Exploring Redirection and Downgrade Attacks on Long-Term Evolution Network

Park Sang Jun
National University of Singapore
School of Computing
A0170243R
+65 94569430
E0191791@u.nus.edu

Jiahan Yu
National University of Singapore
School of Computing
A0210016E
+65 93728115
E045467@u.nus.edu

Calvin Tantio
National University of Singapore
School of Computing
A0160601X
+65 84020996
E0053483@u.nus.edu

Valerie Tan Yi Jia
National University of Singapore
School of Computing
A0185679E
+65 92351476
valerie.tan@u.nus.edu

Leong Eng Sea
National University of Singapore
School of Computing
A0161390L
+65 97835861
E0072487@u.nus.edu

ABSTRACT
With the development of 4G LTE technology and its global deployment, mobile subscribers have been able to enjoy higher capacities and faster speeds of mobile communication. This, in turn, leads to the rapid and massive adoption of the technology worldwide. In its "Mobile Economy" report, GSMA (Global System for Mobile Communication) predicted that the technology will make up 53 per cent of the global connections by 2025. While 4G LTE suite is believed to be an improvement over the previous 2G and 3G technologies in various aspects, such as functionality, security and privacy, as LTE adoption becomes more prevalent, it becomes increasingly more important for mobile users to be aware of the potential security risk that it entails, and protect themselves against attacks. In this paper, we present one of the possible practical attacks that can be launched against LTE devices.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *security and protection*;
C1.3 [**Processor Architecture**]: Other Architecture Styles – *cellular architecture*

General Terms
Experimentation, Security

Keywords
4G LTE, LTE security, Redirection attack, Downgrade attack, Denial-of-Service, Software Defined Radio

1. INTRODUCTION
LTE or Long Term Evolution is the most popular fourth generation (4G) mobile telecommunication standard that is developed to be the successor of second generation Global System for Mobile Communications (2G/GSM) and third generation Universal Mobile Telecommunication Systems (3G/UMTS). The development of LTE has not only improved the functionalities of its predecessors but also strengthened some of the security measures in mobile communication technologies.

Early 2G technologies are considered vulnerable and are exposed to various attack vectors. For instance, there is a lack of mutual authentication between the mobile devices and the base stations. This means that an attacker can set up a rogue 2G GSM network and convince the mobile devices to connect to it. Once this is achieved, the attacker can then track the mobility of the mobile devices and their users.

This vulnerability was later mitigated when 3GPP (3rd Generation Partnership Project), an organization in charge of developing protocols for communication technologies, introduced 3G technologies. This is because 3G standard requires mutual authentication and encryption between mobile devices and base stations. The recent 4G standard further tightens this measure by carrying out mutual authentication and encryption in more situations than required in 3G standard.

This leads many to believe that 4G LTE standard is secure and that privacy is guaranteed. While it is true that attacks that are previously possible against LTE's predecessors are considered difficult to succeed in LTE, this paper shows that they are not entirely impossible.

2. LTE ARCHITECTURE
This section serves as an introduction to LTE infrastructure and the process on how a mobile device gets connected to and initiates data transfer in an LTE network.

2.1. LTE Infrastructure
LTE Infrastructure consists of three main components: User Equipment (UE), E-UTRAN (Evolved-UMTS Terrestrial Radio Access Network) and EPC (Evolved Packet Core). These three

components are collectively referred to as EPS (Evolved Packet System).

2.1.1. User Equipment (UE)

UE refers any communication device made for end-user, such as a mobile device or a tablet which comes with a mobile broadband adapter. Every UE that supports LTE requires a Universal Subscriber Identity Module (USIM). USIM has a similar function to the SIM in a GSM device. USIM stores International Mobile Subscriber Identity (IMSI), which uniquely defines an LTE user as a subscriber in the wireless LTE network.

2.1.2. Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN)

E-UTRAN consists of multiple evolved NodeBs (eNodeB or eNB), also known simply as base stations. E-UTRAN stands in between UE and EPC, and relays messages and/or services from UE to EPC and vice versa. Each eNodeB is connected to other eNodeBs via the X2 interface and to the EPC by the means of the S1 interface. Moreover, an eNodeB communicates with a UE through a series of access network protocols known as Access Stratum (AS). One of the more prominent AS messages include Radio Resource Control (RRC) messages, which are used to locate a UE during the paging process (explained in a later section). Figure 1 below shows the illustration for the E-UTRAN architecture.

