Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

Altaf Shaik*, Ravishankar Borgaonkar†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Seifert*
*Technische Universität Berlin and Telekom Innovation Laboratories
Email: (altaf329, jpseifert) @sec.t-labs.tu-berlin.de
†Aalto University
Email: ravishankar.borgaonkar@aalto.fi
‡Aalto University and University of Helsinki
Email: asokan@acm.org
§University of Helsinki
Email: valtteri.niemi@helsinki.fi

***Abstract*—Mobile communication systems are now an essential part of life throughout the world. Fourth generation "Long Term Evolution" (LTE) mobile communication networks are being deployed. The LTE suite of specifications is considered to be significantly better than its predecessors not only in terms of functionality but also with respect to security and privacy for subscribers. We carefully analyzed LTE access network protocol specifications and uncovered several vulnerabilities. Using commercial LTE mobile devices in real LTE networks, we demonstrate inexpensive, and practical attacks exploiting these vulnerabilities. Our first class of attacks consists of three different ways of making an LTE device leak its location: In our experiments, a semi-passive attacker can locate an LTE device within a 2 km^2 area in a city whereas an active attacker can precisely locate an LTE device using GPS co-ordinates or trilateration via cell-tower signal strength information. Our second class of attacks can persistently deny some or all services to a target LTE device. To the best of our knowledge, our work constitutes the *first publicly reported practical* attacks against LTE access network protocols.**

We present several countermeasures to resist our specific attacks. We also discuss possible trade-off considerations that may explain why these vulnerabilities exist. We argue that justification for these trade-offs may no longer valid. We recommend that safety margins introduced into future specifications to address such trade-offs should incorporate greater agility to accommodate subsequent changes in the trade-off equilibrium.

I. Introduction

During the past two decades, mobile devices such as smartphones have become ubiquitous. The reach of mobile communication systems, starting from the second generation Global System for Mobile Communications (2G/GSM) and the third generation Universal Mobile Telecommunication Systems (3G/UMTS), has extended to every corner in the world. Mobile communication is an important cornerstone in the lives of the vast majority of people and societies on this planet. The latest generation in this evolution, the fourth generation "Long Term Evolution" (4G/LTE) systems are being deployed widely. By the end of 2015 the worldwide LTE subscriber base is expected to be around 1.37 billion [1].

Early 2G systems were known to have several vulnerabilities. For example, lack of mutual authentication between mobile users and the network implied that it was possible for an attacker to set up fake base stations and convince legitimate mobile devices to connect to it. In order to minimize exposure of user identifiers (known as International Mobile Subscriber Identifier or IMSI) in over-the-air signaling messages, 2G systems introduced the use of temporary mobile subscriber identifiers. However, in the absence of mutual authentication, fake base stations were used as "IMSI catchers" to harvest IMSIs and to track movements of users.

The evolution of these mobile communication systems specified by 3GPP (Third Generation Partnership Project) have not only incorporated improvements in functionality but also strengthened security. 3G specifications introduced mutual authentication and the use of stronger and well-analyzed cryptographic algorithms. LTE specifications further strengthened signaling protocols by requiring authentication and encryption (referred to as "ciphering" in 3GPP terminology) in more situations than was previously required. Consequently, there is a general belief that LTE specifications provide strong privacy and availability guarantees to mobile users. Previously known attacks, such as the ability to track user movement were thought to be difficult in LTE.

