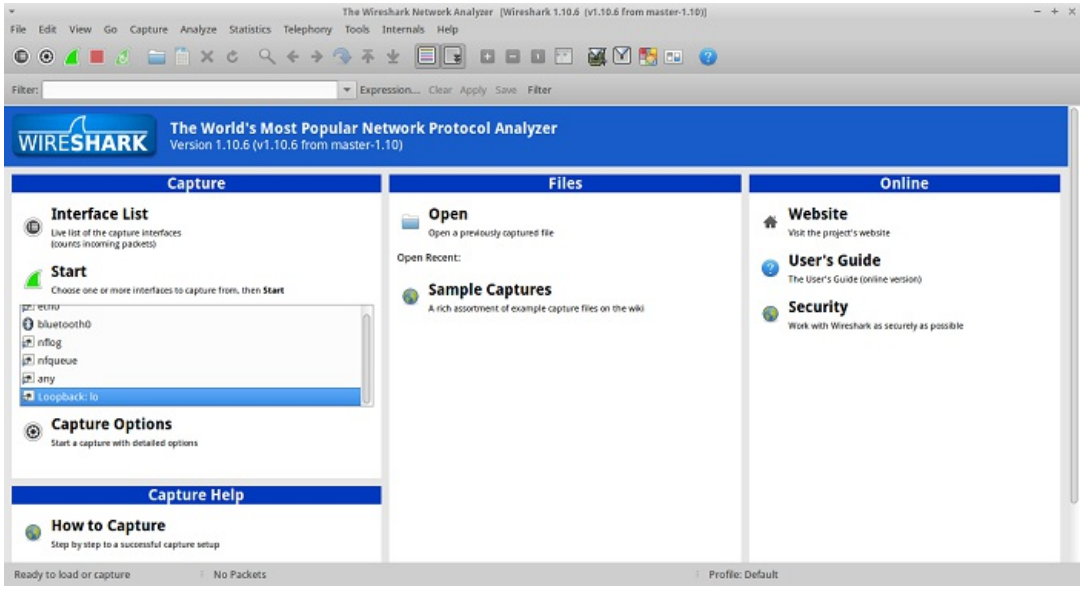

Рисунок 11 - Интерфейс Wireshark

Для версии GNURadio 3.7 стоит воспользоваться командой:

cd home/ubuntu/Install/gr-gsm/apps
./airprobe_rtlsdr.py

После этого откроется модуль Airprobe rtlsdr, в котором сможем наблюдать спектр сигнала.

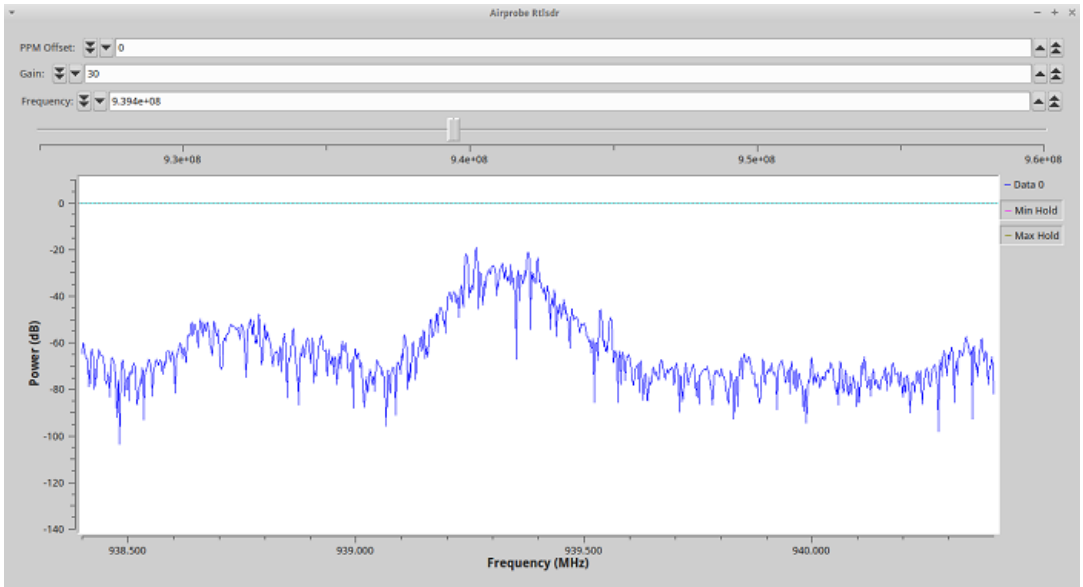

Рисунок 12 - Спектр сигнала

Двигая ползунок настройки частоты добьёмся перехвата системного сообщения: в терминале появится декодированный поток данных в шестнадцатеричном представлении, а в программе Wireshark он распределится по своему назначению.