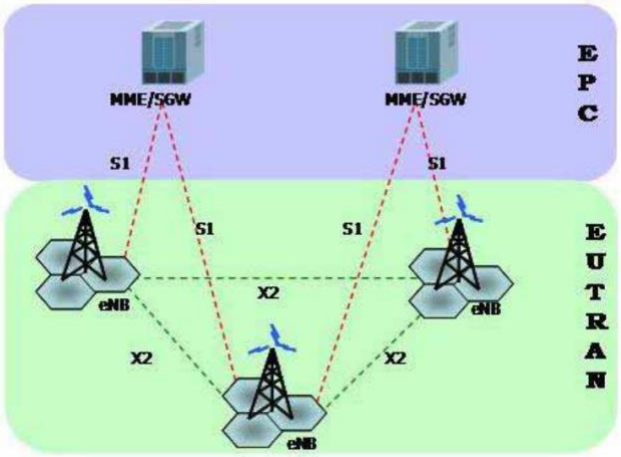

Figure 1. Architecture of E-UTRAN

2.1.3. Evolved Packet Core (EPC)

EPC is a framework for providing converged voice and data of a 4G LTE network. The most important components of EPC that we will focus on in this paper is the Mobility Management Entity (MME) which allocates resources to UEs, manages session states and authenticates and tracks a UE across the network. The MME communicates with a UE through a protocol known as Non-Access Stratum (NAS).

Other components of the EPC include

- Serving Gateway (S-gateway), which routes data packets through the access network
- Packet Data Node Gateway (PDN GW), which acts as the interface between the LTE network and other packet data networks
- Policy and the Home Subscriber Server (HSS), which contains user-related and subscriber-related information and provides support functions in mobility management, call and session setup, user authentication and access authorization.

The EPC architecture is shown in Figure 2.

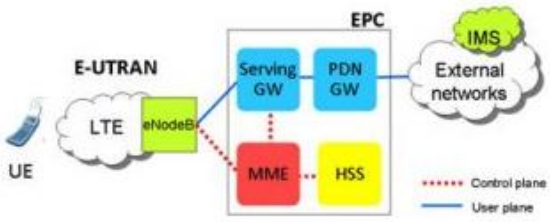

Figure 2. Architecture of EPC

2.2. LTE Deployment

Mobile network operators provide LTE services by deploying LTE components in a geographical region. This region is referred to as a service area. A service area is divided into many Tracking Areas (TAs), each of which is managed by a MME. Each TA is further divided into regions known as "cells". An eNodeB is placed in each cell to manage that particular cell.

A UE is able to identify the mobile operator through the operator specific information broadcasted by the eNodeB. This, in turn, allows the UE to start a connection to the network by initiating the *Attach* Procedure. Having established a connection successfully, the UE will then have access to mobile services based on its mobile subscription. Subsequently, the UE uses TAU procedure to update the mobile network about its location if the UE enters a new TA that the UE has yet to register with the network (among other reasons which will be specified later).

2.3 LTE PRIVACY SECURITY

LTE increases privacy by minimising the transmission of IMSI, which is the permanent identity of a mobile subscriber. Instead, after an LTE device has successfully carried out the *Attach* procedure, GUTI (Globally Unique Temporary Identifier) will be assigned to replace IMSI as the subscriber's identity. GUTI is also periodically changed so it becomes harder for an attacker to track a user's data transmission (traffic) in the LTE network.

LTE increases security through Authentication and Key Agreement (AKA) protocol, during which the UE and the network agree on a session key to secure subsequent NAS and AS messages. This process is done during EPS Mobility Management (EMM) procedure.

2.4. LTE CONNECTION

This section introduces the process of a UE in moving from the Idle state (the UE does not have any active connection with any eNodeB) to a connected state (the UE has an active connection with an eNodeB) and vice versa.

2.4.1. Paging in LTE

Paging is a procedure whereby a MME tries to locate a UE in order to deliver services to the UE. Some examples of services delivered will be messages or incoming phone calls. MME broadcasts a paging message to all the eNodeBs in the TA it manages, and at the same time starts a T3413 timer (paging timer). Upon receiving the paging message from the MME, all eNodeBs will, in turn, broadcast an RRC paging message to locate the UE in its respective cell. The RRC paging message contains the identity of UE in the form of:

- IMSI if the UE has not yet connected with the network, after which the UE will initiate an *Attach* procedure to receive a GUTI.
- GUTI (Globally Unique Temporary Identifier) if the UE has previously initiated Attach procedure with the network and has been assigned a GUTI by the network, after which the UE will receive a radio channel through Random Access Procedure to initiate data transfer.

