

Security of GSM Networks

This version has been prepared for either offline use under COVID-19 restrictions or live use in a laboratory.

GSM, the Global System for Mobile Communications, has formed the basis of mobile telecommunication for years. Despite being a 1980's era standard, it still underpins much of our global communications to this day. This lab will give you the opportunity to explore some of its weaknesses on our very own test GSM network, utilising open-source tools to investigate the inner workings of the protocol and the data that flows between devices.

Note 1. Information

The GSM Network data used in this lab was captured at **1878.8 MHz**.

Note 2. Warning

This lab involves decoding data from a live environment. The use of the techniques explored in this laboratory on commercial networks is an offence under the [Wireless Telegraphy Act 2006](#), and can carry severe penalties.

Submission Instructions

For each numbered section in each task, please write what you did, what you learnt, and aim to answer each sub-question, using the provided template. You should aim to write no more than 100 words per numbered section, with a total of around 1000–1200 words. Bullet points or brief sentences are fine; there is no need to write an essay. What matters is the content and the understanding that you are showing.

Task 1 - Understanding GSM

GSM, or the *Global System for Mobile Communications*, is a common standard utilised by mobile phones worldwide. The standard includes a variety of parameters. In order to understand how a particular GSM network works, a variety of parameters must be understood and defined. Answer these questions in your submission:

1. Which frequency bands does GSM use in the UK? From which band is the sample capture you have been given?
2. What is an ARFCN? Which ARFCN was the capture from in this laboratory? (See Note 1)
3. What channel access method is typically used for GSM networks?
4. What encryption methods are available as part of the GSM Standard?
5. Which of these are able to be “cracked” using reasonably accessible resources?
6. What are the MNC (*Mobile Network Code*) and MCC (*Mobile Country Code*) used for?
7. Which parameters on the SIM Card are used to authenticate a mobile device to a network?
8. What is the difference between an IMEI number and an IMSI number?
9. What is a TMSI number?
10. What does it mean when a mobile device is “Network Locked”?
11. What kinds of information are carried in the *Broadcast Control Channel* (BCCH) of a GSM Cell?
12. What kinds of information are carried in other *Control Channels* (CCCHs) of a GSM Cell?
13. What kinds of information are carried in the *Traffic Channels* (TCHs) of a GSM Cell?

Task 2 - Analysing network parameters

For this task, you will need to utilise the `b.gr_gsm` tools to analyse the broadcast channel on an active GSM cell.

If this exercise is run in the laboratory, you are asked to use the `grgsm_livemon` command with the following arguments:

```
grgsm_livemon -f 1806.0M -s 1e6 --args=driver=lime,soapy=0,antenna=LNAW
```

This command utilises your *LimeSDR Mini* to capture live data from the specified broadcast channel, outputting encapsulated packets over the loopback interface for analysis with compatible software.

If this laboratory is being run offline, you are instead asked to run the following command:

```
grgsm_decode -f 1806.0M -c gsm_capture.cap -v
```

The command `grgsm_decode` utilises a pre-existing capture file rather than a live SDR interface, and has essentially the same functionality as `grgsm_livemon`.

With `grgsm_livemon` running, open *Wireshark*, which a popular network protocol analyser. Select `lo0`, the loopback interface, and you should see a stream of packets appearing from `grgsm_decode`. If you don't see any packets, check that your command is actually completing without errors, and that you can access the `gsm_capture.cap` file.

In Wireshark, you can select different packets from the list and inspect each layer of the captured protocols by expanding the triangle next to each line. If you experience packets of types other than **GSMTAP** appearing in the list, simply add a filter of "`gsmtap`" by typing it in the display filter box at the top of the application.

By exploring the Wireshark analysis of your capture, answer the following questions:

1. What do each of the command line parameters in the above commands do?
2. What signal level (dBm) was received by the SDR which made the capture?
3. In the Cell Channel Description, which ARFCN is advertised for this cell?
4. What Mobile Country Code (MCC) is in use?
5. What Mobile Network Code (MNC) is in use?
6. To what region is this MCC and MNC assigned?
7. What is the minimum signal strength required to join the network?
8. What is the maximum allowed Tx power devices should use when contacting the cell?
9. What is the maximum number of retransmissions allowed by mobile devices?
10. Is call re-establishment allowed by the cell?
11. What is the value of the radio link timeout parameter? What does this parameter mean?

Task 3 - Decoding SMS messages

The infrastructure in this lab has been modified to send a SMS message to a connected mobile device every 30 seconds. In this task, you will interpret captured packets to find the content of this message, and other related information.

The previous task utilised `gr_gsm` to decode packets from a standalone Broadcast Control Channel (BCCH) contained within the capture. This channel contains basic data about the network, and deals with global control parameters. If we want to access data sent to a specific device, we need to look inside the other Control channels (CCCHs).

Control channels can operate in a variety of modes as part of GSM, and we first need to find out the type of control channel used by the network we are inspecting. To do this, you will need to search for an “Immediate Assignment” packet in your capture from `grgsm_decode`, and interpret its contents.

Using the information you gained from investigating the Immediate Assignment packet, modify your `grgsm_decode` command to decode the Control Channel, and find the SMS message sent to the mobile device. To find the TMSI of the device which was sent the Immediate Assignment, you may wish to search the few “Paging Request” packets preceding it.

You may find the `grgsm_decode` help useful:

```
grgsm_decode -h
```

By exploring the Wireshark analysis of your capture, answer the following questions:

1. What does an “Immediate Assignment” message do?
2. What type of control channel is in use in this cell and contains the SMS data? What does the descriptor mean?
3. What is the TMSI of the device the SMS message is intended for?
4. From what phone number did the SMS message originate?
5. What phone number is the intended destination of the SMS message?
6. What is the content of the text message?
7. Is encryption enabled on this GSM Cell? What type of message would answer this question?
8. If A5 encryption were in use, how would you use `grgsm_decode` to decrypt it?
9. If instead we wished to decode a voice call, which arguments would you need to pass to `grgsm_decode` to achieve this?

Task 4 - Extension: Decoding Voice Calls

The mobile device connected to the test cell initiates a voice call every few minutes. This call contains a two-factor authentication code which is spoken by the caller.

You will likely wish to utilise **grgsm_capture** and **grgsm_decode** for this purpose as the call occurs infrequently; this will allow you to attempt multiple methods of decoding your capture without having to listen for the next call.

1. Which channel will need to be captured and decoded to obtain the voice data?
2. If you listen on the frequency in Note 1, will you recover the full (2-way) conversation? If not, which other frequency would you have to listen on?
3. What codec is used to encode the audio?
4. What is the content of the voice message?

Revision History

Version	Date	User	Changes
1.0	2021-07-10	JC	Initial document revision
1.1	2021-07-16	DAN	Language tweaks