In this paper, we demonstrate the *first practical* attacks against LTE access network protocols. Our attacks are based on vulnerabilities we discovered during a careful analysis of LTE access network protocol specifications. They fall into two classes: location leaks and denial of service. In the first class, we describe three different attacks that can force an LTE device (User Equipment or UE in 3GPP terminology) into revealing its location. The first two allow a passive or semi-passive attacker to localize the target user within about a 2 km^2 area in an urban setting which is a much finer granularity than previously reported location leak attacks [2] against 2G

NDSS '16, 21-24 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2016.23236

devices, while still using similar techniques. Notably, we show how popular social network messaging applications (e.g., Facebook messenger [3] and WhatsApp [4]) can be used in such attacks. Our third attack allows an active attacker exploiting vulnerabilities in the specification and implementation of LTE Radio Resource Control (RRC) protocol [5] to accurately pinpoint the target user via GPS co-ordinates or trilateration using base station signal strengths as observed by that UE. *We believe that all LTE devices in the market are vulnerable to this attack.*

In the second class, we describe three further attacks where an active attacker can cause persistent denial of service against a target UE. In the first, the target UE will be forced into using 2G or 3G networks rather than LTE networks, which can then make it possible to mount 2G/3G-specific attacks against that UE. In the second, the target UE will be denied access to all networks. In the last attack, the attacker can selectively limit a UE only to some types of services (e.g., no voice calls). The attacks are persistent and silent: *devices require explicit user action (such as rebooting the device) to recover.*

We have implemented all our attacks (except one) and confirmed their effectiveness using commercial LTE devices from several vendors and real LTE networks of several carriers. The equipment needed for the attacks is inexpensive and readily available. We reported our attacks to the manufacturers and carriers concerned as well as to the standardization body (3GPP). Remedial actions are under way while writing.

Specification of a large system like LTE is a complex endeavor involving many trade-offs among conflicting requirements. Rather than merely report on LTE vulnerabilities and attacks, we also discuss possible considerations that may have led to the vulnerabilities in the first place. Based on this we suggest some general guidelines for future standardization as well as specific fixes for our attacks.

- Fine-grained location leaks: New passive and active techniques to link users' real identities to LTE temporary identities assigned to them and to **track user locations and movements to much higher levels of granularity** than was previously thought possible. (Section V)
- Denial-of-Service (DoS) Attacks: New active **DoS attacks that can silently and persistently downgrade LTE devices** by preventing their access to LTE networks (limiting them to less secure 2G/3G networks or denying network access altogether) or limiting them to a subset of LTE services. (Section VI)
- Implementation & Evaluation: **Inexpensive software and hardware framework** to implement the attacks based on `srsLTE`, `OpenLTE`, and Universal Software Radio Peripherals (USRP) (Section IV), and evaluation of the attacks using commercially available LTE phones in real networks. (Sections V–VII)
- Security Analysis: Discussion outlining **possible underlying reasons for the vulnerabilities**, including perceived or actual trade-offs between security/privacy and other criteria like availability, performance and functionality, as well as recommending fixes. (Section VIII).

II. Overview of LTE Architecture

We briefly describe LTE infrastructure as well as security and paging mechanisms to assist readers in understanding the vulnerabilities and attacks we present in this paper.

A. LTE infrastructure

We consider a simplified LTE architecture involving components required to set up access network protocols between a base station and mobile devices. We hide other details of the architecture which are not relevant from the point of view of understanding our attacks. Figure 1 depicts this simplified architecture which contains three main components: User Equipment (UE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and Evolved Packet Core (EPC). All three components are collectively referred to as Evolved Packet System (EPS) according to 3GPP terminology. In the interest of simplicity, throughout this paper we refer to the whole system as LTE. The three components are described below (A list of common acronyms related to LTE appear in the full version of this paper [6]).

