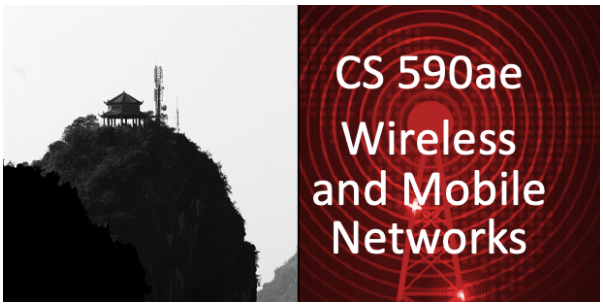
CS590ae: Lab 5

Assigned: 4/9/25
Due: 4/16/25

Spring 2025
Professor Jim Kurose

"Tell me and I forget. Show me and I remember. Involve me and I understand."
Chinese proverb



Introduction

In this lab, we'll examine *mobility* in 5G networks. Mobility has always been a key design goal of cellular networks, with the earliest generations of cellular networks providing call handover with uninterrupted voice service as a user ranged from cell to cell across a provider's network, and from one provider's network to another. With mobility "baked in" to the earliest cellular telephony network architectures, the addition of mobile data services followed quite naturally in later generation cellular networks.

We've learned in class that handover of a UE from the gNB to which it is currently attached (referred to as the **source gNB** in the handover process) to a different, nearby gNB (referred to as the **target gNB**) occurs for one of several reasons, including *(i)* there may be a superior-quality radio channel from the UE to the target gNB than to the source gNB, or *(ii)* the target gNB is more lightly loaded (in terms of number of attached UEs and their traffic demands) than the source gNB.

We also learned in class that handover is orchestrated between the RAN and 5G Core control planes and involves the reconfiguration of the device's RAN and 5G Core data plane, making it a truly network-wide activity. In this lab, we'll mostly focus on *(i)* the events that led to a handover decision by the source gNB *(ii)* the messaging between a UE and the gNBs when it's time to switch to a new physical cell.

Setup and Trace Files

Once again, we'll use a Wireshark .pcap trace file that has already been gathered for you. The .pcap trace for this lab can be downloaded from here: https://gaia.cs.umass.edu/wireless_and_mobile_networks/files/trace3.1.pcapng. This trace file was collected by driving a car in North Amherst, MA, USA between 13:58 EST and 14:24 EST[1], as shown in Figure 1.

---

[1] This trace was gathered by Atharva Kale, one of our TAs for CS590ae. Atharva also wrote the most significant parts of this Wireshark Lab. We appreciate all of his amazing efforts!

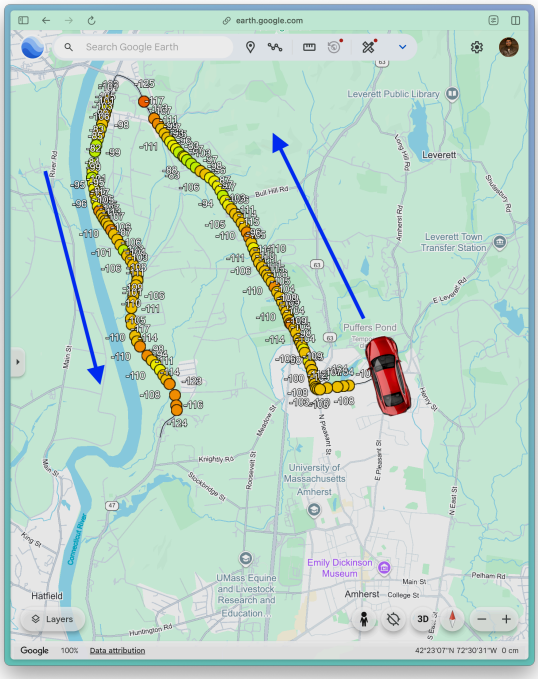


Figure 1: A map of the route taken to generate this trace. The dots indicate the RSRP (Received Signal Reference Power) in dBm with darker colors indicating poorer coverage.

You should download this trace and make sure that you have installed the scat-v2.lua extension https://gaia.cs.umass.edu/wireless_and_mobile_networks/files/scat-v2.lua which we also used in previous labs. If you have already installed it, you're all set. If not, install this file following the instructions in Lab 2, and then restart Wireshark.

