# LTE is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks

Teng Fei and Wenye Wang
Department of Electrical and Computer Engineering
*North Carolina State University, Raleigh, NC 27606*
Email:{tfei3, wwang}@ncsu.edu

***Abstract*—Recent years have witnessed the rapid growth of mobile users, which further accelerates the deployment of mobile communication networks, especially LTE networks, due to its high data rate, as well as comprehensive functionality. Compared to its predecessors, LTE networks have incorporated a number of security measures specified by 3GPP, including amalgamation of temporary identities, mutual authentication, and enhanced signaling procedures, which are meant to protect the system and individual subscribers against various forms of attacks. However, as we show in this paper, flaws in real-world implementation render commercial LTE systems vulnerable to several attacks, including identity spoofing and denial-of-service (DoS), which have severe impacts on subscriber's data integrity, QoS, and even privacy. Specifically, we identify the vulnerabilities by carefully analyzing LTE specifications, list possible attacks targeting these vulnerabilities, and successfully implement two attacks on a commercial LTE network with a USRP-based testbed. Our work reveals severe security risks in real-world LTE systems, which call for immediate enhancement from both standardization organizations and cellular service providers.**

***Index Terms*—LTE, Vulnerabilities, Attacks**

## I. INTRODUCTION

During the past two decades, mobile devices have become an important component in the communication system. Starting from the Second Generation Global System (2G/GSM) and third generation Universal Mobile Telecommunication Systems (3G/UMTS), cellular network extends to everywhere in the world. Global mobile data traffic increased 63 percent in 2016 and also reached 7.2 exabytes per month [1]. Consequently, the fourth generation "Long Term Evolution(4G/LTE)" systems are being deployed widely. By the end of 2017, over 55 countries have reached a penetration rate over 70 percent [2]. And there were 3.2 billion LTE subscriptions around the world at the end of March 2018 [3]. As a result, cellular network, especially LTE, does not only affect society as a whole, but also has tremendous impacts on each individual.

Early 2G and 3G systems were known to have several vulnerabilities. For example, although a Temporary Mobile Subscriber Identity (TMSI) is used instead of the permanent one called International Mobile Subscriber Identity (IMSI), the 3GPP standard does not specify when and how to update this temporary identity. As a result, this identity can be static for hours or days. To this end, Arapinis et al. collect TMSIs and map it to specific users, which leads to leakage of subscriber's location [4]. Another vulnerability is that 2G systems lack mutual authentication between subscribers and base stations, such that it is feasible for an attacker to set up a fake base station and force the illegitimate user to connect to it or masquerade as a legitimate user receiving phone calls and messages. For instance, Nico et al. establish a malicious UE and response the paging messages instead of the legitimate one, which causes denial of service [5]. A rogue base station can even track subscriber's traffic in [6].

As 2G and 3G systems have such vulnerabilities, the 3GPP strengthens LTE specification in many aspects. First it proposes the Global Unique Temporary Identifier (GUTI) instead of the TMSI as subscriber's identity [7], which updates much more frequently than TMSI, thus more difficult to be sniffed and mapped to a subscriber. Second improvement is that 3G and LTE network add mutual authentications by using authentication and agreement (AKA) protocols, which makes it almost impossible for an attacker to set up a rogue base station and reveal the data that is transmitted through the air interface. From the network architecture's perspective, data is transmitted with pure packet-switching technology over LTE network instead of involving circuit-switching in 3G network. This provides the LTE network a more flexible way of traffic handling, and also protects the confidentiality of subscriber's data as more spectrum sniffing will be needed.

Owing to high speed that LTE network can provide, much more applications are developed comparing to GSM/3G network, including streaming videos in real time, online banking and navigation in LTE network. However, such convenience comes at the cost of security though much effort has been made in LTE security enhancement, implementation flaws still exist. Altaf et al. [8] trigger paging messages in order to extract user identities to expose subscriber's location. And even GUTI is used, the user's identity is still not safe. Hong et al. [9] show that changing patterns of GUTI can be tracked, which means that the same location tracking attack can also be applied the same way as TMSI. As so many problems appear in LTE network, we ask the following research question: What vulnerabilities still remain in LTE network and what attacks can we perform to sabotage subscriber's privacy?

