Bachelor thesis
Computing Science


Radboud University

# Systematic Analysis on the effect of 4G LTE Reconfiguration Settings on Measurement Report Generation

*Author:*
Floris Valentijn
1031160

*First supervisor/assessor:*
dr. K.S. (Katharina) Kohls
katharina.kohls@ru.nl

*[Second supervisor:]*
T. (Thijs) Heijligenberg, MSc
thijs.heijligenberg@ru.nl

*Second assessor:*
dr. E. (Erik) Poll
e.poll@cs.ru.nl

June 26, 2022

**Abstract**

Measurement reports contain important signal information in order for the base station to make connection decisions. The base station specifies how and when this information must be sent by the user device by creating a configuration. In this thesis we create a simulation and perform a systematic analysis by executing the simulation in order to see the effects of configuration differences in the amount of measurement reports that are generated. This information may be used to increase the understanding of event generation in LTE or in further research looking at the information that can be obtained from measurement reports. Based on the results we can see that the expected patterns were indeed present but also that there are derivations that may be worth looking further into. From the simulation and its results we can also make speculations about handover and fake base station detection research, although making necessary assumptions.

# Contents

# Chapter 1

# Introduction

Mobile networks are used more and more everyday. Nowadays the 4G LTE protocol specifically is used more than any other internet connection protocol for many people who are on their way to work, shopping outside and anywhere they do not have local internet connection available. During most of these activities we travel a lot of distance while wanting to stay connected to the internet. In addition to not being able to use Wi-Fi because of its low range, LTE outperforms Wi-Fi 40% of the time [4]. For our devices to maintain this proper connection they need to be connected to a radio tower with a good enough signal strength. Our travels require us to be able to connect to different radio towers depending on where we are to keep this proper signal strength. We do not want to lay this burden onto the user and this means that our device and the connected radio tower together need to decide whether the device is going to connect to a different radio tower or not. Doing this improperly can result in the mobile device having suboptimal internet connection or losing their connection entirely. This problem is dealt with accordingly in the 4G LTE protocol technical specifications [5]. The protocol specifies that the base station can create a configuration which tells the mobile device when to send reports back, containing for example information about signal strengths towards the connected base station and others within their proximity.

We call the reports that are then sent by the device, "Measurement reports". These Measurement reports are crucial in order for the radio tower to make valid connection decisions because they contain the signal information of the device. From this the question arises how much are these measurement reports sent, according to which configurations, and are these measurement reports useful enough? Most of the previous research done in this area is looking at power efficiency, handovers and fake base stations. However, there has been done little to no research on the effects of different configurations on the generation of the measurement reports [17][2]. This

research looks at this question by creating a simulation from the official LTE protocol documents.

The purpose of this thesis is to analyze the LTE measurement report generation process. To achieve this goal we first study the measurement reporting process and its report configurations. Then, we create an implementation of the process according to the 3GPP specification [5]. Finally, we use the implementation to identify the strengths and weaknesses of particular configurations according to its power consumption statistics.

In the Preliminaries we will explain in depth what a LTE network is exactly and what components it contains. In this section we will also explain what the possible events are that the base station can choose inside their report configurations and how these report configurations are build up. Then, in the simulation chapter we will explain the implementation we created in order to gain more insight into the problem. After this, in the Results chapter we will then give the results obtained from this implementation. Next, in the Discussion and Related Work chapter we discuss the results and their appliance to related work. At last, in the Conclusion we conclude the research.

# Chapter 2

# Preliminaries

In order to make the concepts clear, this section describes the most important components of LTE. It contains information about what some of the abbreviations that we use, stand for. It explains the LTE network, the concepts of a measurement report and a report configuration and it shows how events and handovers work. At last, there is some additional information about fake base stations necessary for the discussion in related work.

## 2.1 Network setup

In order for a LTE network to be functional it needs communication between a User Equipment (UE), an evolved Node B (eNodeB/eNB) and an evolved packet core (EPC). Then, the network is setup as displayed in figure 2.1. An eNodeB provides internet connection from a connected EPC to the UE. The UE can choose an eNodeB that it wants to connect to or leave this decision to the eNodeB that it was previously connected to [10]. There can be multiple UEs connected to one eNodeB and multiple eNodeBs to one EPC. The eNodeBs are in reality often placed in populated locations and they are not placed close to each other. According to Merz et al. (2014) The UE can travel up to around 200km/h when using the LTE network [9]. The UE can also be located at an inconvenient place for the eNodeB signal to reach it. There could be for example a range of concrete buildings in between the UE and the signal.

## 2.2 Components

There are three main components in the LTE network. These components are the user equipment, the evolved node B, and the evolved packet core. These components are setup individually before connecting to each other and forming the LTE network.

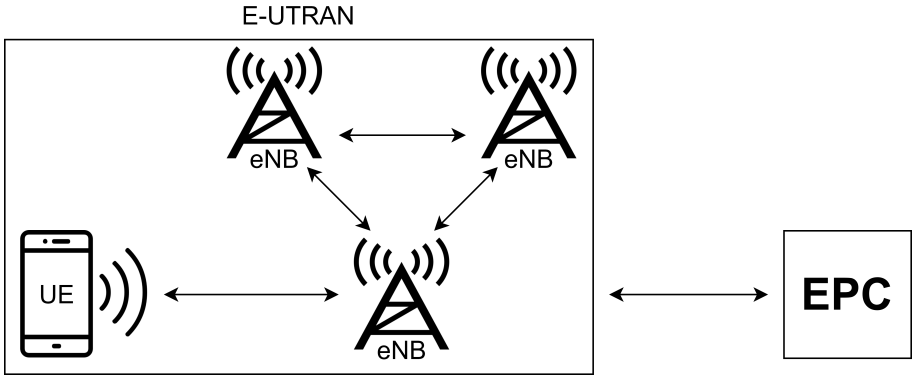


Figure 2.1: LTE network setup

### 2.2.1 User Equipment

The abbreviation we use for the User Equipment is UE. The UE can also sometimes be called a user device instead. This UE contains a chip that enables the device to connect to the LTE (Long Term Evolution) network. This chip is called a Subscriber Identity Module (SIM-card) and is provided with an International Mobile Subscriber Identity (IMSI). This IMSI is used to identify the UE to the mobile network. In addition this SIM-card also stores your phone-number, contact information and data usage. The devices that are used as a UE are mostly cell phones, tablets and laptops but nowadays are also used increasingly for drones and other robotic systems.

### 2.2.2 Evolved Node B

The abbreviation we use for the Evolved Node B is eNodeB. In the context of LTE These can also be called radio stations, base stations or cells. The eNodeB acts as an interface and connects to the EPC (Evolved Packet Core) in order to connect the UE to the internet. In reality an eNodeB is a signal transmission device containing a large antenna. These must be located on large buildings in order to avoid signal blockage and thus improve coverage. The eNodeB together with the UE we call the E-UTRAN. This E-UTRAN takes care of making the right connection decisions concerning different signals. The E-UTRAN then sends its data towards the evolved packet core with handles the rest of the LTE connection.

### 2.2.3 Evolved Packet Core

The abbreviation we use for the Evolved Packet Core is EPC. The eNodeB communicates with the EPC so that the internet connection can be fully setup. The EPC takes care of the authentication of the UE and the improvement the existing LTE connection that it was setup in. The EPC

consists out of multiple parts that work together to connect the E-UTRAN to the internet [7].

- **HSS**: Home Subscriber Server. This part contains user-related information. It helps with for example mobility management and user authentication.
- **Serving GW**: Serving Gateway. IP traffic gets sent between the internet and the E-UTRAN. It also serves as a control pane connection from the Mobility Management Entity.
- **PDN GW**: Packet Data Node Gateway. This part is the direct connection to the internet. It routes packages between the Serving GW and the Internet and takes care of IP address management.
- **MME**: Mobility Management Entity. This part takes care of locations and security of data going into the E-UTRAN.

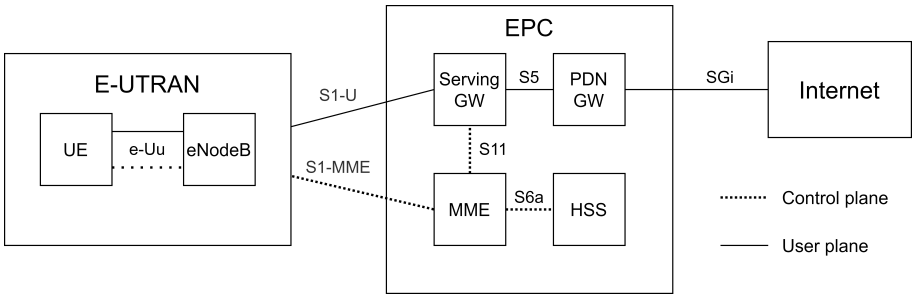


Figure 2.2: The Evolved Packet Core [7]

## 2.3 LTE

The LTE components have to communicate among each other in order to allow for packages to be correctly sent, thus forming the network. These components thus, are setup and communicate according to specifications in order for the LTE network to work for all sorts of different user devices ranging from smartphones to drones.