Now let's take a look at this .pcap trace file. First, let's change the "Time" column in Wireshark. to display the "time-of-day wall clock" time, which will give you a better sense of how "close" two packets are in real-time so that we can get an intuition on coverage blind spots as well as how often your UE changes its point of attachment when travelling in a car. To do this, in the Wireshark top menu select View→Time Display Format → Time of Day. Your display should look like Figure 2.

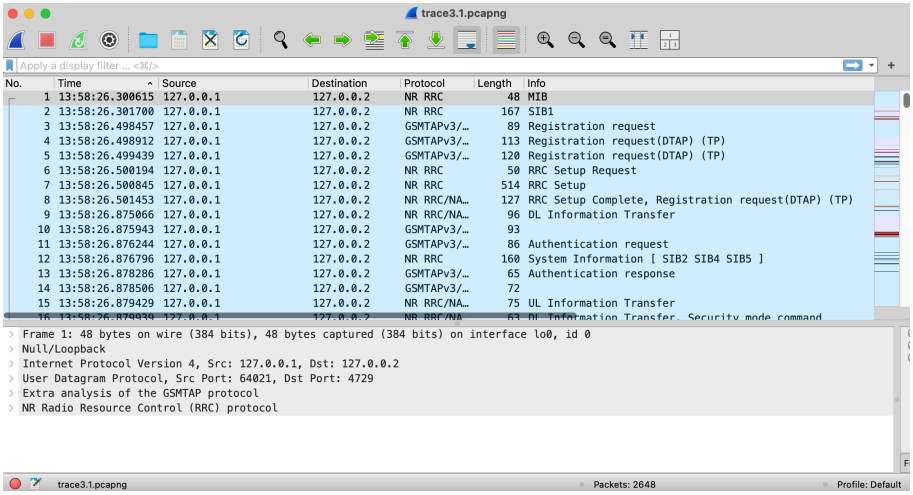


Figure 2: Showing the time-of-day time in the Time column

The key decision maker for 5G handover is the gNB to which the UE is currently attached, i.e., the **source gNB,** as shown in Figure 3 below you (this is Figure 9.3 in our class readings, in http://gaia.cs.umass.edu/wireless_and_mobile_networks/readings/Chapter_9_Mobility.pdf). In this lab, we will focus on three aspects of the handover process:

1. The measurement activity (labelled "1" in Figure 3)
2. The re-configuration of radio and measurement parameters (labelled "2" in Figure 3)
3. The confirmation ACK (RRC reconfiguration complete) message sent by the UE that indicates that the handover is complete from the UE point of view (labelled "3" in Figure 3)

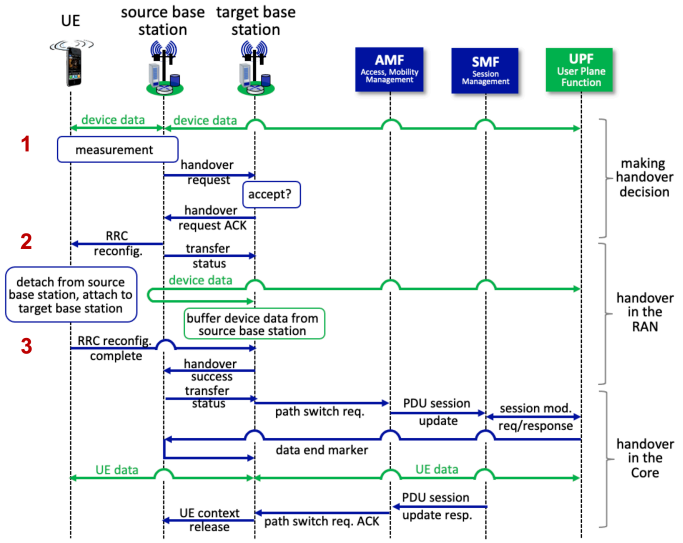


Figure 3: Device handover: RAN and Core actions

PART 1: Channel measurements—configuring and reporting measurements

We know that the decision to initiate a handover is made by the source gNB based on measurements reported to the gNB by the UE to be handed over. As we'll see, the gNB uses the **RRC Reconfiguration message to** instruct the UE about what measurements to make and when to report them. The UE will report its measurements using a **Measurement Report** message.

Configuring UE Measurements

Let's begin by looking at how the gNB instructs the UE to make and report measurements in a downlink RRC configuration message. To display only the RRC reconfiguration messages in a trace, you could type the filter specification *_ws.col.info matches "RRC Reconfig"* into the filter window at the top of the Wireshark display. Let's begin by looking at packet 39, which is an RRC configuration message.