In order to identify the vulnerabilities in LTE network, we make the following contributions:

- We reveal two vulnerabilities in LTE network.
- We implement identity spoofing and Denial-of-Service attacks on commercial devices based on the revealed

vulnerabilities.

This paper is organized as following. Section II discusses some preliminaries. Section III introduces our experimental and adversary set up. Section IV introduces revealed vulnerabilities and attacks in LTE network. Section V gives the conclusion.

## II. Preliminaries

This section briefly reviews LTE architecture as well as attach procedures and RRC messages that are relevant to the vulnerabilities and attacks considered in this paper.

### A. LTE architecture

As shown in Fig. 1, LTE network consists of three entities: User Equipment (UE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and Evolved Packet Core (EPC). UE refers to the cellular device equipped with a SIM card which has a universal subscriber identity module(USIM) application on it [10]. E-UTRAN is a geographical area which consists of several eNodeBs (base station) which can provide LTE network services to UE within the cell. Evolved Packet Core (EPC) is in charge of providing UEs with network service. The EPC consists of MME, HSS and many other core network components. MME plays an important role on attach and authentication of the mobile device [11] that are key procedures where we find vulnerabilities. It is also responsible for keeping track of UE's locations. The HSS stores subscriber's identities along with the cryptographic keys, which are used to generate authentication challenges and symmetric session keys for each subscriber.

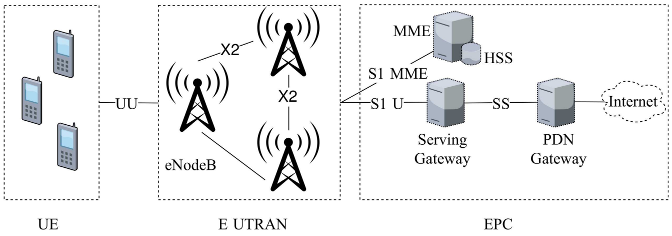


Fig. 1. LTE architecture.

### B. Attach procedure in LTE

A simplified attach procedure is shown in Fig. 2. When UE initiates the attach procedure, it first scans the surrounding spectrum to acknowledge eNodeBs with the highest power and then it will perform the random access procedure. Such random access procedure is necessary since UE needs to synchronize its clock with the network and also be assigned a dedicated channel to receive messages. It will then set up the RRC connection with the eNodeB. After RRC connection establishment, UE will send an attach request message containing its temporary identity to MME, which will later retrieve the materials for the authentication. Then these material will be contained in the authentication request message that will be sent to UE. After receiving the message, UE will send back an authentication response message to authenticate the network. If authentication is successful, then the UE will enter the security complete mode. With the message *attachaccept* arriving, the attach procedure is complete. During initial attach, IMSI is transmitted through LTE air interface within plaintext messages. This gives an adversary a chance to receive these messages and IMSI inside.

