Secure Systems & Network Engineering

Advanced Security

Lab 5 GSM SDR sniffer

Grebennikov Sergey, Fofanov Dmitry

February 7, 2018

Introduction

GSM (**G**lobal **S**ystem for **M**obile communication) is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

Figure 1 illustrates a simplified GSM network architecture. It consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces.

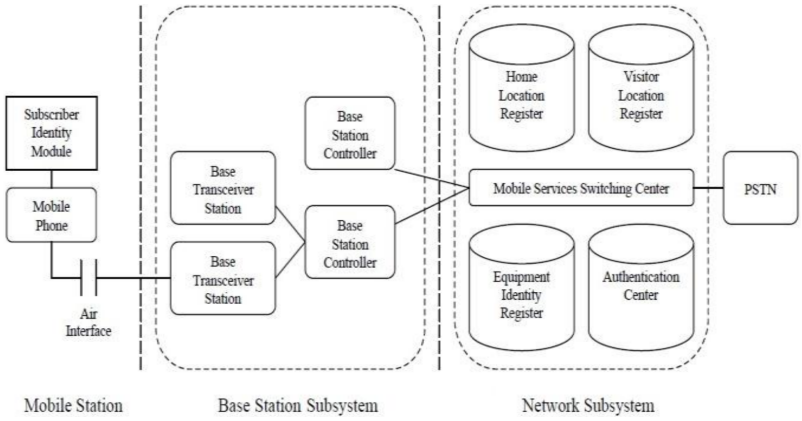

Figure 1: GSM network architecture

The subsystems are:

- Base Station Subsystem (BSS):
  - Mobile Station (MS): Mobile equipment (ME), Subscriber Identity Module (SIM)
  - Base Transceiver Station (BTS)
  - Base Station Controller (BSC)
- Network and Switching Subsystem (NSS):
  - Mobile Switching Center (MSC)
  - Home Location Register (HLR)
  - Visitor Location Register (VLR)
  - Gateway Mobile Switching Center (GMSC)
- Operation Support Subsystem (OSS):
  - Authentication Center (AuC): International Mobile Subscriber Identity (IMSI), Permanent key associated with every SIM (Ki)
  - Equipment Identity Register (EIR): International Mobile Station Equipment Identity (IMEI)

Using an RTL-SDR to receive GSM traffic we can sniff these packages an analyze it. The most complicated part of the task is to pick the right signal frequency and and to capture the broadcast data from the base station.

Main Part

Question 1

How can you receive GSM traffic using the an SDR?

Answer

First, it is required to find out at what frequencies we have GSM signals in our area. For most of the world, the primary GSM band is 900 MHz. There are two GSM standards (GSM-900 and GSM-1800) in Europe and Asia.

GSM-900. The digital standard of mobile communication in the frequency range from 890 to 915 MHz (from the phone to the base station - **uplink signal**) and from 935 to 960 MHz (from a station to the telephone - **downlink signal**).

GSM-1800. Modification of the GSM-900 standard, the digital standard of mobile communication in the frequency range from 1710 to 1880 MHz.

Beginning with the RTL-SDR we have to install the **Kalibrate** utility. *Kalibrate* is a useful tool that enables us to identify the available principal GSM channels in our area. (Figure 2)