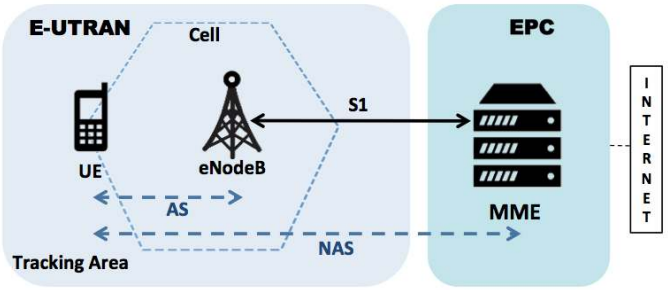

Fig. 1. LTE system architecture

User Equipment: UE refers to the actual communication device which can be, for example, a smartphone . A UE contains a USIM (Universal Subscriber Identity Module)[7], which represents the IMSI and stores the corresponding authentication credentials [8]. This IMSI is used to identify an LTE user (generally referred to as "subscriber" in 3GPP terminology) uniquely. The USIM participates in LTE subscriber authentication protocol and generates cryptographic keys that form the basis for the key hierarchy subsequently used to protect signaling and user data communication between the UE and base stations over the radio interface.

E-UTRAN: E-UTRAN consists of base stations. It manages the radio communication with the UE and facilitates communication between the UE and EPC. In LTE, a base station is technically referred as "evolved NodeB (eNodeB)". The eNodeB uses a set of access network protocols, called Access Stratum (AS) for exchanging signaling messages with its UEs. These AS messages include Radio Resource control (RRC) protocol messages. Other functions of eNodeB include paging UEs, over-the-air security, physical layer data connectivity, and handovers. Each eNodeB is connected to the EPC through an interface named S1.

MME in EPC: EPC provides core network functionalities by a new all-IP mobile core network designed for LTE systems. It consists of several new elements as defined in [9]. However, for

our work we need to describe only the Mobility Management Entity (MME) in detail. MME is responsible for authenticating and allocating resources (data connectivity) to UEs when they connect to the network. Other important functions of MME involve security (setting up integrity and encryption for signaling) [10] and tracking UE's location at a macro level. The set of protocols run between UE and MME are referred as Non-Access Stratum (NAS).

Now, we explain how the system components presented above can be deployed in a geographical region (e.g., in a city) by mobile network carriers (more commonly referred to as "operators" in 3GPP terminology) to provide LTE services. A service area of a mobile operator is geographically divided into several regions known as Tracking Areas (TAs). TAs are similar to Location Areas in GSM networks and are managed by the MME. Further, a TA contains a group of "cells"[1] each of which is controlled by an eNodeB. The eNodeB broadcasts operator-specific information such as Tracking Area Code (TAC), Mobile Country Code (MCC), Mobile Network Code (MNC), and cell ID via System Information Block (SIB) messages [5]. This allows UEs to identify their serving network operator, and initiate a connection to the network. A UE attaches to the network by initiating the $Attach$ procedure [11]. Upon successful acceptance the UE receives access to services based on its subscription. The UE uses the $TrackingAreaUpdate(TAU)$ procedure to inform the network about its mobility in the serving area [11].

B. Security in LTE

As IMSI is a permanent identifier of a subscriber, LTE specifications try to minimize its transmission in over-the-air radio communication for security and privacy reasons. Instead, a Globally Unique Temporary Identifier (GUTI) [8] is used to identify subscribers during radio communication. It is assigned to UEs during $Attach$ and may be periodically changed to provide temporal unlinkability of traffic to/from the same UE. An Authentication and Key Agreement (AKA) protocol is used for mutual authentication between UE and the network and to agree on session keys that provide integrity and confidentiality protection for subsequent NAS and AS messages [10]. Both NAS and AS security are collectively referred as EPS security. It is established between a UE and a serving network domain (eNodeB and MME) during EMM (EPS Mobility Management) procedures [11] and includes agreeing on session keys, preferred cryptographic algorithms, and other values as defined in [10].