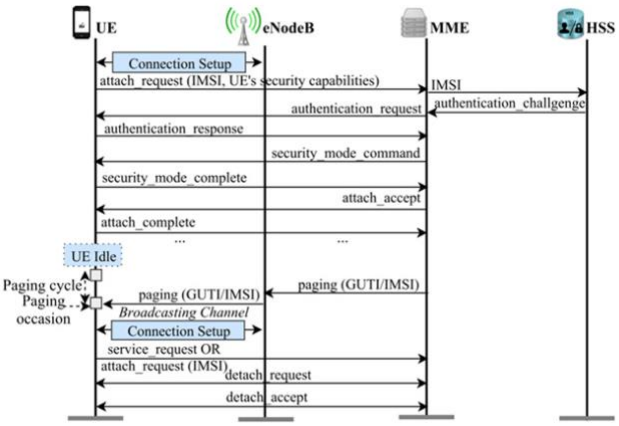

Figure 3. Attach, Paging and Detach in LTE

2.4.2. LTE Attach Procedure

(1) **Random Access Procedure**: The procedure is used by the UE to initiate a data transfer and obtains uplink timing information from the initial handshake. After synchronizing to the network and reading the configuration information in System Information Block 2 (SIB2), the UE can send a preamble to the eNodeB in order to access the network. The eNodeB in turn send back a Random Access Response. The random access procedure is also used when the UE responds to a paging message.

(2) **RRC Connection Establishment**: Having received the uplink frequency, the UE adjusts the timing and sends an RRC Connection request to the eNodeB. The eNodeB responds with an RRC Connection message. The message creates the signalling radio bearer (SRB) in acknowledged mode, indicating the establishment of the RRC Connection. It allows the UE to inform the network of its connection purpose (e.g. Attach, TAU or Service Request).

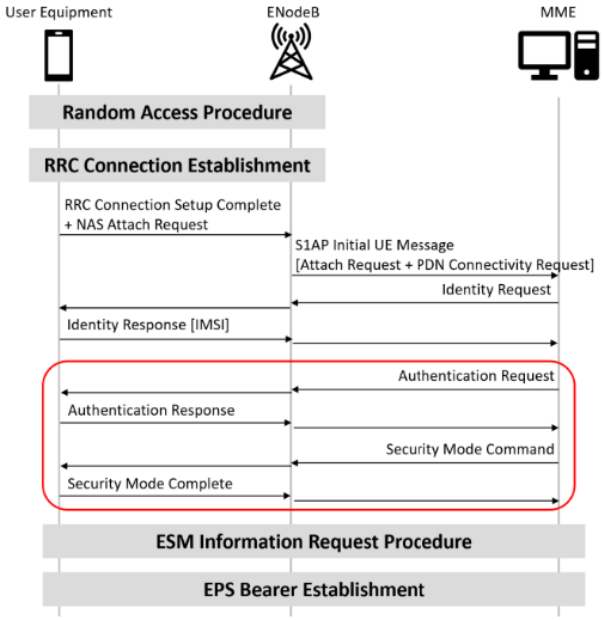

Figure 4. LTE Attach Procedure

(3) **Attach Request and Initial UE message**: Having set up RRC Connection, the UE sends an Attach Request to the eNodeB with its IMSI or old GUTI. The eNodeB forwards the attach message with PDN Connectivity Request to new MME. The PDN connectivity request is used by the UE to request for the setup of default EPS bearer to the PDN. EPS bearer is a virtual connection between the UE and the PDN GW, which allows identification of data sent between the 2 endpoints.

(4) **Identification Procedure**: Since the MME has changed since detach, the new MME uses GUTI received from the UE to derive the old MME, and send an Identification Request (old GUTI, Attach Request message) to the old MME to request the IMSI. If the UE is unknown in old and new MME, the new MME sends an Identity Request to the UE to request the IMSI. The UE sends back an Identity Response containing its IMSI.

(5) **Authentication and Setup Encryption**: The MME challenges the UE by sending an Authentication Request to the UE. The UE is required to do computations and attach the answer in Authentication Response. If the authentication fails, the MME will reject UE's connection. Otherwise, the MME will initiate a NAS security procedure in which the encryption and integrity protection algorithm is attached to the message. Since then all messages will be encrypted.