### 2.3.1 The LTE network

The LTE network provides the UE of internet connection. Through using eNodeBs as signal emitters, the LTE network can provide the UE with access to the internet via a mobile connection. Within this network there is a message exchange between the UE and the eNodeBs in order for the UE to maintain a proper connection. Within the active state the eNodeB specifies

a report configuration and sends it towards the UE. Within the idle state the UE takes decisions by itself without needing a report configuration. The UE takes this report configuration and creates a measurement report containing the information that is specified inside the report configuration. Using this information the eNodeB can make connection decisions in behalf of the UE. These connection decisions have to do with handing over a UE to a different eNodeB, cutting connection and similar decisions.

The LTE network is implemented by all service providers according to the 3GPP LTE specifications [5]. These specifications contain directions on how the LTE network should work but has no specific coding directions. Because of this there are many different possible implementations that could all be slightly different. There are, however, formulas inside the specification so that these can be implemented just the same. For event triggering all the variables that should be used are specified, including when exactly the events should be triggered.

### 2.3.2 The LTE protocol stack

The LTE network consists of a protocol stack of 3 layers. Figure 2.1 displays a visual representation of the LTE protocol stack. The layer L1 contains the Physical layer. This layer is responsible for the physical connection between the UE and the eNodeB. For the LTE network this physical connection is a wireless connection. The layer L2 contains the Packet Data Convergence Protocol, the Radio Link Control and the Medium Access Control. The protocol together are responsible for the connection between the UE and the eNodeB. The layer L3 contains the Non Access Stratum, the Radio Resource control and the Internet Protocol [8]. These protocols are responsible for the data sent between the UE, the eNodeB and the core network. The User Plane handles the user traffic from the network. The Control Plane handles the signalling messages between the UE and the eNodeB. Below, we explain each of the protocols separately.

- **NAS**: Non Access Stratum. This protocol handles the communication between the core network and the UE.
- **RRC**: Radio Resource Control. This protocol takes care of connection and system information. This includes report configurations and measurement reports.
- **IP**: Internet Protocol. The internet protocol carries all the internet traffic of the user.
- **PDCP**: Packet Data Convergence Protocol. This protocol is responsible for transporting the data in packets.

- **RLC**: Radio Link Control. This protocol handles data to control the connection between the UE and the eNodeB
- **MAC**: Medium Access Control. This protocol controls the hardware for the physical layer.
- **PHY**: Physical Layer. This physical connection is a radio signal connection with a certain strength.

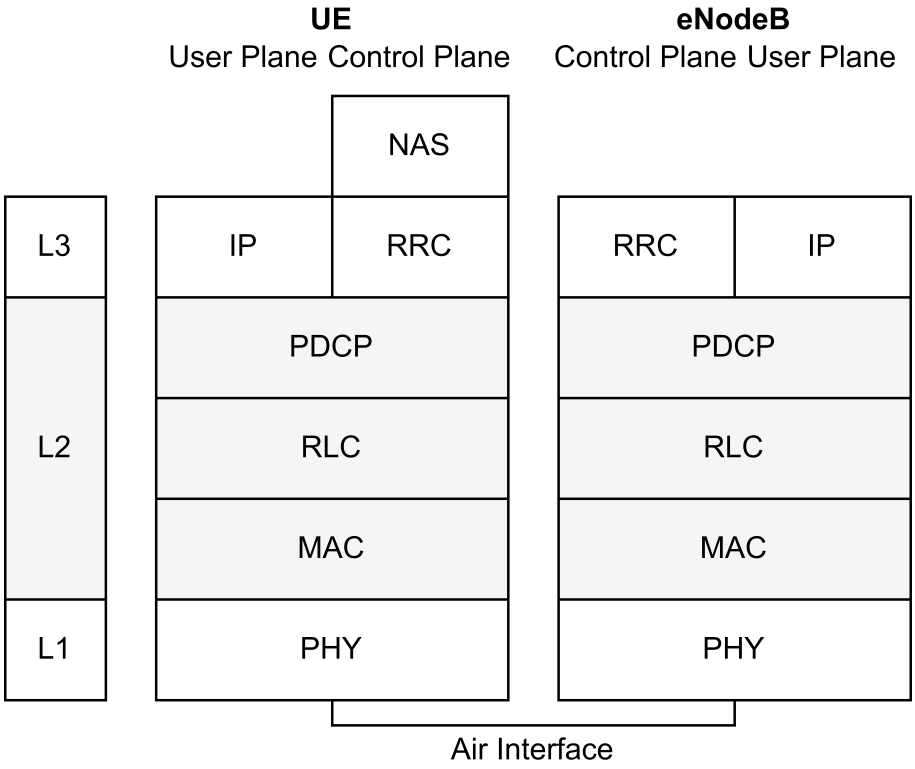


Figure 2.3: The LTE protocol stack

## 2.4 Important Terms

For this thesis it is important to understand the basic concepts of LTE and the concepts necessary to understand the report configurations and corresponding measurement reports. This section contains the basis of these concepts and some specific information, necessary for this thesis.

### 2.4.1 Reference Signal Received Power

Within the network we will only be looking at Reference signal received power (RSRP). This value is a measure for the signal strength of a signal [12]. The UE usually also measures RSRQ (Reference Signal Received Quality). This RSRQ value is derived from RSRP and RSSI (Received Signal Strength Indicator). The RSSI is the total signal strength that the UE receives from all possible signals together. The RSRQ is then the signal quality of a particular signal.

### 2.4.2 Measurement reports

Measurement reports contain signal information collected by the UE. This signal information consists of signal information that the UE receives. This information can be any information about signals. In this research we only look at RSRP, which is the strength of the signal. We also only look at the eNodeB's signal information. In figure 2.2 we can see that in step 1 the eNodeB sends a report configuration towards the UE. Second, in step 2 the UE preforms the measurement procedure as specified by the report configuration. At last, in step 3 sends the collection of data from the measurement procedure within a measurement report towards the serving eNodeB.

### 2.4.3 Handovers

A Handover can be carried out by the eNodeB in order to provide the UE of a better signal coverage from a different eNodeB. There are multiple cases when an eNodeB can do this. We will say in this thesis that the eNodeB does a handover when event A3 or A5 is triggered. This means that the measurement report which the UE returns contains information that the neighbour has become better than itself or that the neighbour has become better than a threshold and itself has become worse than a threshold [6]. The eNodeB then signals the neighbour in order to start the handover process. In figure 2.2 we call this the handover decision. Next, the serving eNodeB and the target eNodeB prepare for handover. Afterwards, the serving eNodeB initiates the handover by sending a message towards the UE. The UE then detaches from the serving eNodeB, connects to the target eNodeB and then signals both eNodeBs that the handover is complete.

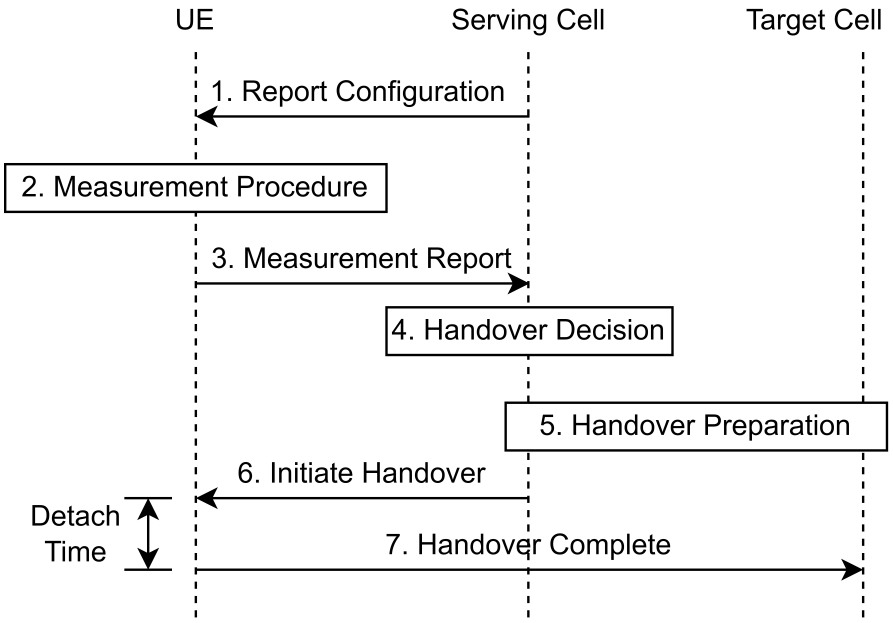


Figure 2.4: Handover after a measurement report [22]

### 2.4.4 Report configurations

When the eNodeB wants to specify what report configuration the UE has to use, it can send an RRC connection reconfiguration. Inside this message the eNodeB puts the new report configuration that the UE is going to use for future communication. Depending on the contents of this configuration the UE will send different measurement reports at different moments in time towards the eNodeB. Since the goal of the report configurations is to specify when measurement reports have to be sent, it contains the necessary variables. These are events, intervals, amounts and the maximum eNodeBs it should record. Events are pre-specified triggers that determine under what circumstances a measurement report should be sent.

