Digital Wireless Communication Practical Laboratory Session

WIRELESS COMMUNICATIONS 371-1-1903

SPRING 2020

Part 1 – GSM Sniffing

Description

In this experiment we will use the GSM receiver you've built in your theoretical session to sniff out messages from a base station.

Equipment needed

- 1 Linux PC with GNU Radio installed.
- 1 LimeSDR/USRP Software defined radios.
- 1 SMA GSM band antenna.
- 1 ULF-SMA Adapters.

If any of the above equipment is missing or defective, notify the lab instructor prior to starting this session or otherwise you may obtain false results (and major frustration).

Equipment Setup

- Connect the SDR using a USB3 extension cable.
- Connect 2 antennas to the RX1 ULF connection using the ULF-SMA adapters

Recording

This is a practical session; thus, you most likely do not have this equipment at your disposal at home other than currently, here. Therefor it is highly recommended that you document and record your results during this session. This will assist you in completing you report at home. You may not fully complete what that is required of you during the time you have, take this into account.

Instructions

1. Open your GSM code from the theoretical session and make sure it has no errors on the laboratory computer.
2. Connect the SDR and run your code. If the code isn't working, check for errors and try to fix.
3. After you code is running on your SDR, open Wireshark with root privileges (*sudo wireshark*).
4. In Wireshark choose the **Loopback: lo** in order to listen to your own computer (127.0.0.1).
5. Slowly change the Frequency until you see a "hill in the spectrum", move it to the center of the spectrum. You should see messages stat to flow in Wireshark of the GSMTAP and LAPDm protocols. (This should happen at about 955MHz and/or 1800MHz).
   This means that you are now on some GSM base station frequency and intercepting the messages flowing between the base station and its users.

6. Let the Wireshark record pickup the messages of about 5 minutes. Go and get some coffee or the beverage of your choice. When you return, stop the Wireshark recording and save the .pcapng file. You can also stop the SDR in GNURadio.

Report

Let's use what we've sniffed from the GSM network and try to figure out what was happening while we were out for coffee.

Notice: It is recommended that you answer the following questions at home. Make sure you have recorded and saved the data and that the experiment was successful.

Notice that most of your incoming .pcapng messages are of the Protocol type **GSMTAP**:

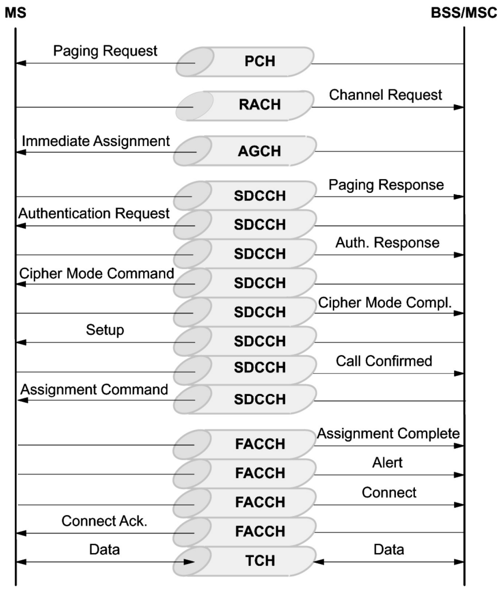
> GSMTAP is a pseudo-header format, used to encapsulate frames from a GSM Um (air) interface into UDP/IP packets. GSMTAP is implemented as Wireshark dissector on UDP port 4729.

The other common type is **LAPDm**:

> LAPDm is a data link layer protocol used in GSM cellular networks. LAPDm forms Layer 2 of the Um interface between the Base Transceiver Station and Mobile station, which is to say that it is used in the radio link between the cellular network and the subscriber handset.

The **Packet Common Control Channel** (PCCCH) transports signaling information for functions of the network access management, i.e. for allocation of radio channels, medium access control and paging.

In the theoretical session we've introduced the connection setup for incoming call.



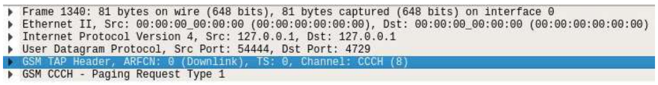
Submit your answers with snapshots and .pcapng to proof of your findings.
A submission without sufficient proof will result in deduction of grade!