(6) **ESM Request Procedure**: EPS Session Management (ESM) Request Procedure is used by the network to acquire protocol configurations like the Access Point Network (APN).

(7) **EPS Bearer Establishment**: EPS Bearer Establishment indicates Attach Request has been accepted by the network and data service is established. Next, the UE will respond to Attach Accept message and sends back an Attach Complete. It signifies the conclusion of the Attach Procedure. Once it is completed, in subsequent requests, the UE can perform data transfer over encrypted channels without going through these security procedures again.

After the UE successfully enters the connected state, the eNodeB forwards the TAU/Service Request message to MME, following which stops the T3413 timer. Next, the eNodeB sets up the security configurations in UE, and provides the UE with LTE network services.

2.4.3. TAU Request and Response

UE notifies the MME through a Tracking Area Update (TAU) and also includes its network modes. The UE can trigger a TAU only when it is in the RRC Idle or RRC connected state. If a TAU Request is rejected by the eNodeB, the UE will initiate Attach Procedure.

Below are some events that will trigger a TAU:

(1) The UE moves to a new TA which is not included in the list of TAs the UE is registered to.

(2) When T3412 timer expires. The value of the T3412 is initialized by the Attach Accept message during the Attach procedure.

(3) MME load balancing. It happens if the eNodeB releases RRC connection with the cause "Load Balancing TAU Required".

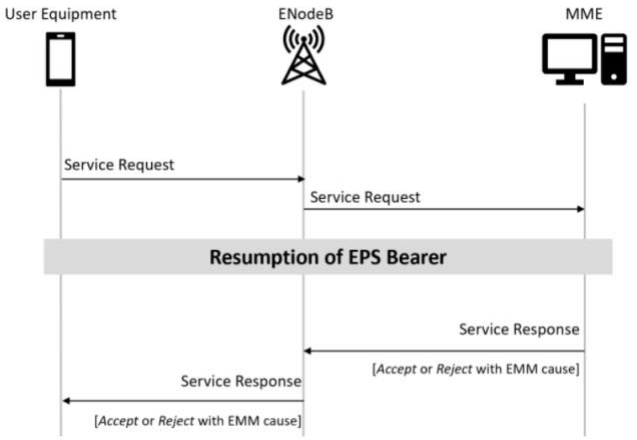

Figure 5. Serve Request and Response

2.4.4. Serve Request and Response

UEs will go into RRC Idle state during inactivity. When it has pending data to be sent, the UE will send Service Request to the network. The message requests to resume previously established EPS bearers. The MME will reply with a Service Response Accept if the resumption of EPS Bearer is successful. Otherwise, the MME reject with EPS Mobility Management cause.

3. ADVERSARY MODEL

In this section, we discuss the various attack vectors against an LTE network. We also specifies the model that we use for the attack that we carry out. In general, we not only deny a mobile LTE subscriber of LTE services, but also force the subscriber to connect to a more vulnerable 2G GSM network. Once the subscriber is connected to the 2G GSM network, various known attacks against 2G GSM network can be carried out against the subscriber.

4. EXPERIMENTAL SETUP

In this section, we discuss our low-cost experimental setup using easily available open source software and LimeSDR with simple programming skills and initial understanding of LTE specification.

Requirements:

- Ubuntu 18.04 64-bit
- Software-defined radio with UHD and SoapySDR support
- LTE and GSM handset

4.1. Hardware

This section introduces the hardware used in demonstrating the adversary attack against an LTE device.

4.1.1. LimeSDR Mini

The LimeSDR-Mini is a low-cost software defined radio board that can support any type of wireless communication standards and has the capability to receive and transmit frequency ranging from 10MHz to 3.5GHz. The LimeSDR-Mini can also send and receive LTE, UMTS, GSM, LoRa, Bluetooth, Zigbee, RFID, and Digital Broadcasting.

Two LimeSDR-Mini was used during this experiment for the purpose of setting up as a LTE network and the GSM network. LimeSDR-Mini was used as the eNodeB when setting up the LTE Network.

4.1.2. Mobile Phone

Commercial mobile phone with LTE support is used for this project to act as the UE. The mobile phone used were the *OnePlus 5T* and *iPhone XR.*

4.2. Software

This section introduces the software used in demonstrating the adversary attack against an LTE device

4.2.1. srsLTE

srsLTE is an open source 4G LTE software suite which includes the required component for setting up a complete end-to-end LTE network:

- srsUE - complete SDR LTE UE (User Equipment)
- srsENB - complete SDR LTE eNodeB (Base station)
- srsEPC - light-weight LTE EPC (Core Network) implementations with MME, HSS and S/p-GW.