The report configurations that are used in our simulation look as follows.

1. `event`
    - `event_a1 threshold`
    - `event_a2 threshold`
    - `event_a3 offset`
    - `event_a4 threshold`
    - `event_a5 threshold1, threshold2`
    - `event_periodical`

The event configuration option contains the events that are enabled and their respective configurations. The event threshold and offset are expressed in dBm (decibel-milliwatts). Further explanation can be found in part 2.9.

2. `maxReportCells`

   The maxReportCells configuration option contains the number of eNodeBs that the UE has to take into their measurement report. The range of this option is [1...8] where the number stands for the number of eNodeBs that the UE has to report.

3. `reportInterval`

   The reportInterval configuration option contains the interval in which event triggers must be checked. The range of this option is [0...12] where the values correspond to intervals of (120ms, 240ms, 480ms, 640ms, 1024ms, 2048ms, 5120ms, 10240ms, 1m, 6m, 12m, 30m, 60m) respectively.

4. `reportAmount`

   The reportAmount configuration option contains the amount of reports that can maximally be sent. The range of this option is [0...7] where the values correspond to report of (1 report, 2 reports, 4 reports, 8 reports, 16 reports, 32 reports, 64 reports, infinite reports).

### 2.4.5 Events

| Event Type | Description |
|---|---|
| Event A1 | Serving becomes better than threshold |
| Event A2 | Serving becomes worse than threshold |
| Event A3 | Neighbour becomes offset better than serving |
| Event A4 | Neighbour becomes better than threshold |
| Event A5 | Serving becomes worse than threshold1 and neighbour becomes better than threshold2 |

Figure 2.5: Events and triggering conditions [11]

The LTE protocol specifies multiple events for triggering measurement reports. Some of these events are the events A1/2/3/4/5, events B1/2, events C1/2, events W1/2/3, events V1/2, events H1/2 and the *periodical* event[11]. The events specified in this thesis are A1, A2, A3, A4, A5 and the *periodical* event. The *periodical* event constantly triggers the measurement report

generation at the specified time between intervals. The other events are a subset of the periodical event. These events can be triggered within the same intervals at the configured point of time. Consequently, the UE sends a measurement report to the eNodeB at this interval. These points depend on the serving eNodeB and the eNodeB neighbours signal strengths in respect to the UE. Figure 2.3 contains a simplified table for seeing what events get triggered on what conditions [11].

For event A1 and A2, *Ms* is signal strength of the serving eNodeB towards the UE expressed in dBm since we are only looking at RSRP. *Hys* is the hysteresis which is used to decrease the amount of measurement reports generated because of small fluctuations. Since we do not simulate these fluctuations we will not use this value in the simulation of this thesis. *Thresh* is the threshold which we specified in the report configuration.

For event A3, A4 and A5 we also have the variables *Ofn*, *Ocn*, *Ofs*, *Ocs* and *Off*. *Ofn*, *Ocn*, *Ofs* and *Ocs* are eNodeB specific offsets that must be requested from the respective eNodeB, these variables fall out of the scope of this thesis. *Off* is the offset that is specified in the report configuration.

According to the LTE protocol specifications the trigger conditions for the events are as follows [5].

Event A1:

$$Ms - Hys > Thresh$$

Event A2:

$$Ms + Hys < Thresh$$

Event A3:

$$Mn + Ofn + Ocn + Hys < Ms + Ofs + Ocs + Off$$

Event A4:

$$Mn + Ofn + Ocn - Hys > Thresh$$

Event A5:

$$Ms + Hys < Thresh1$$

$$\&$$

$$Ms + Ofn + Ocn - Hys > Thresh2$$

### 2.4.6 srsRAN

During this research we have also worked with srsRAN. srsRAN is a piece of software that simulates the entire LTE protocol stack by creating the UE, eNodeB and EPC separately from each other. This software is freely available on github and an in depth manual for setting up the network is located on their site [15]. By starting these pieces of software up on different devices or on separate terminals within one computer we can generate LTE messages and intercept them. During this research we intercepted them using Wireshark. Figure 2.4 contains a measurement report that we received using Wireshark. The report configuration used for this measurement report was configured with event A3. The corresponding report configuration is not displayed as this required the piece of software to be altered which we tried but could not get working. As seen in figure 2.4 the measurement report contains the RSRP and RSRQ values of the signal strengths from the eNodeB to the UE. We have not tried this using multiple eNodeBs since we first wanted to implement all the events A1, A2, A3, A4, A5 fully, however, this proved hard to do.

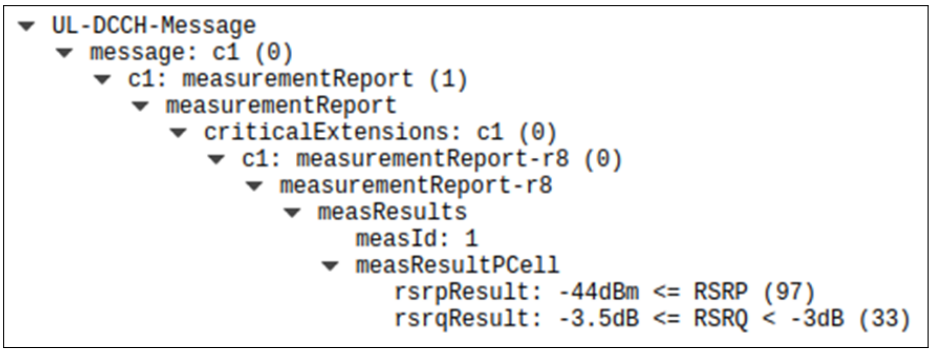


Figure 2.6: A measurement report as received by Wireshark

### 2.4.7 Fake base stations

Within the protocol the UE never checks if the measured eNodeB is a legitimate eNodeB. Because of this vulnerability, adversaries can set up fake base stations and spoof existing ones to make UEs connect to them. When a UE connects to the fake eNodeB the adversary can abuse the pre-authentication NAS layer messages which includes an identification procedure [1]. It is then possible for the eNodeB to steal the UEs identifiers and thus execute an attack making use of this vulnerability. From the information inside the measurement report, which is mostly signal data, we may be able to tell when a fake eNodeB is present within the UE's operative area. The connected eNodeB can then prevent the UE from connecting to the fake base station and report it to the relevant authority.

# Chapter 3

# The simulation

In order to find out the relation between report configurations and measurement reports we need an implementation of the LTE protocol. Our first try was using the open-source LTE implementation srsRAN. However, the event generation part of the LTE protocol was not fully implemented into srsRAN and this proved hard to do [14]. In order to take a fair look at the effects of report configuration on measurement reports we created a simulation from the official LTE specification in python. We used python for this simulation because of past experience with the language and because there is no performance goal that we need to achieve. The simulation code is fully available from the corresponding link.[1] The pseudocode for the algorithm used in the simulation is contained in algorithm 1.

## 3.1 Signal simulation

In our simulation we simulate a UE traveling a path through a field of eNodeBs. The location of these eNodeBs is arbitrary during the final simulations in order to get the most realistic graphs. Within this path we assume that the UE travels at a constant speed of 10m/s, which equals 36km/h. According to research, LTE seems to be robust until at least 200km/h so a speed of 36km/h should not be a problem [9]. In this simulation we only look at RSRP values because these values display the power of the received signal. RSRP values are measured in decibel-milliwatts (dBm).