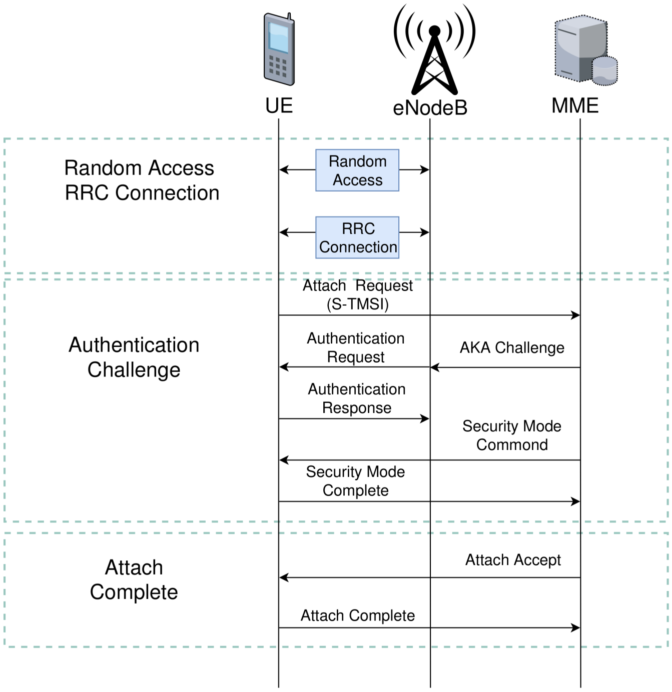


Fig. 2. Attach procedures in 4G LTE.

### C. RRC protocols

The radio resource control (RRC) protocol is used in LTE on the air interface, it is part of LTE control plane. It has following main functions according to [12], broadcast of system information, paging, RRC connection between the UE and E-UTRAN, and mobility functions. In this paper, we concentrate on RRC broadcasting messages. In LTE network, UE should listen to these messages all the time whether it is in `RRC_CONNECTED` mode or `RRC_IDLE` mode [12]. These messages include important system information, cell selection parameters, neighbouring cell information and common channel configuration information. Among them, system information is basically the most important one. It consists of the Master Information Block (MIB) and a number of System Information Blocks (SIB) messages. The MIB is broadcasted on the Physical Broadcast Channel (PBCH), while SIBs are sent on the Physical Downlink Shared Channel (PDSCH) through Radio Resource Control (RRC) messages. However, these messages are not encrypted and broadcasted periodically which makes itself vulnerable to eavesdroppers.

### D. Related work

Vulnerabilities in LTE networks have been addressed by a few existing studies. In [13], Lichtman et.al find vulnerabilities in physical channels and signals. Instead of performing traditional attacks by interfering signals sent by base station, they achieve to jam specific physical channels. This methodology requires much less transmission power and improves efficiency. However, a common issue in jamming is that although it does do harm to LTE network, it does not provide any useful information which means that jamming can not hurt subscriber's privacy.

In [9], authors perform GUTI reallocation and analyze the changing pattern of it such that user's identities and location will be in danger. They exploit Circuit Switched Fall Back (CFSB) service in LTE network by making silent calls (Call the victim and hang up before it rings) to trigger paging messages in the air. Then they eavesdrop the spectrum to collect GUTI. However, according to LTE specifications, the assignment and changing pattern of GUTI are determined by network operators which implies that the data set to find this pattern should be re-collected whenever there are changes of location. And the size of the data set is flexible such that it is hard to find out how much time it costs to finish the attack.

In another work [8], the authors demonstrate three attacks against LTE network by injecting $TrackingAreaUpdate$ messages with different details, which leads to service downgrade and denial-of-service. This works since those messages are not encrypted and not authenticated by UE. However, these attacks involve generating new messages transmitted through air interface. As a result, if there is a network monitor, the messages might be sniffed and recognized as modified.

## III. ADVERSARY MODEL AND EXPERIMENTAL SETUP

### A. Adversary Model

In this section, we consider our adversary models. The adversary has a full knowledge of LTE specification and we assume that it is in the same geographical location as the victim. However, the adversary should not have direct contact with UE, EPC or any other entities in LTE network.

A passive adversary has the ability to silently sniff over LTE air interface. Consequently, both UE and network can not know its existence. An active adversary is able to establish a rogue base station or a malicious UE as long as it has necessary parameters of a legitimate base station or a LTE subscriber.

Generally, both adversaries have the ability to change some parameters to play as different UEs and eNodeBs. For example, the malicious UE is able to change its IMSI and a rogue base station is also capable of adjusting its frequency bands, public land mobile network (PLMN) identity, cell identity and etc. There are many messages involved in the attack as shown in Fig. 3. For simplicity, we limit ourselves to messages containing useful information and indicate which channels they use to transmit.