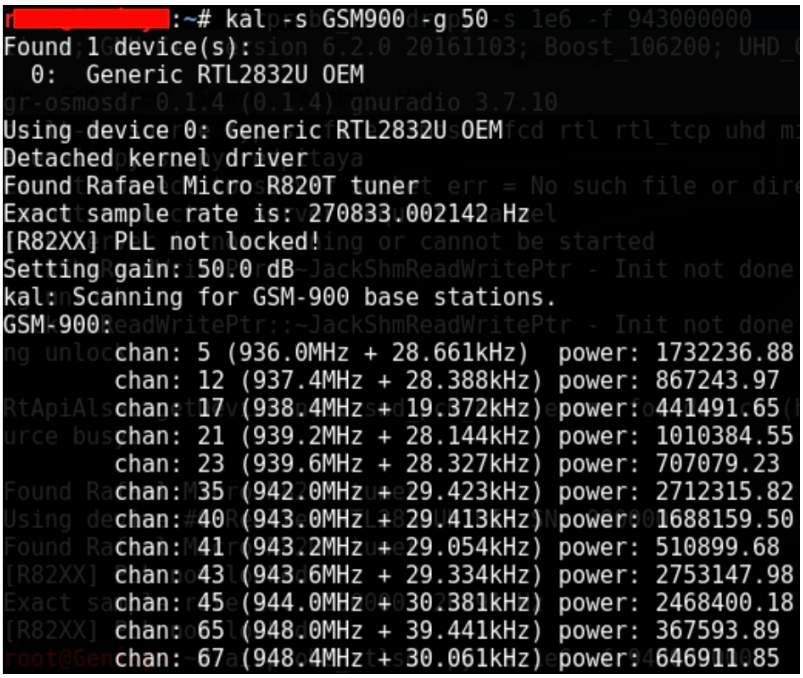

Figure 2: Scanning BTS Frequencies

The **SDRSharp** application can be used to detect GSM traffic on the certain frequency using the RTL-SDR dongle. For example, this application scan the 936.375MHz band for a signal that looks like the waterfall image below (Figure 3). This is a non-hopping GSM downlink signal.

These are the frequencies that we have to tune with our RTL-SDR dongle to start receiving the downlink GSM traffic generated from a specific BTS. From that purpose we have to execute **grgsm_livemon** python script included in the **GR-GSM** library. The *grgsm_livemon* decodes in realtime C0 GSM channel selected by the user. C0 channel is transmitted by every BTS and carries synchronization information, configuration of the cell and user data (such as short messages and voice). The program uses cheap RTL-SDR receivers as a source of the signal. In order to have better results regarding the captured traffic it is better to use the frequency with the best power (HZ). Now we execute the python script by command