### 3.1.1 Path simulation

In order to simulate a path we started with a square field of 17km by 17km. We have then chosen a path within this area that the UE travels along at its assumed speed. This chosen path is fixed because the eNodeBs are randomized instead. The signal simulation thus randomizes the location of the

[1] `https://gitlab.science.ru.nl/fvalentijn/lte-event-triggering-simulator`

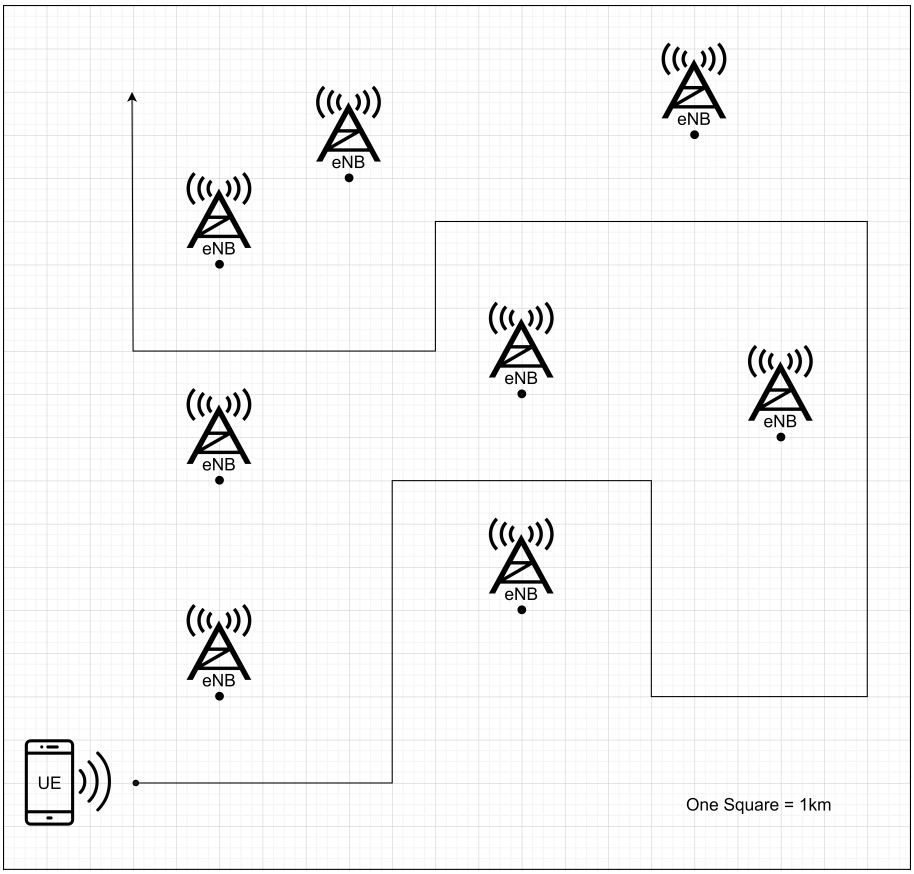


Figure 3.1: Path traveled by the UE.

eNodeBs in order to simulate different situations and thus get more generalized results. The problem with this approach is that there may be outliers when not doing enough executions. We tried to minimize this problem by doing as many executions as was feasible for the simulator in its final state. A possible scenario for the placement of the eNodeBs is displayed in figure 3.1. The UE travels a total distance of 66km with 9 changes of direction. In reality this entire path would thus take 1 hour and 50 minutes for the UE to fully traverse.

### 3.1.2 Signal loss formula

The calculation of the signal strength for UE with eNodeB pairs is done using the signal loss formula FSPL (Free-space path loss). In this formula $d$ is the distance between the UE and the eNodeB and $\lambda$ is the wavelength of the signal. The result of the formula is a decibel (dB) value which can be used to calculate the actual signal strength. This signal loss formula as

used inside the simulation is as follows [19].

$$FSPL = 20 * \log_{10}(\frac{4\pi d}{\lambda})$$

## 3.2 Event implementation

The events are implemented as was previously shown in figure 2.3. The events are implemented separately using a formula adapted to the LTE specifications as shown in chapter 2.9. Only the events A1, A2, A3, A4 and A5 are within the scope of this thesis and are implemented as shown in algorithm 1. The other existing events simply take some extra factor into account that has to be considered for triggering measurement reports. We chose not to implement these events because they are not top priority for research onto fake base stations.

## 3.3 Handover implementation

In this simulation we decided that the handovers should take place in the events A3 and A5. When a handover is triggered, the simulation swaps the values of the serving and neighbour eNodeBs. Afterwards, The simulation goes on as before using the previous neighbour cell as serving cell and the previous serving cell as neighbour cell.

## 3.4 Report configurations for result generation

In this simulation, report configurations contain an extra field in which we have specified how much the event variables should change after one run of the algorithm in order to plot the effects that this change has on the amount of measurement reports generated. The report configurations 1, 2, 3, 4 and 5 are shown in figure 3.2. The report configurations 6, 7, 8 and 9 are shown in figure 3.3. We put all the values inside the report configuration at least between -50 and -100 dBm. We chose these values by using the table of measured RSRP values for LTE [13]. We made the number of runs for the algorithm to correspond to the distance between the signal strengths, which is in the range of 100–500 times. The report configuration changes with 0.1 dBm for each run, which for each run also fully randomized base stations within the map space. We also chose to run the algorithms for configurations where only one of the events is enabled, so we can see the effects of the different events separately. All the executions of the simulation can be found in figure 4.1 until 4.10.

## 3.5 The setup

The setup consists out of three main parts: The initialization of one simulation run, the single simulation run and the running of the simulation for multiple times including the creation of the graphs.

### 3.5.1 The initialization

In order to generate the results, we have to run the algorithm multiple times with different randomized eNodeBs. The eNodeBs are randomized by picking a random value for the x and y axis within the field of 17km by 17km. We decided to do this 10 times for every execution. Since the algorithm already has to run 100-500 times in order to get usable results, a number of 10 runs seems to be a valid option. This is also because execution times were becoming more than 1 hour per full execution when going over 10 runs which was a significant increase.

### 3.5.2 A single simulation

Within a single run of the simulation, the path gets traversed by the UE traveling in a field with random eNodeB locations. The corresponding events get triggered at their specified intervals. When the event A3 gets triggered, the handover will take place and the UE continues traversing the path using the neighbour eNodeB as its serving cell. When the simulation is finished, the algorithm provides a list of events that were triggered with their corresponding time of trigger. We can then use these events to show the event trigger points of interest and how the signals relate to each other.

### 3.5.3 Final setup

To get our end results, we execute the single simulation for every report configuration and within its range. This means that if we have for example configuration five, we will get the following range of values for the simulation: event A1 with threshold -100;-50, event A2 with threshold -50;-100, event A3 with offset -25;25, event A4 with threshold -100;-50 and event A5 with threshold1 -100;-50, threshold1 -50;-100. The starting values are also visible in figure 3.2. In the end the result shows a table with on the y axis the average number of events triggered, which is the sum of all the 10 executions divided by 10. On the x axis the results show the configuration offset in dBm, from which we can derive the corresponding report configuration.

| Configuration: | | | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| event | event_a1 | on | threshold | -60 | -70 | -80 | -90 | -100 |
| | event_a2 | on | threshold | -50 | -50 | -50 | -50 | -50 |
| | event_a3 | on | offset | -5 | -10 | -15 | -20 | -25 |
| | event_a4 | on | threshold | -60 | -70 | -80 | -90 | -100 |
| | event_a5 | on | threshold1 | -60 | -70 | -80 | -90 | -100 |
| | | | threshold2 | -50 | -50 | -50 | -50 | -50 |
| | event_periodical | off | | | | | | |
| maxReportCells | 8 | | | | | | | |
| reportInterval | 0 | | | | | | | |
| reportAmount | 7 | | | | | | | |

Figure 3.2: Report configurations 1, 2, 3, 4 and 5.

| Configuration: | | | | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|
| event | event_a1 | on | threshold | -100 | -100 | -100 | -100 |
| | event_a2 | on | threshold | -60 | -70 | -80 | -90 |
| | event_a3 | on | offset | -20 | -15 | -10 | -5 |
| | event_a4 | on | threshold | -100 | -100 | -100 | -100 |
| | event_a5 | on | threshold1 | -100 | -100 | -100 | -100 |
| | | | threshold2 | -60 | -70 | -80 | -90 |
| | event_periodical | off | | | | | |
| maxReportCells | 8 | | | | | | |
| reportInterval | 0 | | | | | | |
| reportAmount | 7 | | | | | | |

Figure 3.3: Report configurations 6, 7, 8 and 9.