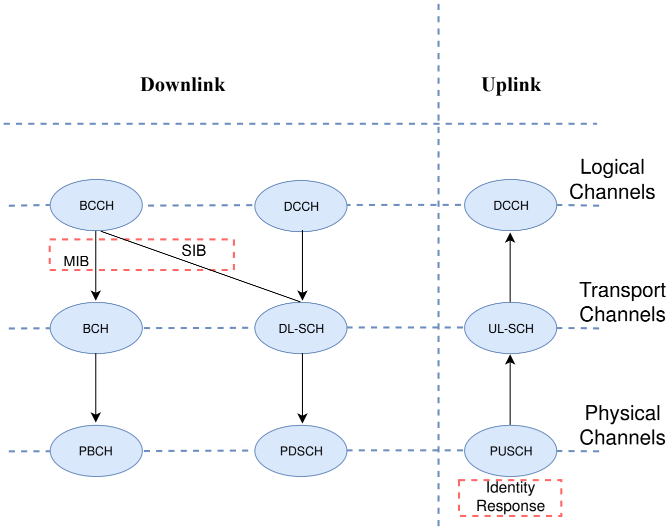


Fig. 3. Three messages involved in our attacks.

### B. Experimental setup

Software and hardware in LTE network are thought to be expensive and not open sourced. However, the appearance of USRP and free open soured software srsLTE [14] changes this situation, and is exploited by our attacks.

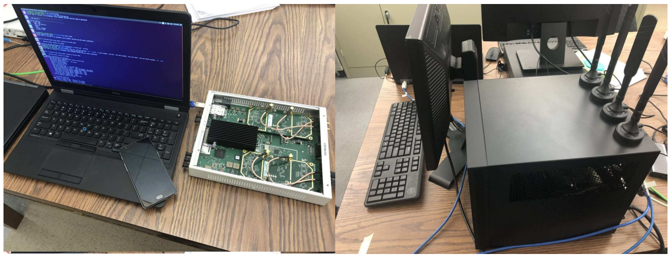
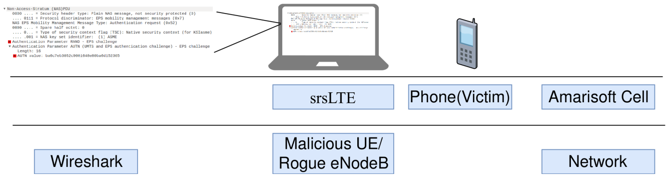


Fig. 4. Experimental Setup: Our testbed consists of Amarisoft Cell and a high performance PC connected to USRPX310.

The basic experimental setup is shown in Fig. 4. We set up our testbed with USRPx310 and a high performance PC. The USRP is a high performance software defined radio platform for designing and deploying next-generation wireless communications systems [15]. By attaching a daughterboard it can support up to 6 GHz transmission. In order to perform our implementation, the PCs processor speed should be at least 2GHz. The USRP is connected to PC with a 1Gbit Ethernet cable.

To avoid ethical problems, we use Amarisoft OTS 100 cell instead of commercial base station. It is a full LTE network software suite, includes eNodeB, EPC, eMBMS gateway and IMS server. It originally only support MIB, SIB1 and SIB2 broadcasting. We modified the configuration file and add SIB5 message in the cell. For UE, we use a Oneplus5 smartphone which is a subscriber registered in Amarisoft network with a commercial USIM card.



```
▾ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    NAS EPS Mobility Management Message Type: Authentication request (0x52)
    0000 .... = Spare half octet: 0
    .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
    .... .001 = NAS key set identifier:  (1) ASME
  ■ Authentication Parameter RAND - EPS challenge
  ▾ Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge
      Length: 16
    ■ AUTN value: ba6c7eb3052c9001648e80ba6d152365
```

Fig. 5. Testbed architecture: srsLTE can play as a rogue base station or a malicious UE, Our victim is a OnePlus5 cellphone and they are both in the same location area along with Amarisoft Cell.