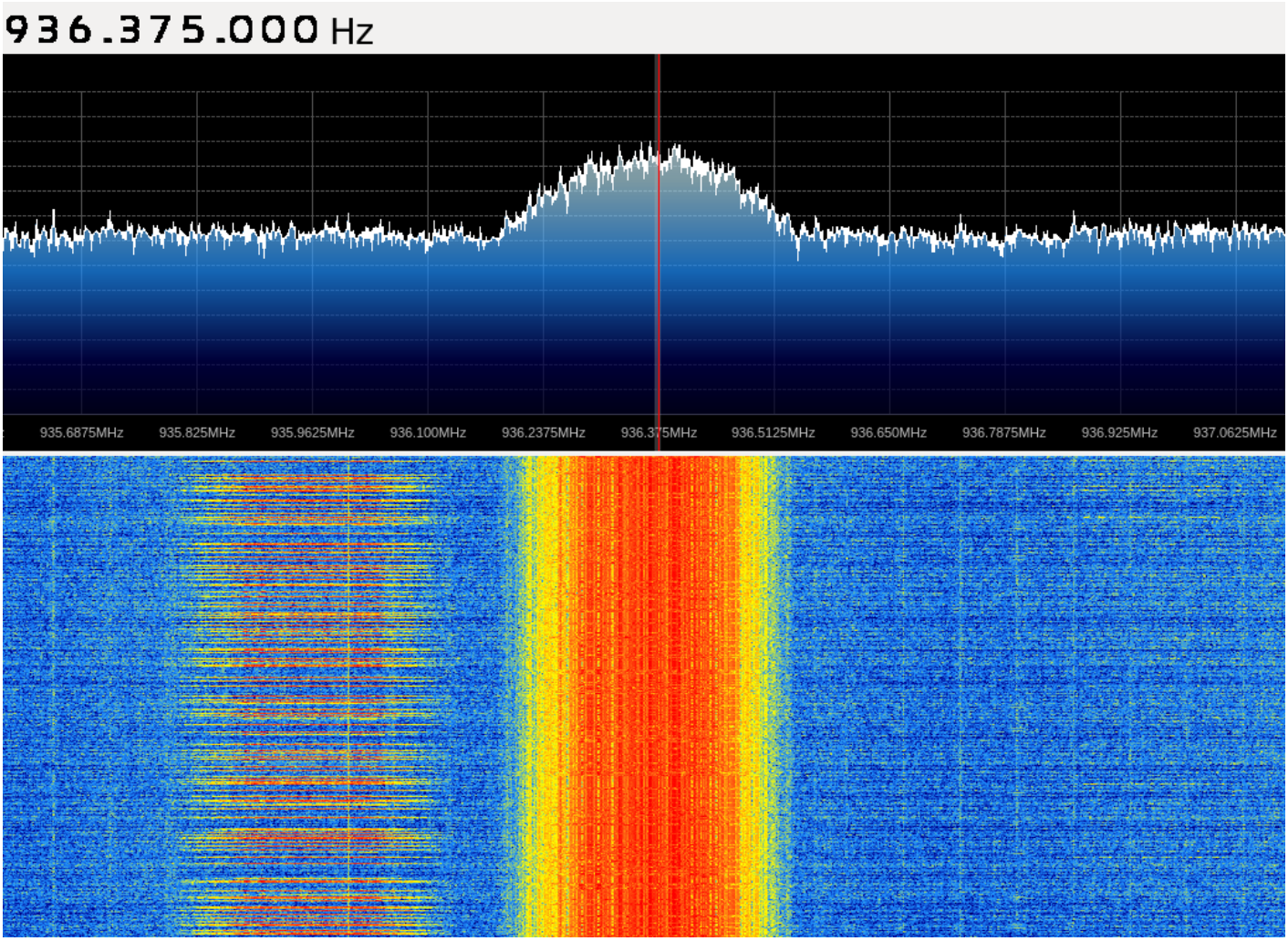

Figure 3: GSM traffic using the SDRSharp application

```
$ grgsm_livemon -f 936.375M
```

Here we choose 953 MHz frequency. Then data in hex-format will be retrieved (Figure 4).

Figure 4: Retrieving GSM information

Alongside (Figure 5) , we start **Wireshark** on a new terminal window. *grgsm_livemon* dumps data into a UDP port, so we had to set *Wireshark* to listen to this by the following command:

```
$ sudo wireshark -k -Y '!icmp && gsmtap' -i lo
```

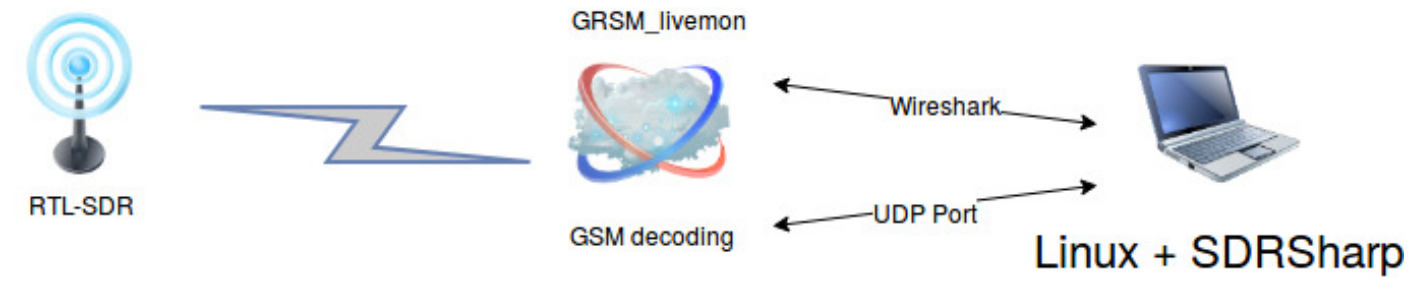

Figure 5: Operation of RTL-SDR

Wireshark allows detecting packets that operate on the following two protocols: GSMPTAP and LAPDm. (Figure 6)

GSMTAP is a pseudo-header that is used to transport frames from the GSM air interface (Um interface) inside UDP/IP packets. A pseudo-header is an additional header in front of a protocol message, which is not part of the actual protocol.

LAPDm is a modified version of LAPD (Link Access Protocol in the D channel), the Data link layer protocol. It is used in GSM to support the transport of information between the mobile and the network. Stopping the *grgsm_livemon* we continue with the analysis of the packet capture files.