**Algorithm 1:** Simulation code

**Input:** Report configurations
**Output:** Measurement report trigger graph
**Data:** Randomly generated eNodeB map $ENBmap$

```
Function event_a1(threshold, serving):
    return serving > threshold

Function event_a2(threshold, serving):
    return serving < threshold

Function event_a3(offset, serving, neighbour):
    return neighbour > serving + offset

Function event_a4(threshold, neighbour):
    return neighbour > threshold

Function event_a5(threshold1, threshold2, serving, neighbour):
    return (serving < threshold1) and (neighbour > threshold2)

Function neighbour_step():
    Check if events are triggered by running the event functions

Function meas_step():
    for maxReportCells do
        neighbour_step()

Function meas_trigger_sim():
    for reportInterval do
        meas_step()

Function Main:
    for number of normalizing runs do
        for number of simulation runs with changed configuration do
            meas_trigger_sim()
    Print Measurement report trigger graph
```

# Chapter 4

# Results

Using the graphs from this chapter in combination with the report configurations from figures 3.2 and 3.3 we can derive the exact report configuration for the configuration offsets. We can then argue what would be the best report configurations for use within the chosen situations. First, we executed the simulation for all configurations with all events turned on to find out which one is the most optimal. Second, we executed the simulation for all configurations and for each event separately in order to find out what events have the most impact.

## 4.1 Result Generation

The results are generated by running a script that runs each of the simulations for all the different configurations. Then, the graph with the configurations combined is created by putting all the data from these simulation runs into one figure. The separate graphs for the configurations are created by taking all the separate event data for the events and plotting them separately into the different graphs.

The results are generated with the report configuration and its effect on event triggering in mind. We expect the results to have peaks at the point where all events have equal thresholds and event A3 has a offset of 0dBm. The peaks would thus be located at the following points for each configuration:

- One and Nine : offset = 5dBm
- Two and Eight : offset = 10dBm
- Three and Seven : offset = 15dBm
- Four and Six : offset = 20dBm

- Five : offset = 25dBm

While the steps for the results are in steps of 0.1dBm, we chose to show the steps within the graphs only in intervals of 5dBm. This has to do with readability and the fact that we use interpolation to show the lines of the power consumption that resulted from the signals.

## 4.2 Graph setup

We have smoothed the lines in the graphs by applying two spline interpolations to each of the data sets. The x-axis displays the configuration offset for the particular configuration. This means that we can apply x times the offset configuration to the event configuration. The graph then reads the particular configuration which has that specific y value. The y-axis displays the power consumption in milliampere (mA). This value is calculated from the amount of measurement reports that were triggered by that exact configuration. The results from research by Tayyab et al. (2019) show a graph from which we can deduce that a UE uses, by preforming a single measurement report, on average 7 milliwatt [17]. Now suppose that this particular device uses a standard 3.8 volt lithium ion polymer battery. We can use the formula: $P = I * V$ in order to calculate the amount of ampere that is used by the UE. A single measurement report would thus use: $\frac{7mW}{3.8V} \approx 1.84mA$.

## 4.3 Differences between configurations

We will look at figure 4.1 and compare all the configurations with each other whenever possible. There may be multiple factors involved in the change of the amount of generated measurement reports, but we will only look at the variables chosen in this research.

From the figure 4.1 we can derive that the UE has the highest power consumption between the expected threshold values that were predicted within the creation of the configurations. The configurations one, two and three seem to be the biggest outliers and this is most likely because these configurations have higher dBm values (between -50dBm and -80dBm). It is also interesting to see that after the point where all event values have crossed each other, at an offset of 30dBm and 40dBm, most of the configuration keep triggering a high amount of events and thus having a high power consumption. We can see that configuration one with an configuration offset of 30dBm and a report configuration of (A1:-30dBm, A2:-80dBm, A3:-15dBm, A4:-30dBm, A5:-30dBm;-80dBm), still has a very high power consumption despite the low high threshold values of A1, A4 and A5. This can be explained by the event A2 or the event A3 which show more realistic values.

There seems to be a significant peak in power consumption for measurement report generation in the cases of configuration six, seven and eight. For configuration six the peak in power consumption we see in the graph has a report configuration of around (A1:-80dBm, A2:-80dBm, A3:0dBm, A4:-80dBm, A5:-80dBm;-80dBm). This report configuration thus consumes a significant amount of power by generating measurement reports and would for such a path not be desired. The same holds for configuration seven with a report configuration of (A1:-85dBm, A2:-85dBm, A3:0dBm, A4:-85dBm, A5:-85dBm;-85dBm) at its peak, and configuration eight with a report configuration of (A1:-90dBm, A2:-90dBm, A3:0dBm, A4:-90dBm, A5:-90dBm;-90dBm) at its peak, although having a less sharp power consumption peak.

From figure 4.1 we can say that in general, for the configurations five, six, seven and eight the most measurement reports get generated at the point where the report configuration variables are at the average of the signal strengths, which would also be as expected. For the configurations one, two, three and four this does not hold as strongly. These first four configuration have higher dBm more towards -50dBm while the values of the last five configuration have values more towards -100dBm.

## 4.4 Differences between events

The separate events each have a different effect on the power consumption and therefore it is hard to do a complete analysis. Instead we look at the effects that the separate events have on each of the nine configurations and their respective report configurations. These results are located in figures 4.3 until 4.10. In comparison to the lines in figure 4.1 and 4.2 these figures show the effects of the separate events instead of the entire power consumption of the report configuration. Below is a summary of the all the interesting results found within the separate event graphs.

- The events A1 and A4 seem to follow approximately the same line when the configuration increases. For the events A2 and A5 we see the same thing happening only in the opposite direction.
- The event A3 seems to more steeply increase as the offset increases until hitting a peak and less steeply after this peak has been hit. This is true for all the configurations.
- The event A5 seems to be the most power consuming and is thus the most triggered for the configurations one until five. After these configurations, the event A5 seems to be less significant as opposed to the other events.

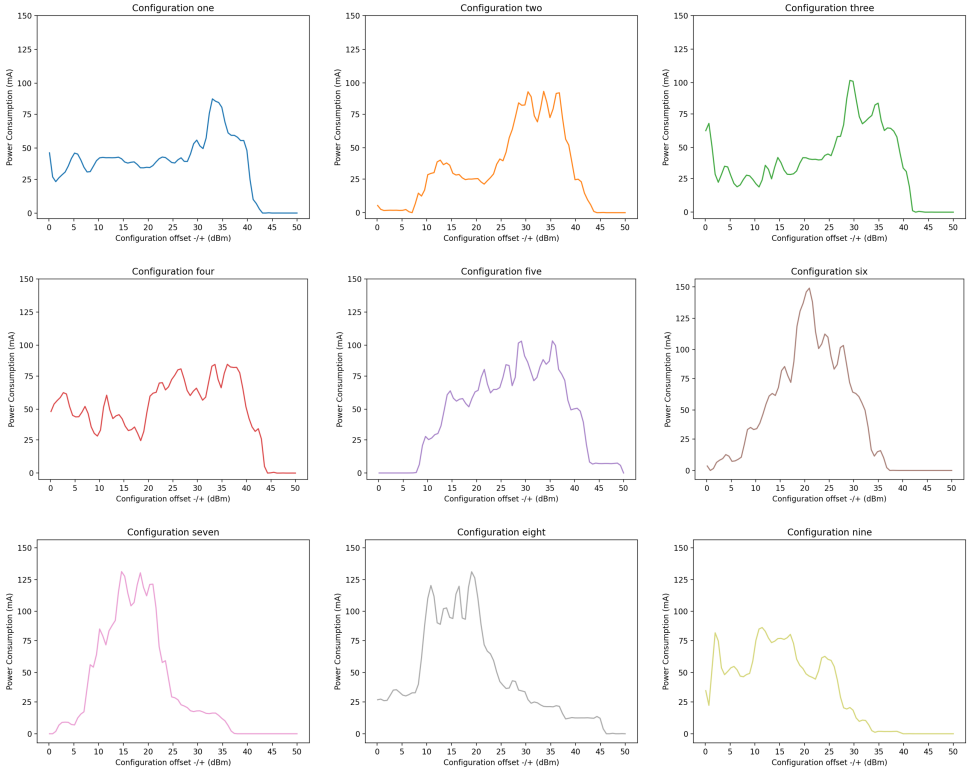


Figure 4.1: Separate simulation runs for all configurations.