Another reason for using srsLTE is that it works best with LimeSDR Mini.

4.2.2. LimeSuite

LimeSuite is a collection of software supporting several hardware platforms including the LimeSDR, drivers for the LMS7002M transceiver RFIC, and other tools for developing with LMS7-based hardware. Installing the Lime Suite enables many SDR applications such as GQRX to work with supported hardware through the bundled SoapySDR support module.

4.2.3. GSM Network

The GSM network was set up using open source software from the Osmocom project. It consists of the following components:

- OpenBSC
- OsmoTRX
- OsmoBTS

Using the telnet interface of OpenBSC, it was possible to send spoofed message and make calls to users connected to the GSM network.

5. RESULTS

This section shows the experimental results that the we have managed to achieve.

5.1. Spoofing of Messages and Phone Calls

By modifying the HLR database, it was possible to create new false users with any extension. The attacker could telnet into OpenBSC to send spoofed messages or phone calls to any user connected to the GSM network.

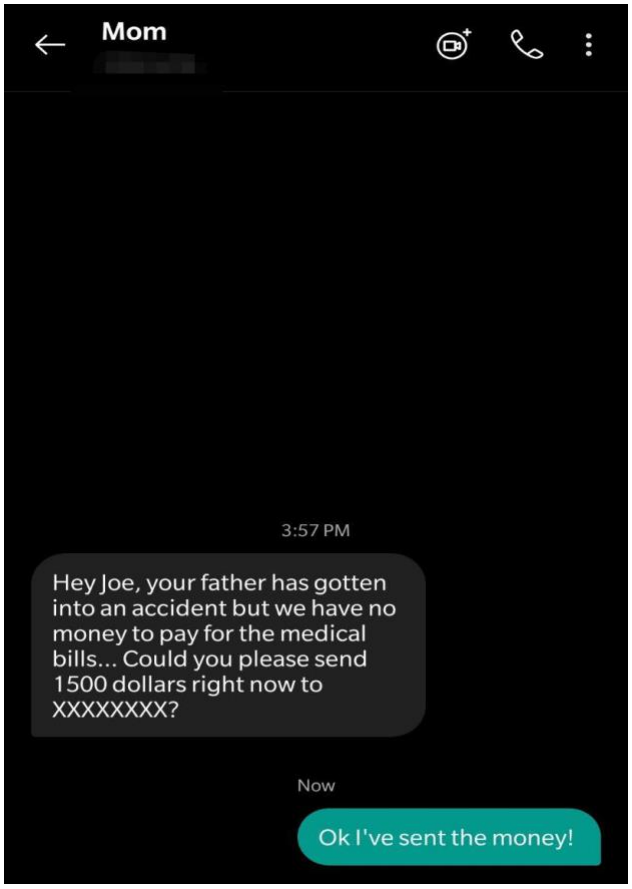

Figure 6. Spoofed Message from Selected Extension Number

5.2. Man-in-the-middle Attack

If two users were connected to the network, the attacker running the network would not be able to view the plaintext as the network is end-to-end encrypted. However, the cipher suite used in encryption of messages uses the stream cipher A5/1 which has been broken for more than a decade using ciphertext-only cryptanalysis. Hence, it is trivial to decrypt any communication over the attacker's network. Combined with the spoofing capabilities of the attacker, it is easy to see how an attacker might be able to insert himself to any conversation between any two users in his network and impersonate them.

6. DISCUSSION

Discovering the vulnerabilities in LTE Network and its undesirable effect to end-users, the reliance on technology today also shows the importance to emphasise on LTE security. At the same time, there are possible trade-offs between security and end-user performance. How do we weigh them? In this section, we will discuss how the equilibrium points in the trade-offs have shifted.

Security vs. Availability: There's a vulnerability in LTE RRC protocol specification that allows adversary to obtain unprotected measurement reports from UE. There are unprotected reports for the purpose of troubleshooting to ensure the availability of UE connectivity.

Security vs. Performance: UEs are required to reboot or re-insert SIM to regain network services after DoS attacks. Frequent unsuccessful Attach request from UE would increase signalling load on network. Hence, this behaviour is as per LTE specification: when network denies services for valid rejects, UE restricts itself from reinitiating any *Attach* procedure in order to conserve battery power.