1. In packet 39, what is the physical cell identifier of the gNB that is sending this RRC Reconfiguration? This is the physical cell identifier of the gNB to which the UE is currently attached. (Hint: you will have to look under "Extra analysis of the GSMTAP protocol)

RRC reconfiguration messages serve many purposes, but our interest here is on channel measurement. So, let's expand the packet display to show the measurement configuration that the gNB is specifying to the UE: **`rrcReconfiguration->criticalExtensions: rrcReconfiguration->measConfig.`** Two important items of the measurement configuration are: **`the measObjectToAddModLis`**t (which tells the UE *what* to measure) and **`reportConfigToAddModList,`** (which tells the UE *when* to report). See Figure 4.

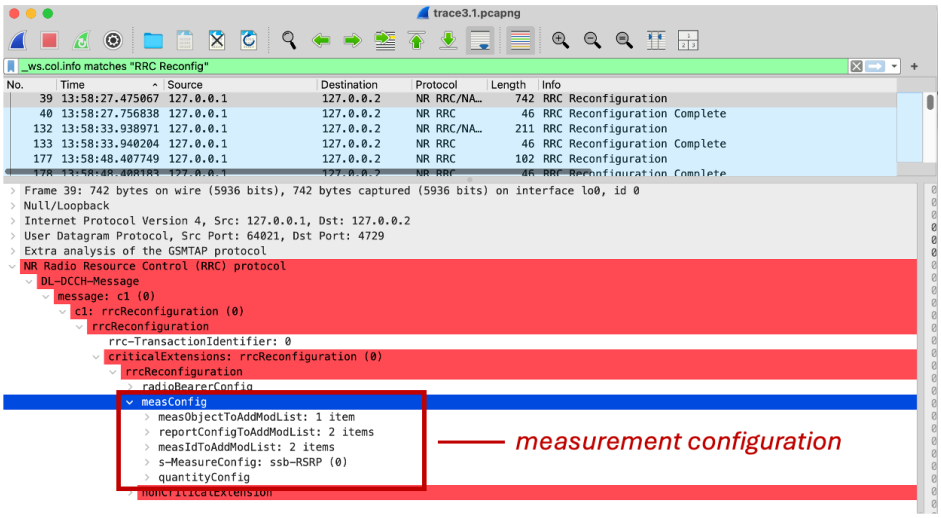


Figure 4: measurement configuration in an RRC reconfiguration message

2. What is the radio frequency that the UE is being instructed to monitor? The UE will then measure SSBs (Synchronization Signal Blocks) transmitted by the UE in this frequency band? Hint: look under **`measObjectToAddModList.`** The value listed after ssbFrequency: is not an actual frequency but rather the Absolute Radio Frequency Channel *Number* (ARFCN). A standard and tools (you can find them via Google) exist to map from ARFCN to an actual channel frequency.
3. What is the maximum number of cells that the gNB instructs the UE to report measurements for under event ID A2? Hint: look under **`reportConfigToAddModList`**
4. The gNB only asks the UE to trigger a measurement report when specific conditions are met, such as the signal strength dropping below a certain threshold, as in the case of an A2 event. This event-based mechanism decreases the overall measurement signaling load. For this case, the gNB specifies that a measurement message should be sent when the Synchronization Signal Reference Signal Received Power (SS-RSRP) falls outside of a given range. What is the *upper* limit of this power range?

Reporting Measurements

The UE reports its measurements to the gNB in "Measurement Reports." Packet 176 contains such a measurement report, as shown in Figure 5.