A high-level testbed architecture is shown in Fig. 5. We run srsLTE application on our deployed hardware equipment. srsLTE project is a free and open sourced LTE software suite developed by SRS and it includes an open sourced implementation of the LTE baseband and various other applications aiming to implement a LTE UE, eNodeB or EPC. In particular, we run the srsUE application to simulate a LTE subscriber. On the network side, the srsLTE supports establish the MME and eNodeB on one host computer by running srsEPC and srsENB applications at the same time. The mobile traffic can be captured through wireshark network traffic analyzer.

### C. Adversary Setup

In order to sniff broadcast messages, we use modified srsUE application. srsLTE just supports UE side of the LTE but recently it releases its core network part as well. In our testbed, we use high performance PC since sniffing the air interface should be in real time since it needs to keep synchronized with eNodeB. Specifically, we use modified UE application to sniff and decode SIB messages broadcasted by eNodeBs.

There are two goals for our active adversary to accomplish. First, we need it to be a malicious UE. Comparing to build a fake base station this is more straightforward since all we need is the IMSI of a legitimate subscriber. Then we can implement this by running the srsLTE UE application and configuring its IMSI. For rogue base station, what we want is letting it impersonate a real network operator and forces the UE to attach to it. The process of building a rogue base station is described below.

When UE is turned on, it performs a cell selection procedure before initial attach. The details of selection criteria and algorithms are in [16], but the high level guideline is Absolute Priority, Radio Link Quality, and Cell Accessibility. The absolute priority mainly refers to high priority frequencies, which is mainly transmitted in SIB messages according to [16]. If we operate the rogue eNodeB at a higher priority frequency than the legitimate eNodeB, we can manage to force the UE to attach to our eNodeB. This is once mentioned by [8], however in their settings, they need to sniff 4 MIB messages to force cell reselection. In our experiments, we found that what we need is only SIB5 message. Except for the operating frequency, our eNodeB should have almost the same identities as a real network operator. To achieve this, we need to acquire necessary parameters, such as MCC and MNC numbers, spectrum bandwidth and etc. to configure our rogue eNodeB. This is done by the passive adversary through sniffing the MIB, SIB1 and SIB2 messages.

## IV. IMSI AND CELL IDENTITIES CATCHER ATTACK IN LTE NETWORK

In this section, we demonstrate our attacks and results using testbed which is mainly consisted of srsLTE and Amarisoft Cell. Before that, we briefly discussed the LTE vulnerabilities exploited by our attacks.

### A. Vulnerabilities In LTE Network

*1) Vulnerabilities in IMSI:* Not only in LTE network, but also in 2G/GSM and 3G/UMTS, the IMSI is a unique Identifier which globally identifies a Mobile subscriber. According to [7], the IMSI should be allocated to each mobile subscriber in the GSM/UMTS/EPS system. The IMSI of a subscriber is very essential and should not be obtained by a third party. And 3GPP also introduces several temporary identities such as GUTI and TMSI to reduce the chance of IMSI directly transmitted through the air interface. However, the IMSI is still used in initial attach procedures transmitted by identity response messages in plain text. We operate a rogue eNodeB to retrieve the IMSI of our subscriber.

*2) Vulnerabilities in broadcasting messages:* Whenever the UE tries to do the initial attach, it will need to establish connection with the network side. However, since the UE and network are not connected at the moment, it will need to tune its clock (System frame number in LTE network) to synchronize with the network. In order to achieve this function, eNodeB should broadcast several messages periodically to help UE to connect and synchronize with it. These messages are called MIB and SIB messages. Since these messages are designed to be received by any capable UE, it is not encrypted thus can be sniffed by anyone. Among these messages, we specifically look at three which are utilized by our attacks.

**MIB**

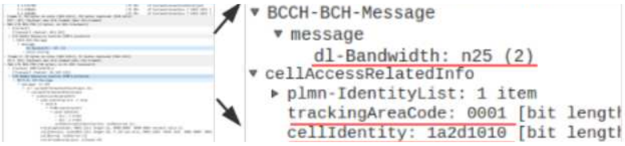
The Master Information Block messages is one of the most important messages. It carries the following information: downlink bandwidth, number of transmit antenna and system frame number. In most cases, it transmits every 40 ms and repeats every 10 ms.