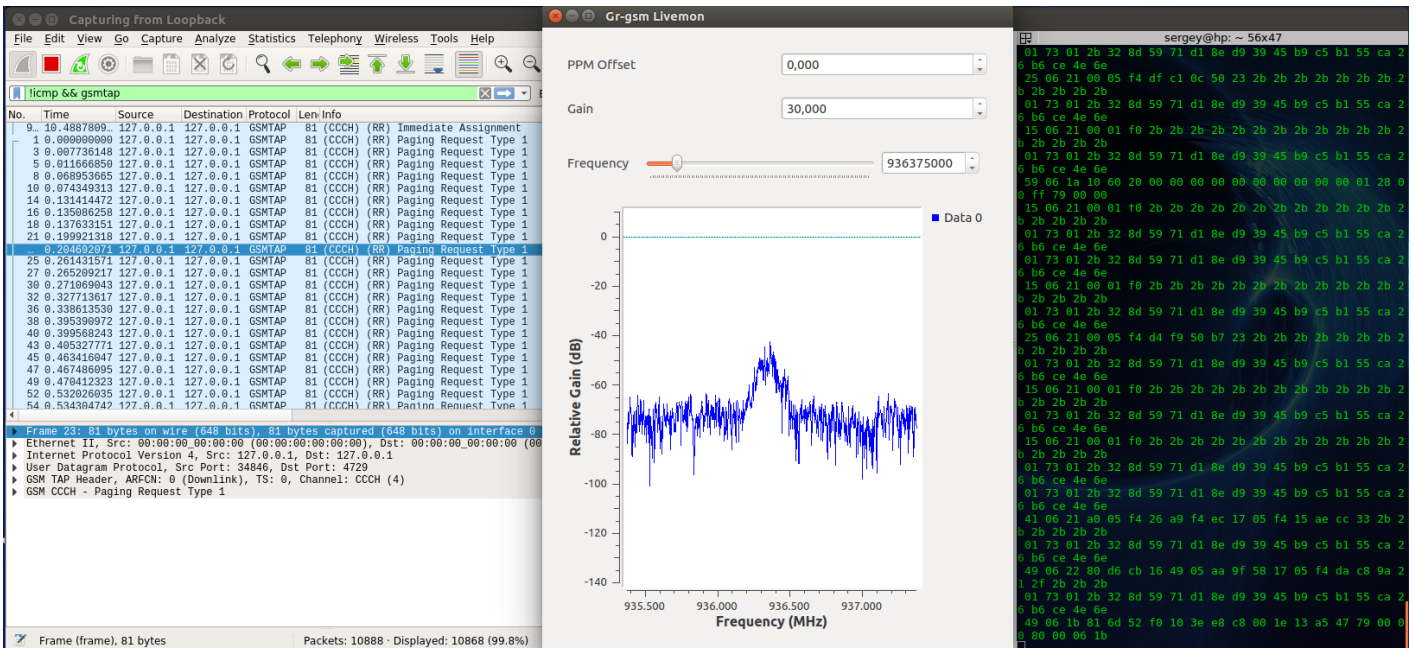

Figure 6: Retrieving GSM live traffic

Question 2

What information can be retrieved?

Answer

As we observe from the screenshots (Figure 6), packets transmitted from BTS to different MSs named as **Paging Request** (Figure 8) or **System information** (Figure 9), each one of this contains different information. The system information messages describe the identity, configuration and available features

of BTS that can be retrieved by analyzing a **broadcast control channel** (**BCCH**). These messages also provide a list of **absolute radio-frequency channel numbers** (**ARFCNs**) used by neighboring BTSs. The BCCH is a point to multipoint, unidirectional (downlink) channel used in the **Um** interface of the GSM cellular standard. The Um interface is the air interface between the **mobile station** (**MS**) and BTS. Um is defined in the lower three layers of the OSI model. (Figure 7)

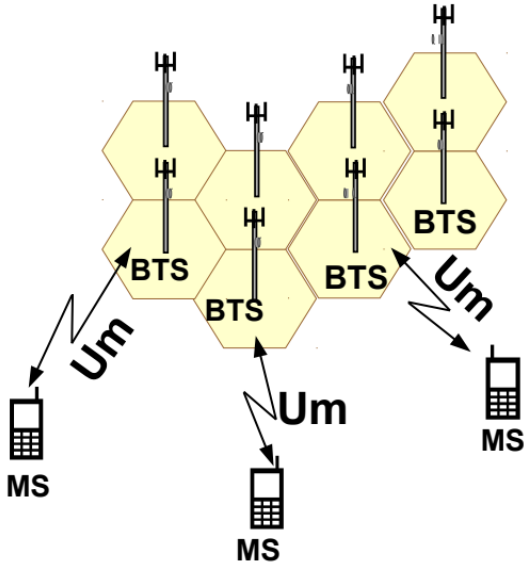

Figure 7: The interconnection between BTS and MS

Here is a brief analysis from each one of the captured messages:

System Information Message

Generally this type of message contains the info that MS needs in order to communicate with the network. As we can see there are different types of such messages each one contains various piece of information.