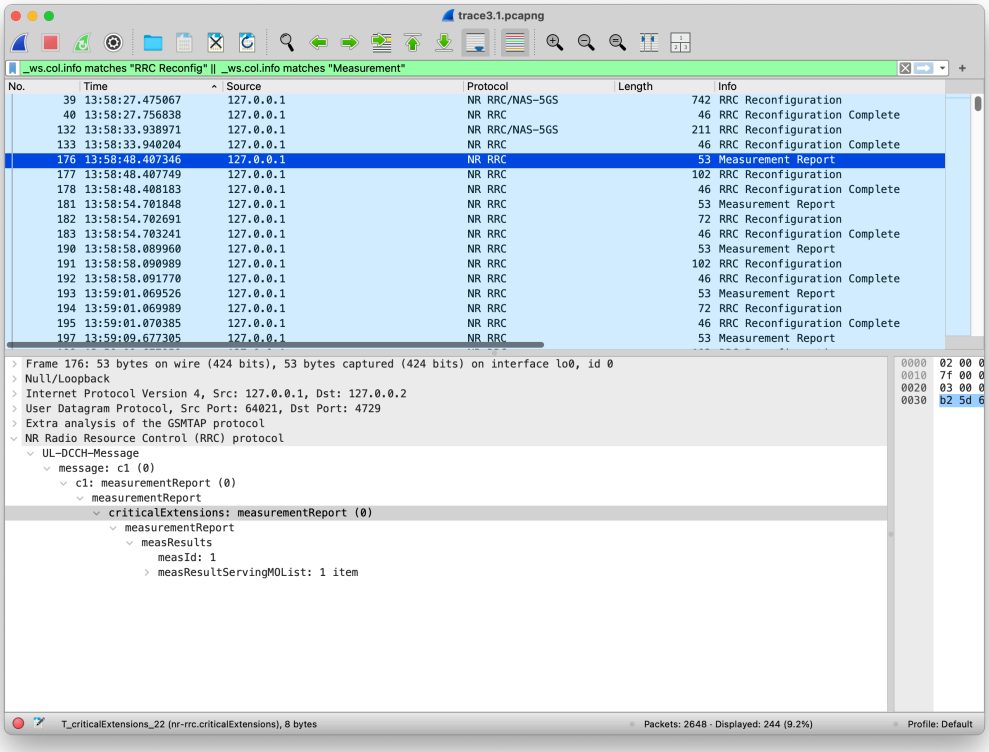


Figure 5: A Measurement Report

5. In packet 176, what is the physical cell identifier of the gNB receiving the measurement report from the UE (hint: you will have to look under "Extra analysis of the GSMTAP protocol")?
6. What is the physical cell identifier of the gNB for which the UE is measuring channel quality?
7. Does this measurement report contain measurements for the currently serving cell? Are your answers to questions 5 and 6 the same? (Think about the cases when they would/would not be the same)
8. What is the average Received Signal Reference Power (RSRP) strength of the synchronization signal block (SSB) that the UE has measured?

PART 2: Initiating the handover decision

Now, let's look at a measurement report sent by the UE *just before* the gNB instructs the UE to change its point of attachment to the network.

9. Examine the Measurement Report in packet 295. Are there channel quality measurements for more than one gNB (assuming the physical cell identifier represents exactly one gNB)?
10. What is the physical cell identifier of the gNB receiving this measurement report from the UE (hint: you will have to look under "Extra analysis of the GSMTAP protocol)?
11. What is the physical cell identifier of the serving cell for which measurements are reported?

12. What is the physical cell identifier of the neighboring cell for which measurements are reported?

Now let's look at the RRC Reconfiguration message (packet 296) from the gNB back to the UE that immediately follows (less than a fraction of second later) this measurement report in packet 295. If you want to view RRC reconfiguration requests and Message reports in relationship to ehac in ther in the traces, with other packets remoived, you can enter Use the filter: **`_ws.col.info matches "RRC Reconfig" || _ws.col.info matches "Measurement"`** into the filter area of the Wireshark Display, as in Figure 6.