7. CONCLUSION

In this paper, we have discussed the vulnerabilities in LTE access network that could lead to potential confidentiality and availability threats impacting users of LTE. This paper brings to light the need and importance to properly weigh out the correct trade-offs between security and other requirements that will affect the UE network performance.

8. ACKNOWLEDGEMENTS

We would like to extend our gratitude to the CS3235 Computer Security teaching team for the opportunity to embark on this project. We specially thank A/P Hugh Anderson for the guidance, feedback and the specific hardware equipment provided, without which this project could not have been accomplished.

9. REFERENCES

[1] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.(January 2016). DOI: 10.14722/ndss.2016.23236

[2] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert. Practical attacks against privacy and availability in 4g/lte mobile communication systems. In Network and Distributed System Security Symposium. NDSS, 2016

[3] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. *ACM Trans. Program. Lang. Syst.* 15, 5 (Nov. 1993), 795-825. DOI: http://doi.acm.org/10.1145/161468.16147.

[4] Ding, W. and Marchionini, G. 1997. *A Study on Video Browsing Strategies*. Technical Report. University of Maryland at College Park.

[5] Dialogic. User Equipment(UE) Retrieved from https://www.dialogic.com/glossary/user-equipment-ue

[6] EventHelix.com . 2012. LTE Attach and Default Bearer Setup Messaging. Retrieved from http://www.eventhelix.com/lte/attach/LTE-Attach-Messaging.pdf#page=3

[7] EventHelix.com. 2015. LTE Random Access Procedure. Retrieved from https://www.eventhelix.com/lte/random-access-procedure/lte-random-access-procedure.pdf

[8] EventHelix.com. 2019. LTE Attach and Default Bearer Setup.(March 2019). Retrieved from https://www.eventhelix.com/lte/attach/lte-attach.pdf

[9] EventHelix. 2017. Tracking Area Updates in an LTE network. (May 2017). Retrieved from

https://medium.com/long-term-evolution/tracking-area-updates-in-an-lte-network-32b2c7d045e6

[10] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands, April 01 - 06, 2000). CHI '00. ACM, New York, NY, 526-531. DOI: http://doi.acm.org/10.1145/332040.332491.

[11] Global Scenario: LTE deployment trends and developments. (April 2018). Retrieved from http://www.tele.net.in/index.php?option=com_k2&view=item&id=23442:global-scenario-lte-deployment-trends-and-developments

[12] Google. Default Bearer Setup. Retrieved from https://sites.google.com/site/amitsciscozone/home/lte-notes/default-bearer-setup

[13] Gkioulos, V., Wolthusen, S. D., & Iossifides, A. A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE).

[14] Kevin Beaver. 2018. LTE(Long Term Evolution). (June 2018). Retrieved from https://searchmobilecomputing.techtarget.com/definition/Long-Term-Evolution-LTE

[15] MyriadRF. Lime Suite. Retrieved from https://myriadrf.org/projects/software/lime-suite/

[16] Margaret Rouse. Evolved Packet Core(EPC). Retrieved from https://searchnetworking.techtarget.com/definition/Evolved-Packet-Core-EPC

[17] Netmanias. 2013. LTE Security I: Concept and Authentication. (July 2013) Retrieved from https://www.netmanias.com/en/post/techdocs/5902/lte-security/lte-security-i-concept-and-authentication

[18] Paschal A. Ochang and Philip J. Irving. 2016. Evolutionary Analysis of GSM, UMTS and LTE Mobile Network Architectures. Retrieved from https://pdfs.semanticscholar.org/0ebe/b97769f73d0d0b66ed02d652d4f141d974ad.pdf

[19] srsLTE Documentation Release 19.6.0 [‘Software Radio Systems’].(July 2019) Retrieved from https://buildmedia.readthedocs.org/media/pdf/srslte-docs/latest/srslte-docs.pdf .

[20] Techopedia. International Mobile Subscriber Identity(IMSI). Retrieved from https://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi

[21] Tavel, P. 2007. *Modeling and Simulation Design*. AK Peters Ltd., Natick, MA.

[22] Zeljka Zorz. 2018. New LTE attacks open users to eavesdropping, fake messages, location spoofing. (March, 2018). Retrieved from https://www.helpnetsecurity.com/2018/03/05/lte-attacks/