Cellular and Mobile Communications

**GSM**

# Decoding GSM data in wireshark

In this lab, you’ll have the opportunity to explore a capture of GSM data using Wireshark. You’ll find similarities to the terms we discuss in class to the values that are deep inside of the actual GSM frames. The data captured was live data, however it’s been scrubbed of anything that would actually identify any particular person or phone data. Essentially, you won’t find any TCH channels in this capture.

You may notice that the GSM Tap Headers are blank when compared to the wireshark data we displayed using OpenBTS. This is because in this particular capture the physical layer was handled by a different piece of software (GNU Radio), which then decoded the data and sent it as a UDP packet to Wireshark. This is different from when we use OpenBTS to send the data, since OpenBTS is handling the physical layer of GSM directly, it’s able to include the information when Wireshark receives it.

## What to submit

Using the Wireshark capture, answer the following questions:

1. When looking at GSM frames, the term “channel” is used a lot. What does ‘channel’ refer to?
2. What frequency and ARFCN is this network operating on? Show a screenshot that clearly shows you found the correct type of BCCH with this info. Describe the ARFCN’s and what their actual frequencies would be.
3. The network broadcasts neighboring ARFCN’s. This is so your phone knows what bands it can handoff to that are nearby. Find the data in the appropriate BCCH and include a screenshot. (note, there are two different batches that were available, depending on which BCCH you look at and what band the phone is capable of, just include one)
4. When searching through the BCCH’s, you’ll find one of the types that contains the network area identification parameters. This includes our MCC and MNC! Take a screenshot that clearly shows you found the MCC/MNC. Describe them, who is the actual carrier?
5. Power levels are very important in cellular networks, we want to make sure the MS hears our signal and we want to make sure we can hear the MS’s replies back. We also want to ensure that one MS’s signal doesn’t overpower another MS’s signal. The BCCH’s contain parameters for minimum power required by the handset before looking for a reselection candidate and it contains the max power a MS may use in the area. (you’ll find this in Cell Selection Parameters). Find these values and report the two values and include a screenshot.
6. There aren’t very many LAPDm frames. These frames are actually GPRS data frames. What is GPRS and why aren’t there very many frames using it?
7. A few PCH’s exist. Paging requests are the network’s tool for waking a phone that’s camped and needs to do something. Some pages are very generic, but our capture has some that area addressed to specific TMSIs. Take a screenshot showing that the TMSIS is broadcast out to the world in the clear (note, it’ll appear as a hexadecimal value, one example is 0xc90a370d).

\*remember to include the answer to each question and not *just* a screenshot!