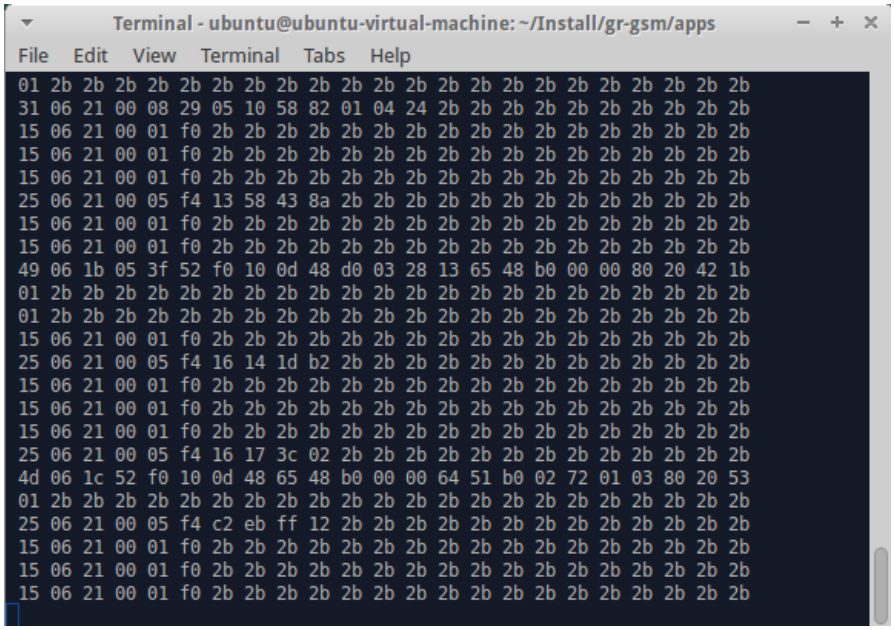

Рисунок 13 - Декодированный поток данных в шестнадцатиричном представлении

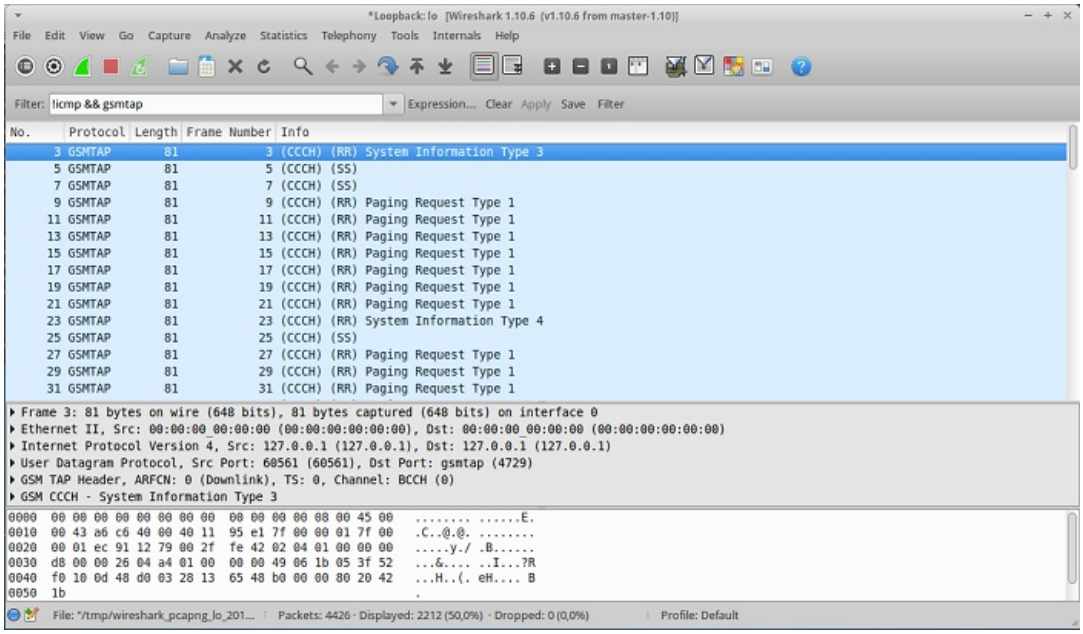

Рисунок 14 - Декодированный поток данных в Wireshark

В данной части статьи было рассмотрено назначение модуля Airbrobe, а так же выполнена практическая реализация работы этого модуля в связке с приёмником.

Список литературы:

1. RTL-SDR Tutorial: Analyzing GSM with Airprobe/GR-GSM and Wireshark
2. Прослушивание сетевых сообщений системы стандарта GSM. Часть 3