- In the configurations six until eight, we see that the events are more uniform then in the other configurations.

## 4.5 Result analysis

The results show some interesting activities that may be worth examining. First, we look at the most important findings from looking at the entire results. Then, we discuss event A3 and A5 since these events signal handovers and thus have a significant impact on the configuration. At last, we discuss the signal generation algorithm since this might affect the obtained results.

### 4.5.1 Important findings

The events A1 and A4 seem to be more power consuming in case of low dBm values. The event A2 also seems to be more active in case of a lower dBm value and A5 uses both high and low values because of having negative and positive dBm values for both its thresholds. Overall configuration seven and

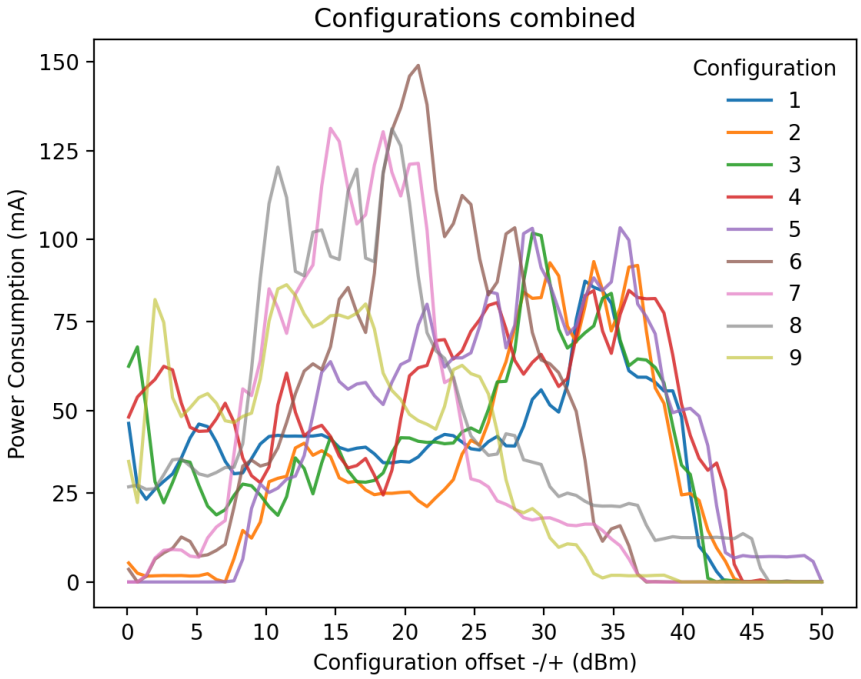


Figure 4.2: Simulation run for all configurations.

eight seem to have the most uniform event triggers for the different report configurations we can see in the configuration execution.

### 4.5.2 Handover events

The events A3 and A5 both trigger handovers within the simulation. This means that event A3 is dependent on A5 and vice versa. Both these events also impact the power consummation of events A1, A2 and A4.

It is interesting that A3 in all cases starts with a lower power consummation for a low offset and decrease more slowly after its peak with a high offset. Judging from the graphs this is most likely because of the influence of the event A5.

### 4.5.3 Signal generation

The signals generation that we used is only one of many options that was available to us. We could, for example, instead have a bigger field in which the eNodeBs are placed. We could also have buildings and other artifacts

that contribute to signal loss. Natural causes could also contribute to signal loss and so the effect of all these situations could be put into further research. We could also have used a different signal generation model instead of FSPL like the Hata model [20]. This model takes into account buildings that may be placed in suburban areas instead of just assuming that we have no signal blockage as FSPL does.

### 4.5.4 Result importance

The results show what might be good report configurations for handovers and other connection decisions, all depending on what power consumption and event trigger amount is preferred. The results could also be used to show the amount of power that is consumed in case of certain report configurations and how this might affect the LTE connection. The results can further be used in research looking towards good report configurations in order to obtain sufficient information to detect attacks like fake base stations. Depending on how much measurement reports actually get sent, the accuracy of the data becomes more useful. However, because we can not send a huge amount of measurement reports to all eNodeBs at regular intervals, it is important that the report configurations are well formed. These well formed report configurations could thus make the difference between noticing that a base station is suspicious versus not noticing any difference between the base stations.

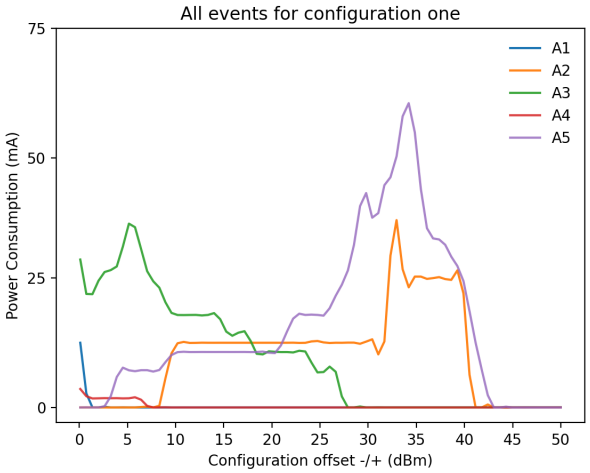


Figure 4.3: The simulation run for all events in configuration one.
The events A1 and A4 are most unused within this spectrum of report configurations. Both these events increase within the report configuration in the graph. The event A3 stably decreases. Event A2 and A5 both rely on decreasing thresholds and seem to be more power consuming the more they decrease.

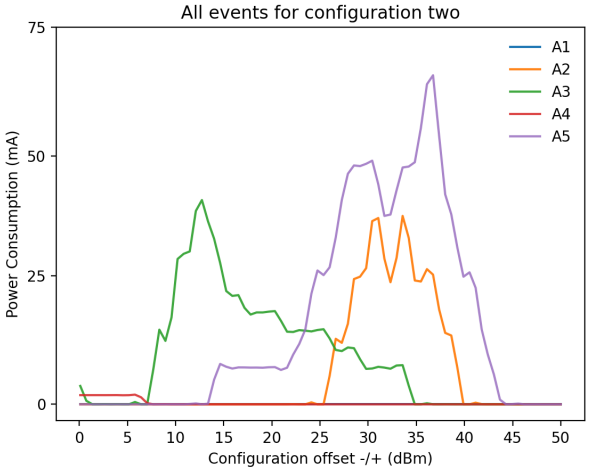


Figure 4.4: The simulation run for all events in configuration two.
The event A1 and A4 are mostly unused as can also be seen in the events for configuration one. The event A3 seems to be stably decreasing however showing a much faster increase for consecutive report configurations. The events A2 and A5 look much like they do in configuration one and have a peak when the dBm values have decreased by around 35dBm.

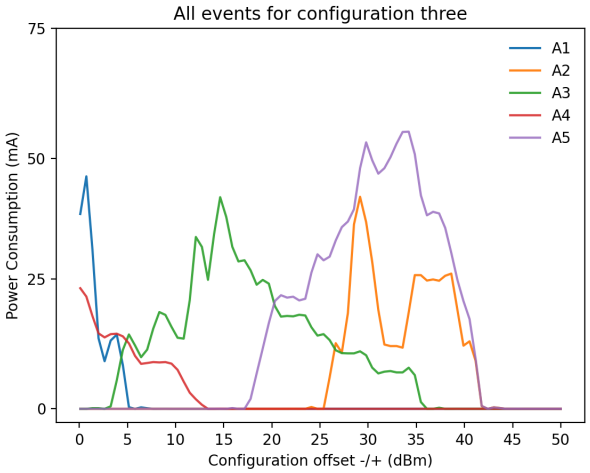


Figure 4.5: Simulation runs for all events in configuration three.
A spike in power consumption for event A1 and A4 can be found at the start of the configuration where their threshold values are around -80dBm. The event A3 now shows a more consistent increase and decrease in power consumption as the offset increases. The events A2 and A5 show much the same thing as in configuration one and two.