- **Type 1:** Channel type = BCCH: Contains a list of ARFCN(Absolute Radio Frequency Channel Number)s of the cell and RACH control parameters.
- **Type 2:** Channel type = BCCH: Contains neighbor cell description (list of ARFCNs of the cell) and BCCH frequency list.
- **Type 3:** Channel type = BCCH: Contains cell identity (cell ID) code decoded, Location Area Identity-LAI(which involves Mobile Country Code (MCC), Mobile Network Code (MNC) and Location Area Code (LAC)) and some GPRS information.
- **Type 4:** Channel type = BCCH: Contains LAI (MCC+MNC+LAC) decoded, Cell selection parameters and RACH control parameters. Some GPRS information too.
- **Type 2ter:** Channel type = BCCH: Contains neighbor cell description (list of ARFCNs of the cell) with Extended BCCH frequency list.
- **Type 2quater:** Channel type = BCCH: Is 3G message with information that we dont take into account in this study. Contains 3G-neighbor cell description.

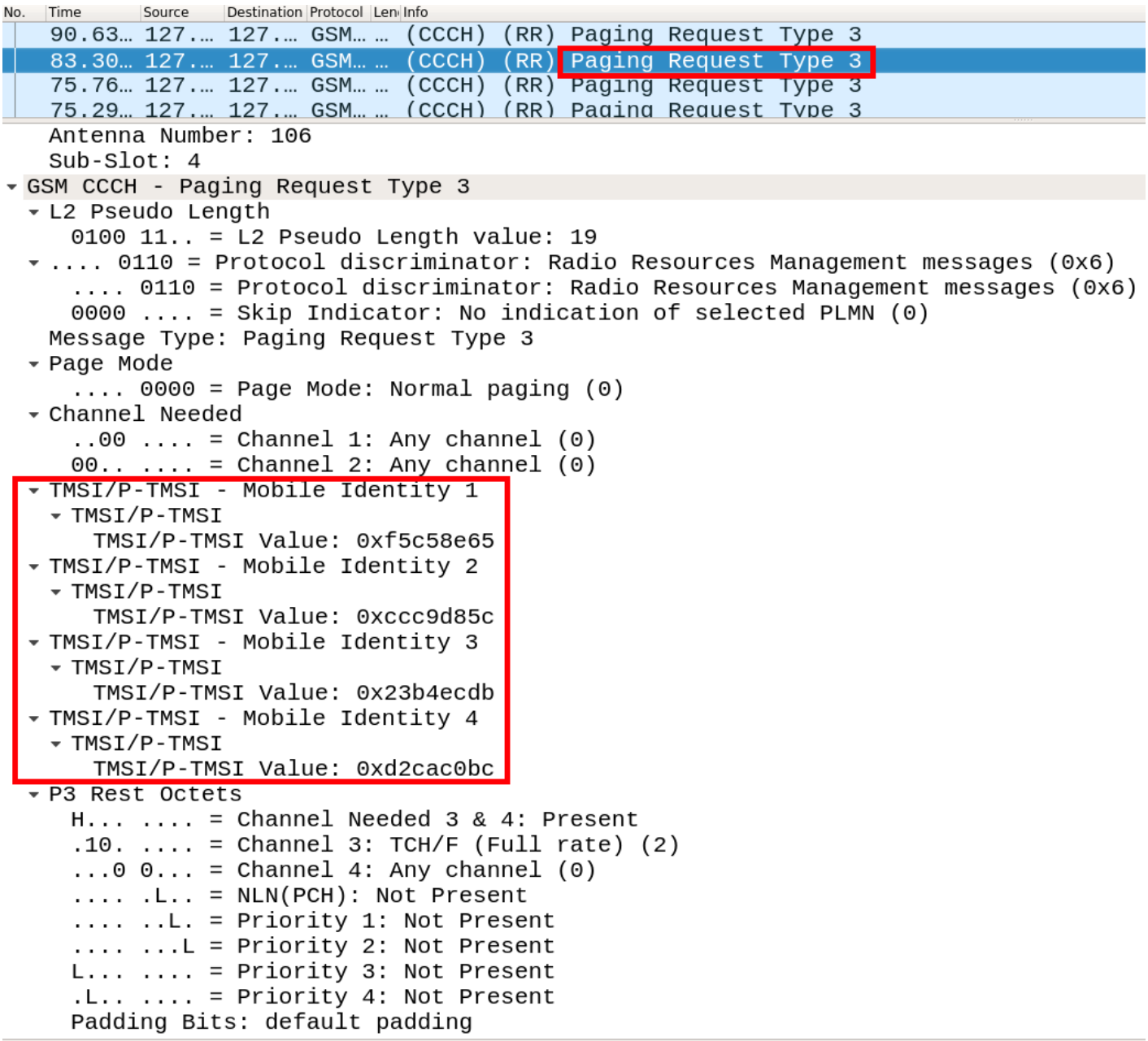

Figure 8: Paging Request package

- **Type 13:** Channel type = BCCH: They contain all the important information about GPRS like GPRSCell options and GPRS power control parameters.

Paging Request Message

- **Type 1:** Channel type = CCCH
  Contains: Mobile Identity 1 number (IMSI)
  Page Mode = normal paging (P1)
  Channel Needed.
  Contains: Mobile Identity 1 and 2 = TMSI/P-TMSI
  Page Mode = normal paging (0)
  Channel Needed