**SIB1**

The SIB1 message contains information to assist the UE to access the cell, and it also defines the scheduling of other SIBs. For cell information, it contains public land mobile network (PLMN) identity , tracking Area Code (TAC), cell identity (PCI), cell selection information, which are the transmission and reception power of the cell. Generally, the SIB1 is broadcasted at every 80 ms and is repeated within 80 ms. The SIB5 message will be introduced in the later cell selection section.

Before looking into attacks details, here are some guides to help to understand our attacks in a high level. At the first stage, we operate our adversary as a passive one to sniff broadcasting messages from Amarisoft cell. After receiving those messages, we get our priority frequency and cell access related information. Then in the second stage, we operate our base station as an active adversary, a rogue base station configured using information retrieved form above messages. The victim UE will be forced to attach to our base station and send its IMSI.

### *B. Attack Implementation*



```
▼ BCCH-BCH-Message
  ▼ message
      dl-Bandwidth: n25 (2)
▼ cellAccessRelatedInfo
  ▶ plmn-IdentityList: 1 item
    trackingAreaCode: 0001 [bit lengtl
    cellIdentity: 1a2d1010 [bit lengtl
```

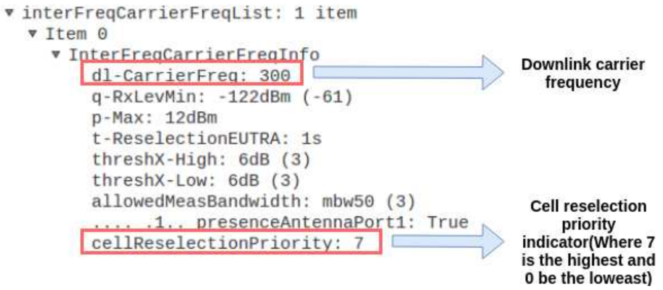
Fig. 6. MIB And SIB1 Message: In our testbed, downlink bandwidth is 5MHz, with the cell identity plmn 00101, TAC code 270b and PCI bbd92100.

*1) MIB and SIB message eavesdropping:* To build our eavesdropper, we use a modified version of srsUE application from srsLTE [17]. By default, the srsUE only decodes MIB, SIB1 and SIB2 messages which are already sufficient enough to locate the identities of the surrounding cells. However, since our cell selection attacks also require the SIB5 messages, which contains the 'inter-frequency cell list', we need the application to decode SIB5 messages. We also make changes to our commercial cell as it only transmits SIB1 and SIB2 messages at the first place. To achieve this, we put SIB type5 in $schedulingInfoList$ in SIB1 message, then we write our own SIB 5 message based on [12] and configure priority 7 for 300Mhz cell.

From Fig. 6, we can see that we already have the cell identities to configure our rogue cell. The PLMN which consists of MMN and MNC indicates which network operator the cell belongs to. The tracking area code is also important in our attacks. Although it makes no difference if we just want to force the UE attach to out base station, however, if we want the victim to begin attach procedure with our eNodeB, we need to keep this value the same as the legitimate eNodeB. This is because if we operate on a different tracking area code, before attach procedure, UE will keep trying to send the TAU request message to its original network instead of beginning to attach to our network. The last parameter is choosing the cell selection frequency which has the highest priority. As shown from Fig. 7, MIB messages have the downlink bandwidth which we need to set up our rogue base station. The n25 indicates a 5MHz bandwidth in LTE network.

Compared to MIB message, this SIB message contains more information that we need for building our rogue base station. The first is PLMN identity which we can think of it as the identity of network operator. In our testbed, it is 00101. Just behind the PLMN identity, there is another important parameter called $TrackingAreaCode$. In our experiment, we have to set up this code exactly the same as the commercial base station. For the same reason as TAC code, we do not change cell identities either. Since our network do not have the authentication material for the UE, the UE will keep continuing trying to attach to our base station and can not access to LTE service.