1. Check your .pcapng, what messages do you see? Explain.

2. Why doesn't all the messages of the connection setup process exist in the .pcapng?

3. What is the purpose of a Paging Request?

4. Open a Paging Request message (Type 1) and view the GSM TAP Header. What is the antenna number? Open several other Paging Requests, is the antenna number different? Why is that?



```
▸ Frame 1340: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 54444, Dst Port: 4729
▸ GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: CCCH (8)
▸ GSM CCCH - Paging Request Type 1
```

5. Under GSM CCCH try to find the identity of the mobile station that the Paging is addressed to. Write what you find.

The Temporary Mobile Subscriber Identity (TMSI) is the identity that is most commonly sent between the mobile and the network.

The international mobile subscriber identity or IMSI is a number that uniquely identifies every user of a cellular network.

https://en.wikipedia.org/wiki/Mobility_management#TMSI

https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

6. Why is the Identity TMSI and not IMSI?

A random-access channel (RACH) is a shared channel used by wireless terminals to access the mobile network (TDMA/FDMA, and CDMA based network) for call set-up and bursty data transmission. Whenever mobile wants to make an MO (Mobile Originating) call it schedules the RACH. RACH is transport-layer channel; the corresponding physical-layer channel is PRACH.

https://en.wikipedia.org/wiki/Random-access_channel

https://en.wikipedia.org/wiki/GSM_procedures

7. Upon receiving the Paging Request, the Mobile station requests a channel in the Random-access channel. Why does the MS request the channel by Randomly sending a request? What happens if several MSs sent a request at the same time?

8. Open the Immediate Assignment message. What did the base station assign the MS?

https://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317

9. What is the purpose of Authentication?

https://en.wikipedia.org/wiki/Stream_cipher

10. What is the purpose of Ciphering? What is the algorithm you find in the Ciphering Mode Command?

https://payatu.com/dissecting-gsm-encryption-location-update-process/

Location updating accepted – After the successful authentication, location update happens where the MS give its location information to the network.

11. Why does the network need to know the MS location? What if the location changes during a call?

12. Open the Location updating accepted message. What is the location? To which provider the base station belongs?

13. A MS leaves the BSS or the network, which related messages can you locate? What is their purpose?

System Information Types:

System Information Type 1

- cell channel description
- RACH control parameters

System Information Type 2

- neighbor cells description
- PLMN permitted
- RACH control parameters

System Information Type 3

- cell identity
- location area identification
- control channel description
- cell options
- cell selection parameters
- RACH control parameters

System Information Type 4

- location area identification
- cell selection parameters
- RACH control parameters

System Information Type 5

- neighbor cells description

System Information Type 6

- cell identity
- location area identification
- cell options
- PLMN permitted

http://read.pudn.com/downloads161/ebook/733562/GSM/GSM_chap6_System%20Information.pdf

14. Select a System Information message, find 2 information elements that are included in that message and explain its necessity.

References

https://www.etsi.org/deliver/etsi_i_ets/300600_300699/30060902/01_60/ets_30060902e01p.pdf

Part 2– SMS and Voice decryption (Bonus 50%)

Description

In this experiment we will use an SDR to record a transmission from a base station, which will later be used to decrypt SMS and Voice calls.

Equipment needed

- 1 Linux PC with GNU Radio installed.
- 1 LimeSDR/USRP Software defined radios.
- 1 SMA GSM band antenna.
- 1 ULF-SMA Adapters.

If any of the above equipment is missing or defective, notify the lab instructor prior to starting this session or otherwise you may obtain false results (and major frustration).

Equipment Setup

Recording

This is a practical session; thus, you most likely do not have this equipment at your disposal at home other than currently, here. Therefor it is highly recommended that you document and record your results during this session. This will assist you in completing you report at home. You may not fully complete what that is required of you during the time you have, take this into account.

Instructions

1. Record a base station, make sure you record significant amount of data to make sure you capture an SMS or call occurrence. You can later use your recording as a live source.
2. SMS Kraken
   https://www.youtube.com/watch?v=sCwBDIEexqo
3. Voice
   https://www.youtube.com/watch?v=krJJKjYdwgc&t=4s

Good luck!