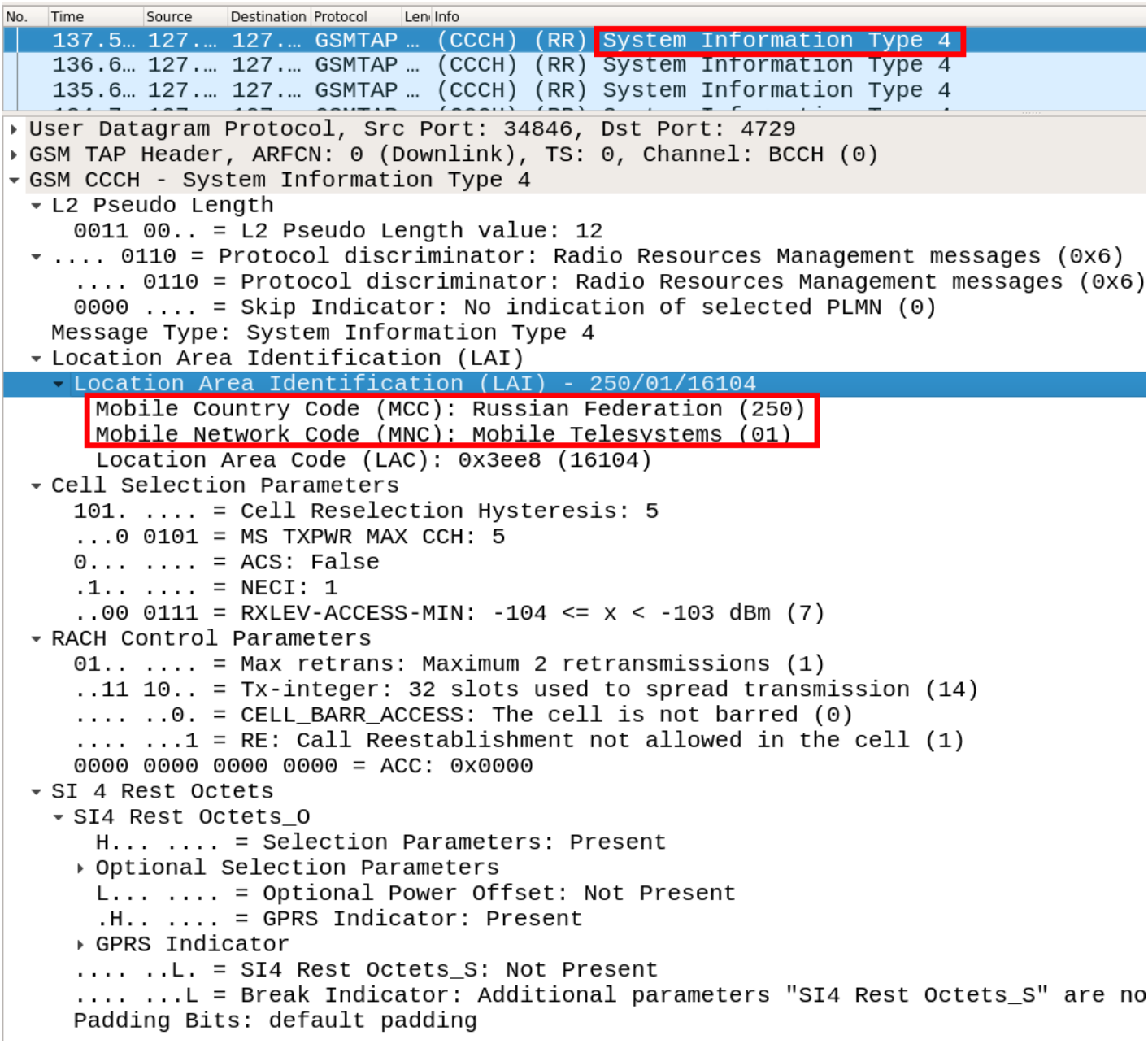

Figure 9: System Information package

- **Type 2:** Channel type = CCCH
  Contains: Mobile Identity 1, 2 = TMSI/P-TMSI or IMSI Mobile Identity 3
  Page Mode = normal paging (0)
  Channel Needed

- **Type 3:** Channel type = CCCH
  Contains: Mobile Identity 1, 2, 3 and 4 = TMSI/P-TMSI (Not decoded)
  Page Mode = normal paging (0)
  Channel Needed

Immediate Assignment Message

Channel type = CCCH
Contains: Time Advance Value
Packet Channel Description (Time Slot)
Page Mode = Extended Paging (1)

As we can show in Figure 9 and Figure 8, it gives the IMSI, TMSI, Cell Id, LAI, MCC, MNC, LAC, etc.

IMSI actually represents the unique identity for the subscriber of the phone including the origin country and mobile network that the subscriber subscribes. It basically identifies the user of a cellular network and every cellular network has its own unique identification. Basically, all GSM networks use IMSI as the primary identity of a subscriber or user. The number that represents IMSI can be as long as 15 digits or shorter. The first three digits are the mobile country code (MCC) and followed by the mobile network code (MNC). The information of IMSI is also contained in the SIM card. IMSI are normally used by network operator to examine the subscribers and whether to allow the subscriber to use another network operator. By tracking your IMSI, the authority can actually track not just the location of your phone but also who you are calling, at what time and where the call is made.