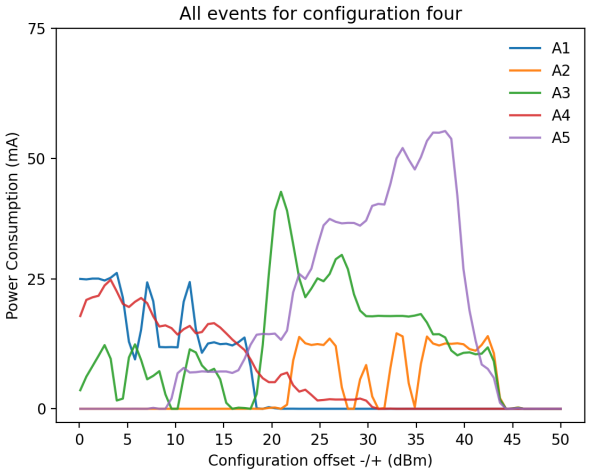


Figure 4.6: Simulation run for all events in configuration four.
Event A1 and A4 start with high values for power consumption. These events have values that start with -90dBm. Event A3 shows an interesting fluctuation at the start of the report configuration sequence, however looks fine after its peak in power consumption. the event A5 looks similar to previous configurations. Event A2 decreases a bit in how much power is used but again shows peaks with lower dBm values.

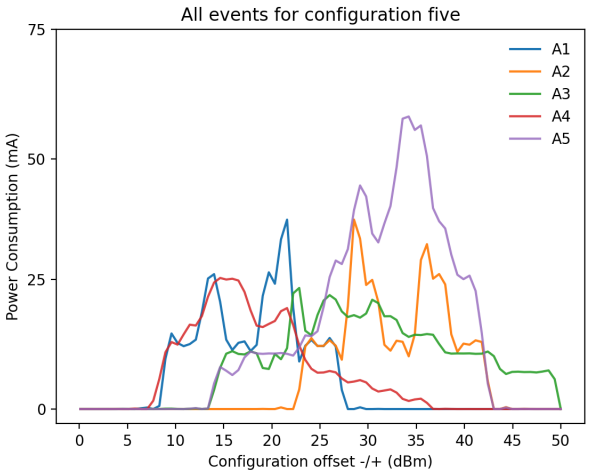


Figure 4.7: Simulation run for all events in configuration five.
This configuration has the most centered offset values. The event A3 seems to need less power for lower dBm values and more power for higher dBm values. The events A1 and A4 use more power for lower dbm values as well as A2 and A5 do.

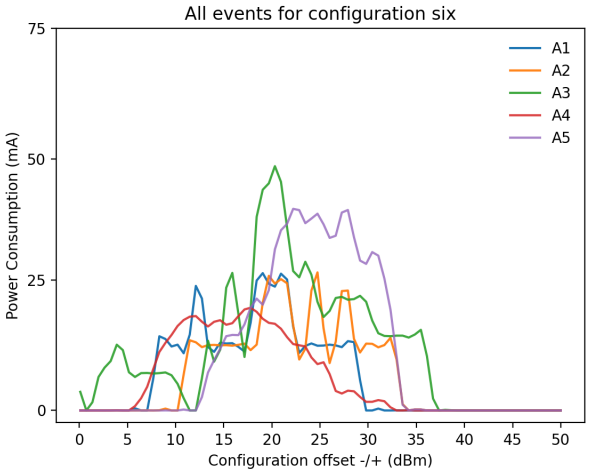


Figure 4.8: Simulation run for all events in configuration six.
The difference between A1 along with A4 and A2 along with A5 is still present. The event A3 still shows more triggers with a higher offset as opposed to a lower offset value.

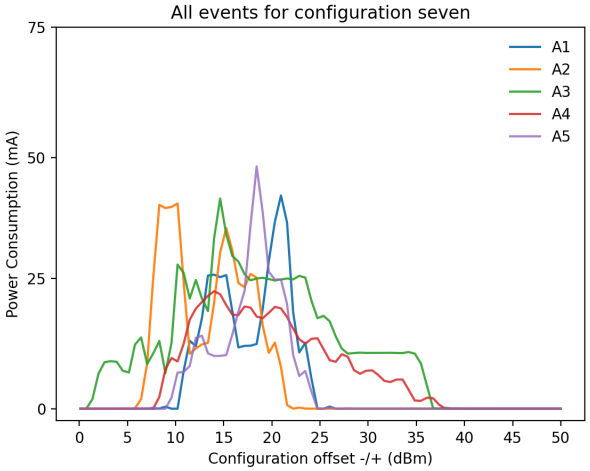


Figure 4.9: Simulation run for all events in configuration seven.
At this point the event A1 and A4 compared to the events A2 and A5 seems to have become very uniform with each other. The event A3 shows also the same things as seen in all previous configurations.

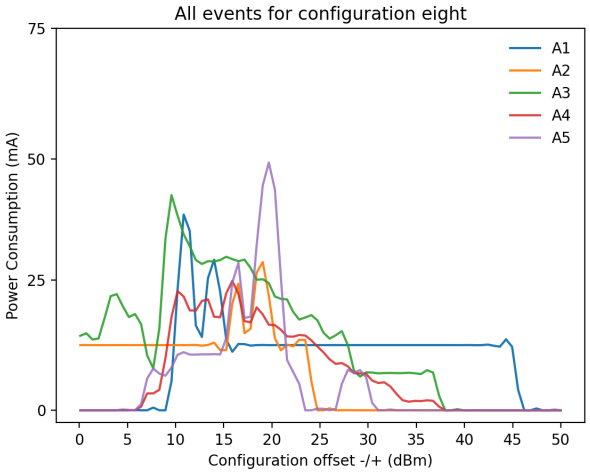


Figure 4.10: Simulation run for all events in configuration eight.
The lower bound for the offset of configuration A3 seems to be cutting off the graph. Also for the event A2 the upper bound seems to be too high and thus cut off from the graph. The A3 event further looks similar as in previous configurations.

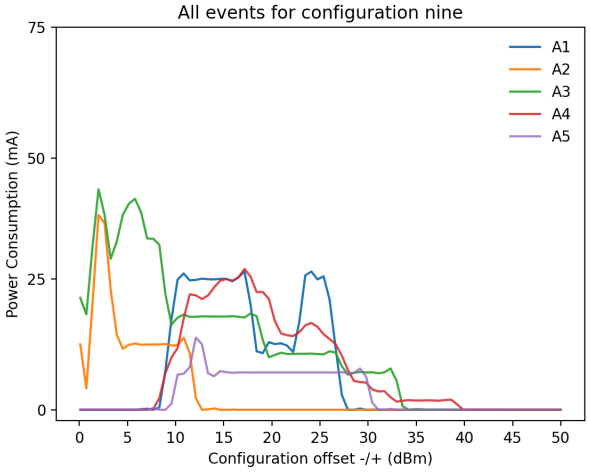


Figure 4.11: Simulation run for all events in configuration nine.
The events A1, A4 and A5 lie well between the bound of the graphs. At offset 20, The value of both A1 and A4 are -80dBm and of A5 are -80dBm and -110dBm. These higher dBm values seem to trigger more measurement reports and thus use more power.

# Chapter 5

# Discussion

The simulation created in this thesis in combination with its executions gives some interesting perspectives on the research question. It is however hard to give concrete insights as research is still missing in this particular area. This section discusses these differences in simulation runs and what we can say about this based on existing information.

## 5.1 Report configuration settings

We found out from this simulation that configurations with dBm values from around -80dBm to -90dBm have the most uniform event triggers. This might be expected because these signals are strong enough to give UEs a good network connection. Additionaly, it would not be interesting to have higher dBm values that are closer to -50dBm trigger events as these signal are already good enough and do not need any setup changes.

## 5.2 Impact of the events

The events A3 and A5 have a big effect on the entire configuration as they also trigger handovers which essentially changes the setup of the connection towards the UE. The effect of event A5 onto A3 might explain why the event A3 has a steeper slope towards the peak where offset values are lower and mostly below an offset of 0dBm. Further, the connection of event A1 and A4 might be explained by how close the signals from the serving eNodeB and the neighbouring eNodeB are to the UE. When eNodeBs are further away or closer they might not trigger at all while eNodeBs that are about the same distance of the serving might be triggered in the same way. The connection between events A2 and A5 might be explained by the fact that the same value is used for when the serving eNodeB becomes worse than the threshold and that there are a lot of neighbours that can become easily better than a certain threshold. The serving eNodeB might already be worse

than this threshold and that would explain why the event A5 gets triggered more often than the event A2.

## 5.3 Simulation setup

There are a significant amount of possibilities for setting up report configurations. Because of handovers, the events A3 and A5 have an impact on each other and the events A1, A2 and A4. In reality eNodeBs may make additional decisions based on the measurement reports they receive and this will thus impact the vastness of the number of possible report configurations even more. In this thesis we chose to make simulation configurations which start with a certain report configuration and consequently change the all the values within the report configuration by an offset of either +0.1dBm or -0.1dBm each time a new execution is preformed. This might not be the most optimal solution and we might think of other ways to analyse this process. Nevertheless, this way of comparing power consumption and measurement report generation shows what is possible in the field.