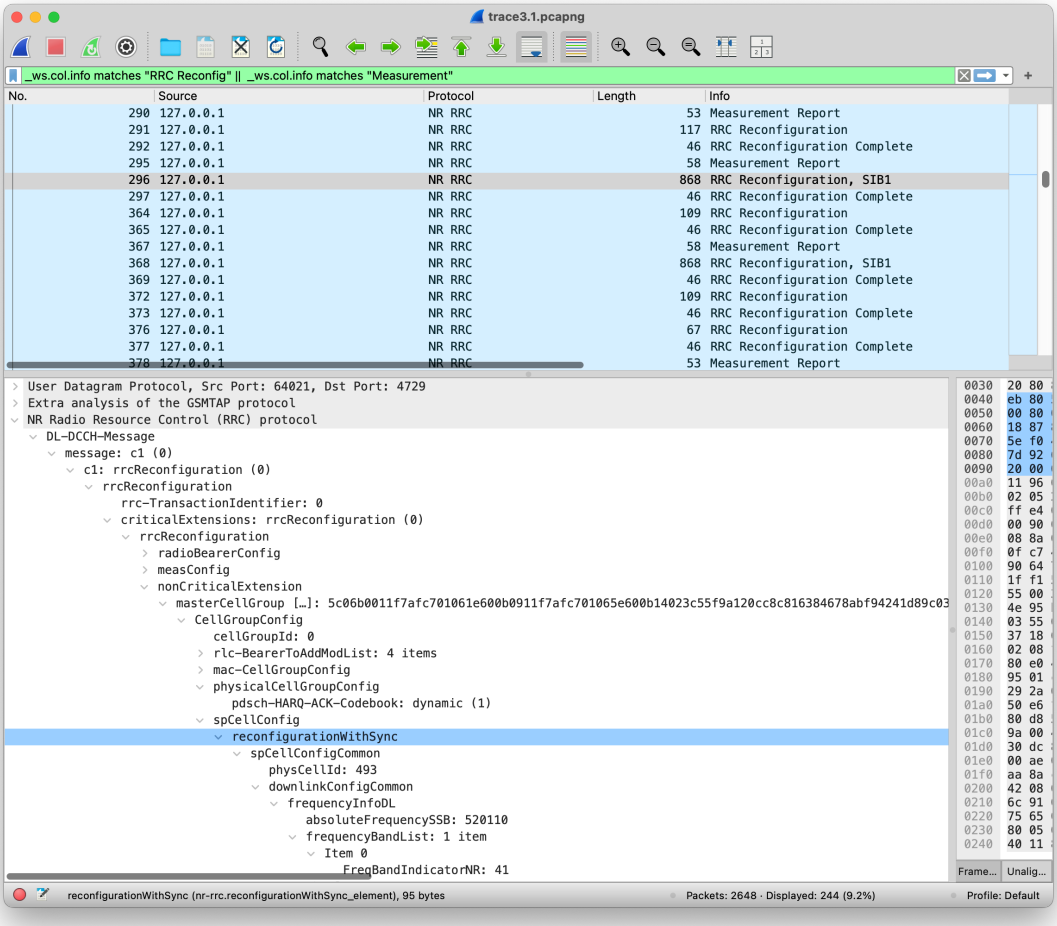


Figure 6: The RRC Reconfiguration that instructs the UE to change its point of attachment (and has decided to do so based on the Measurement Report it hasd just received.

13. In packet 296, see Figure 6, what is the physical cell identifier of the gNB that is sending this RRC Reconfiguration?
14. Now consider at the highlighted line in Figure 6—it is a *reconfigurationWithSync* line! The *reconfigurationWithSync* procedure ensures seamless mobility by synchronizing the UE with a new cell, performing random access if needed, and updating configuration parameters to match the new environment. What is the physical cell identifier of the gNB that the UE is about to join?

15. What frequency band will the UE use in its communication with this new physical cell on the downlink channel?
16. Does this RRC Reconfiguration message have an embedded SIB? Think about why having access to an embedded SIB would be convenient for the UE.

PART 3: Exercising the handover decision

Now, the UE finally has all the information it needs to switch over to the new physical cell.

17. Let's examine packet 297 which is on the uplink (UL). The UE sends the RRC Reconfiguration Complete message to which physical cell identifier?

3. What to hand in for this lab

Now that you've done all of the above, it's time to submit your answers to the questions above. You'll do so on our class's Canvas page.

4. Acknowledgements

1. This trace was collected using a tool called SCAT which operates on a rooted android phone to capture 5G signaling via a diagnostic port on a qualcomm processor. Byeongdo Hong, Shinjo Park, Hongil Kim, Dongkwan Kim, Hyunwook Hong, Hyunwoo Choi, Jean-Pierre Seifert, Sung-Ju Lee, Yongdae Kim, "Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis," *IEEE Transactions on Mobile Computing,* February 2018. https://github.com/fgsect/scat
2. To add the physical cell identifier to the "Extra analysis of the GSMTAP protocol" section, we had to "hack" the SCAT tool to place this information in the trace because the GSMTAP v3 specification is still under development. https://github.com/atharvakale343/scat/pull/1
3. The blog *How LTE Stuff Works* written by a Swedish 3GPP engineer is an incredible technical blogsite that condenses the 3GPP specification well and made the RRC signaling easier to understand for this lab. https://howltestuffworks.blogspot.com/2020/02/5g-nr-measurement-configuration.html
4. Capturing mobility traces "in the wild" is always a fun experience and challenging when it comes to suburban environments with spotty coverage. Thanks to Sagarika Sonni and Khushi Rajoria (UMass students) for driving Atharva around and engaging in this work.