Each location area of a public land mobile network (PLMN) has its own unique identifier which is known as its location area identity (LAI). This internationally unique identifier is used for location updating of mobile subscribers. It is composed of a three decimal digit mobile country code (MCC), a two to three digit mobile network code (MNC) that identifies a Subscriber Module Public Land Mobile Network (SM PLMN) in that country, and a location area code (LAC) which is a 16 bit number thereby allowing 65536 location areas within one GSM PLMN.

The LAI is broadcast regularly through a broadcast control channel (BCCH). A mobile station (e.g. cell phone) recognizes the LAI and stores it in the subscriber identity module (SIM). If the mobile station is moving and notices a change of LAI, it will issue a location update request, thereby informing the mobile provider of its new LAI. This allows the provider to locate the mobile station in case of an incoming call. So we can say that this information are very sensitive to the privacy and security of mobile phone users.

Question 3

What tools can be used to analyze the GSM traffic?

Answer

Durign the GSM sniffing we were using the GNU Radio module GR-GSM (*grgsm_livemon*) together with *Wireshark* which enabled analysis of live GSM transmission in the Um radio interface.

Along with the software indicated there is a plenty of other programs to perform the task. For instance, Airprobe is a GSM air interface analysis tool that also widely used. Also OsmocomBB software and it's clone named gsm-debug with additional sniffing features.

Results

In this lab we presented an effective attack that can exploit chronic and fundamental vulnerabilities that exist in the GSM cellular technology. RTL-SDR can also be characterized as an IMSI catcher and when combined with some hardware and software can build a mechanism of mobile user tracking. So, systems with broadcast paging protocols can leak location information and the leaks can be observed with the available and low cost commodity hardware.