*2) Denial-of-Service Attack:* UE in LTE network should monitor the spectrum and sense surrounding cell's transmission power by listening the SIB messages and also receiving broadcasting messages. Since if the condition of current cell which UE is camping on becomes worse, it can perform this cell selection mechanism to find a more suitable cell using these continuously repeated messages. Altaf et.al [18] perform this by using a more powerful cell to force the UE connecting to it. However, we will need a cell which is far more powerful than the commercial base station by applying this methodology. And more importantly, power is not the only selection criteria and not even in the first priority class. According to [16], the first level criteria is absolute priority which is contained in SIB5 message. The SIB5 message is used for inter-cell selection. In this message, there is a parameter which is called $cellReselectionPriority$. The range for this parameter is from 0 to 7, which 7 indicates the highest and 0 indicates the lowest. If we use the frequency which have a higher priority, we can force the UE attach our cell even if the original cell works well. Some related work have mentioned about cell selection priority [8], but they required four SIB messages instead of one used in our experiment.



```
▼ interFreqCarrierFreqList: 1 item
  ▼ Item 0
    ▼ InterFreqCarrierFreqInfo
        dl-CarrierFreq: 300
        q-RxLevMin: -122dBm (-61)
        p-Max: 12dBm
        t-ReselectionEUTRA: 1s
        threshX-High: 6dB (3)
        threshX-Low: 6dB (3)
        allowedMeasBandwidth: mbw50 (3)
        .... .1.. presenceAntennaPort1: True
        cellReselectionPriority: 7
```

Downlink carrier frequency
Cell reselection priority indicator(Where 7 is the highest and 0 be the loweast)

Fig. 7. SIB5 Message.

Fig. 7 is our captured SIB5 message. As shown from the figure, two messages are critical for our attacks. The 300 MHz downlink frequency is inter-cell selection frequency. The lower message is cell Selection Priority which is 7 in our experiment. We choose to operate our rogue base station at 300MHz which has a 7 priority number. According to cell selection criteria mentioned in Sec. IV-B, UE will choose our base station to camp on.

Once UE tries to attach to our base station, it will send the attach request message. Since our base station do not have the temporary identifier to response, it will send an identity request message and UE will reply with identity response message with its IMSI. The process is shown in Fig. 8. And the Identity Response message is shown in Fig. 9. As long as we do not shut down our rogue base station, the UE will try to connect to it and lose LTE network service.

*3) Countermeasures:* The attacks performed in this paper can cause denial of service and disclose the IMSI, which

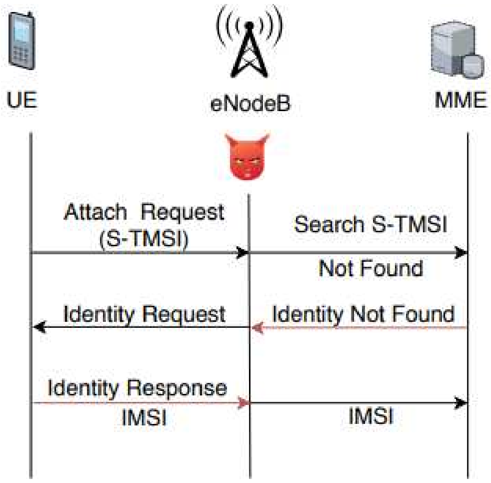
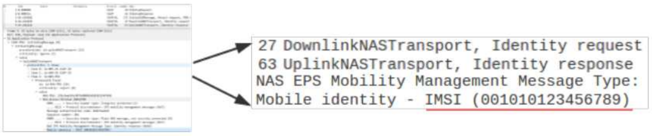


Fig. 8. IMSI Catcher: When IMSI is not found on network side, an identity request message will be sent to UE side and UE will reply with identity response with IMSI in plaintext.



```
27 DownlinkNASTransport, Identity request
63 UplinkNASTransport, Identity response
NAS EPS Mobility Management Message Type:
Mobile identity - IMSI (001010123456789)
```

Fig. 9. IMSI contained in identity response message.

are real threats to the subscriber's privacy. Here we propose two solutions that each of which corresponds to one attack respectively.