## 5.4 Event A3

Event A3 has an impact on the other events because of the handover that is performed when the event is triggered. We have chosen the configuration option of this event to go start at some value below 0dBm and subsequently pass this value at a point where the other event also pass a point when they are equal to one another.

The results show a large increase in power consumption when the event A3 is set to this offset of 0dBm. These results also show that the event A3 has a higher power consumption for offsets above 0dBm and a lower power consumption for offsets below 0dBm

## 5.5 Power consumption

The power consumption of the UE at the most inefficient report configuration is measured in this simulation as 150mA over the entire path. Considering most smartphones have a battery of around 2000mAh we can say that traversing the path uses around 13 percent of the entire battery of the UE. We also need to take into account that an average smartphone also has to use power for its screen and apps, and that this 2000mAh can never be fully utilized. This 13 percent is thus a considerable amount for a path of 1 hour and 50 minutes and preferably we need to find a better report configuration so we can waste less power on sending measurement reports.

We have looked at the power consumption of the UE and the various report configuration options that can be chosen by the eNodeB. The eNodeB itself does however have a different power consumption pattern according to report configurations it has send to its connected UEs. Thus, it would be interesting to also look at the impact that the report configuration has on the power consumption of the eNodeB.

## 5.6 Simulation effectiveness

The simulation implements the A1-A5 events along with options for the maximum amount of eNodeBs, the interval between new event triggers and the maximum amount of measurement reports sent. The simulation however lacks options for hysterisis, timeToTrigger and the events other than A1-A5. It would be most interesting to conduct this research on a fully implemented LTE system and use more complex report configurations. However, the lack of research in this specific area made it more interesting to first look at a simple implementation of the event triggers. This thesis thus gives an overview of the basics of event triggers and sets a step toward more fully understood report configuration and connection decisions within an LTE network.

# Chapter 6

# Related Work

In order to apply the research we looked at event generation and fake base station detection separately. Both have some existing literature on them although they are mostly only scratching the surface of the area. We also looked at some research unconnected from these two specific fields.

## 6.1 Event generation

There exists some research on event generation and handovers. We have found a master thesis that already conducts research on the effect of UE quantity and speed on handovers and shows that there are some differences in performance although not significant [3]. Looking at handover performance in combination with event generation might be interesting for future research.

## 6.2 Fake base station detection

This research might also be of use in the field of fake base station detection. We have looked at what might be interesting effects of changes of report configuration variables. When also looking at the usefulness of the measurement reports we may make choices on what report configurations might be preferred.

As an example, a research looking into fake base stations for catching IMSIs looks at the variables transmitted inside the measurement reports and how these can be used in order to say that some eNodeB was never detected before and is not authorized to be there [16].

## 6.3 Additional research

There is also some other research on measurement reports that has nothing to do with the aforementioned fields. For one, there does exist research on the power consumption of measurement reports. Although not directly transferable to this research it is still worth mentioning. This research gives a method for saving 40% of energy on measurement report activity [18]. There also exists research on the processing of measurement reports in order to find a way to increase the speed in which they are parsed [21].

It is important that research on measurement reports is performed since it can for example be used as a partial replacement for coverage analysis and other network analysis [23].

# Chapter 7

# Conclusions

In this paper we have looked at the generation of measurement reports according to the events A1, A2, A3, A4, A5 and *periodical*. We have created a simulation by looking at the official 3GPP LTE specifications. To apply this simulation we have thought of a set of report configurations to systematically test the measurement report generation of LTE. Using the simulation and the report configurations we can execute the simulation and generate graphs which represent the effect of changing the report configurations. We then look at differences between the total power consumption by the measurement reports that were generated by the report configurations.

Configurations that use thresholds with values between -80dBm and -90dBm for their events seem to have the most uniform event triggers. The report configuration using thresholds of -80dBm for all events and an offset of 0dBm for event A3 creates the largest spike in power consummation as opposed to all the other report configurations. A steep slope of the event A3 in an offset below 0dBm might be explained by the influence of the event A5 on the entire simulation. The most inefficient report configuration uses up to 13 percent of a smartphones total battery power when traveling for 1 hour and 50 minutes.

It is still hard to obtain direct conclusions out of the results discussed in this thesis. This thesis can be used to select interesting report configurations for research on power consumption in LTE or for the detection of various attacks through measurement reports. This thesis can also be extended by preforming a different systematic analysis and by using a more advanced simulation.

# Bibliography


[1] Hamad Alrashede and Riaz Ahmed Shaikh. Imsi catcher detection method for cellular networks. In *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, pages 1–6, 2019.

[2] Kwangrok Chang, Ragil Putro Wicaksono, Seiji Kunishige, and Noriteru Takagaki. Lte idle mode optimization improving end user experiences. In *16th International Conference on Advanced Communication Technology*, pages 14–18, 2014.

[3] José Bruno Iñiguez Chavarría. Lte handover performance evaluation based on power budget handover algorithm. page 56, 2014.

[4] Shuo Deng, Ravi Netravali, Anirudh Sivaraman, and Hari Balakrishnan. Wifi, lte, or both? measuring multi-homed wireless internet performance. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, page 181–194, New York, NY, USA, 2014. Association for Computing Machinery.

[5] Etsi. Lte; evolved universal terrestrial radio access (e-utra); radio resource control (rrc); protocol specification (3gpp ts 36.331 version 9.18.0 release 9). ETSI TS 136 331 V9.18.0 (2014-07).

[6] Ramon Ferrús. Lte handover performance evaluation based on power budget handover algorithm. 2014.

[7] 3GPP MCC Frédéric Firmin. The evolved packet core. `https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core`.

[8] 3GPP MCC Frédéric Firmin. The non-access stratum. `https://www.3gpp.org/technologies/keywords-acronyms/96-nas`.

[9] Ruben Merz, Daniel Wenger, Damiano Scanferla, and Stefan Mauron. Performance of lte in a high-velocity environment: A measurement study. In *Proceedings of the 4th Workshop on All Things Cellular: Operations, Applications, Challenges*, AllThingsCellular '14, page 47–52, New York, NY, USA, 2014. Association for Computing Machinery.

[10] Sharetechnote. Lte network architecuture and interface. https://www.sharetechnote.com/html/Handbook_LTE_NetworkArchitecture.html.

[11] Sharetechnote. Multi cell - measurement in lte. https://www.sharetechnote.com/html/Handbook_LTE_MultiCell_Measurement_LTE.html.

[12] Sharetechnote. Rsrp, rsrq, rssi, sinr interplay. https://www.sharetechnote.com/html/Handbook_LTE_RSRP_RSRQ_SINR_Interplay.html.

[13] Sharetechnote. Rsrp(reference signal recieved power). https://www.sharetechnote.com/html/Handbook_LTE_RSRP.html.

[14] Open source srsRAN project contributors. srsran. In *srsRAN*, 2017. https://www.srslte.com/.

[15] srsRAN. Installation guide. https://docs.srsran.com/en/latest/general/source/1_installation.htmls.

[16] Simen Steig, Andre Aarnes, Thanh Van Do, and Hai Thanh Nguyen. A network based imsi catcher detection. In *2016 6th International Conference on IT Convergence and Security (ICITCS)*, pages 1–6, 2016.

[17] M. Tayyab, G. P. Koudouridis, X. Gelabert, and R. Jäntti. Signaling overhead and power consumption during handover in lte. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2019.

[18] YuPeng Wang. An energy saved useless measurement report suspension method for high-speed user in a 3gpp lte-a heterogeneous network. In *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, pages 3461–3464, 2013.

[19] Wikipedia. Free-space path loss, 10 2021. https://en.wikipedia.org/wiki/Free-space_path_loss.

[20] Wikipedia. Hata model, 10 2021. https://en.wikipedia.org/wiki/Hata_model.

[21] Jian Wu, Ning Yu, Bo Zhou, and Yuwen Duan. Rapid processing methods of measurement reports in lte network. In *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, pages 841–844, 2018.

[22] Shichang Xu, Ashkan Nikravesh, and Z. Morley Mao. Leveraging context-triggered measurements to characterize lte handover performance. In David Choffnes and Marinho Barcellos, editors, *Passive and Active Measurement*, pages 3–17, Cham, 2019. Springer International Publishing.

[23] Sui Yanfeng, Yao Qiling, Quan Xiao, and Bai Yan. Lte network structure evaluation method based on measurement report. In *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, pages 1–4, 2014.