First, the UE should identify if the SIB5 message is sent from a legitimate subscriber. Several previous TMSI/GUTI should be stored on both UE and network side, and instead of sending identity response message immediately, the UE should ask the network to send itself one of those identifiers (TMSI/GUTI), which will be used to match the record stored on UE side. If there is no such identity in the database of UE, then it should discard the connection and stop using the SIB messages sent from that cell.

The IMSI can also be encrypted before sending to the network in identity response message. Actually, 3GPP has already noticed this issue and implements in the 5G network by enabling asymmetric encryption on IMSI during initialization. Since LTE has the same structure as the 5G at this step, the same methodology can also be considered to protect IMSI leakage from our attackers or other eavesdroppers.

## V. CONCLUSION

In this paper, we carefully reveal several vulnerabilities that can cause denial of service and disclose subscriber's IMSI in LTE network. We implemented our attacks based on these vulnerabilities with a laptop and USRP, which costs less than 1500 dollars in our LTE network testbed. With the support of these hardware and srsLTE applications, we believe that our attacks are highly effective and feasible. These attacks can affect both subscriber's service quality and network operator's revenue.

## REFERENCES

[1] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 20162021 white paper. Online, 2018.

[2] WIKI. List of countries by 4g lte penetration. Online, 2018.

[3] GSA Global mobile Suppliers Association. Global number of lte subscribers grows by almost a billion in the last year. Online, 2018.

[4] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Ryan. Privacy through pseudonymity in mobile telephony systems. In *NDSS*, 2014.

[5] Nico Golde, Kevin Redon, and Jean-Pierre Seifert. Let me answer that for you: Exploiting broadcast information in cellular networks. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 33–48, Washington, D.C., 2013. USENIX.

[6] David Perez and Jose Pico. A practical attack against gprs/edge/umts/hspa mobile data communications. *Black Hat DC*, 2011.

[7] 3GPP. Numbering, addressing and identification. Technical Specification (TS) 23.003, 3rd Generation Partnership Project (3GPP), 2015. Version 12.5.0.

[8] Altaf Shaik, Jean-Pierre Seifert, Ravishankar Borgaonkar, N. Asokan, and Valtteri Niemi. Practical attacks against privacy and availability in 4g/lte mobile communication systems. In *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*, 2016.

[9] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. Guti reallocation demystified: Cellular location tracking with changing temporary identifier. In *Symposium on Network and Distributed System Security (NDSS). ISOC*, 2018.

[10] 3GPP. Characteristics of the Universal Subscriber Identity Module (USIM application). Technical Specification (TS) 31.102, 3rd Generation Partnership Project (3GPP), 2017. Version 12.5.0.

[11] 3GPP. Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol). Technical Specification (TS) 29.272, 3rd Generation Partnership Project (3GPP), 2018. Version 15.5.0.

[12] 3GPP. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification. Technical Specification (TS) 36.331, 3rd Generation Partnership Project (3GPP), 2017. Version 13.4.0.

[13] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H Reed. Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, 54(4):54–61, 2016.

[14] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Doug J. Leith. srslte: An open-source platform for lte evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, WiNTECH '16, pages 25–32, New York, NY, USA, 2016. ACM.

[15] Ettus Research. Usrp x310 (kintex7-410t fpga, 2 channels, 10 gige and pcie bus), 2018. [Online; accessed 17-December-2018].

[16] 3GPP. User Equipment (UE) procedures in idle mode. Technical Specification (TS) 36.304, 3rd Generation Partnership Project (3GPP), 2012. Version 9.9.0.

[17] Domonkos P. Tomcsanyi. Open source software radio 3gpp lte ue, 2016. [Online; accessed 17-December-2018].

[18] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. On the impact of rogue base stations in 4g/lte self organizing networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '18, pages 75–86, New York, NY, USA, 2018. ACM.