C. Paging in LTE

Paging refers to the process used when MME needs to locate a UE in a particular area and deliver a network service, such as incoming calls. Since MME may not know the exact eNodeB to which UE is connected, it generates a paging message and forwards to all eNodeBs in a TA. Simultaneously, MME starts a paging timer (T3413) and expects a response from UE before this timer expires. Thus, all eNodeBs present in the paged TA broadcast a RRC paging message to locate

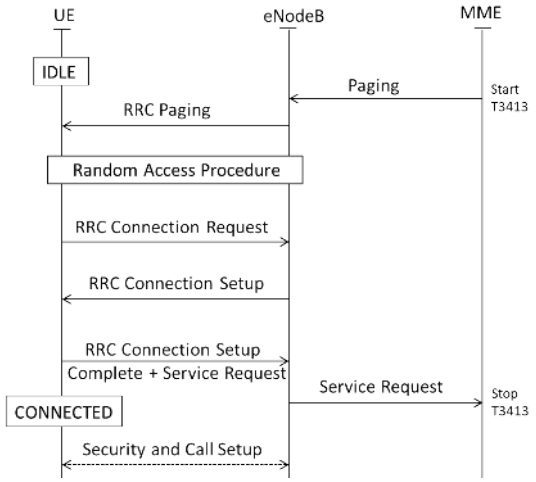

Fig. 2. Paging in LTE

the UE. Paging messages contain identities of UEs such as S-TMSI(s) or IMSI(s). S-TMSI is a temporary identifier (SAE-Temporary Mobile Subscriber Identity). It is part of a GUTI. For the sake of simplicity, we consistently use the term GUTI throughout the rest of this paper even when referring to S-TMSI. Figure 2 highlights LTE paging procedure, described in detail in the relevant LTE specifications [11], [12], [13].

The UE in IDLE state[2] decodes RRC paging messages. If it detects its IMSI then it initiates a new $Attach$ procedure to receive a GUTI as defined in [11]. If UE detects its GUTI, it acquires a radio channel through the *"Random Access Procedure"* [13] for requesting a RRC connection from the eNodeB. *"RRC Connection Setup"* involves the configuration of radio resources for exchanging signaling messages. Upon receiving this setup message, the UE completes a three way RRC handshake procedure by sending a *"RRC Connection Setup Complete"* message along with a *"Service Request"* message. At this point UE leaves IDLE state and enters into CONNECTED state[3]. The eNodeB forwards the service request message to MME, which in turn stops the paging timer. Further, eNodeB establishes a security context and proceeds to deliver network services to UE.

In LTE, the paging procedure is improved to reduce signaling load and locate the UE faster using a technique called Smart Paging [14], [15], [16]. It is compliant with LTE specifications and consists of directing paging messages selectively via the eNodeB (cell) where the UE was last seen. If no response is received, paging is repeated in the entire TA. In our experiments (Section V-B) to study LTE paging procedures in a major city, we observed that several network operators and vendors have implemented smart paging.

III. Adversary Model

In this section, we describe the adversary model for our attacks. The primary goals of the adversary against LTE subscribers are: a) learn the precise location of a subscriber in a given geographical area b) deny network services (both

[1]In LTE, coverage area of an eNodeB is divided into several sectors known as cells.

[2]In IDLE state, the UE has no active connections with any eNodeB.

[3]CONNECTED means the UE has an active connection with an eNodeB.

mobile-terminated and mobile-originated) to a subscriber, and c) force subscribers to use less secure GSM or 3G networks thereby exposing them to various attacks such as IMSI catchers [17]. We assume that the adversary is in the same geographical area as the victim. The adversary model is divided into three attack modes as described below.

Passive

A passive adversary is able to silently sniff LTE over-the-air (radio) broadcast channels. To achieve this, he/she has access to a hardware device (for example Universal Software Radio Peripheral (USRP)) and associated software needed to observe and decode radio broadcast signaling messages.

Semi-Passive

A semi-passive adversary is, in addition to passive monitoring, able to trigger signaling messages to subscribers using interfaces and actions that are *legitimately available* in LTE or in higher layer systems. For example, a semi-passive adversary can trigger paging messages to subscribers by sending a message via a social network or initiating a call. The adversary is assumed to be aware of social identities of subscribers. For example, these identities can be a Facebook profile or a mobile phone number of the subscriber. A semi-passive adversary is analogous to the 'honest-but-curious' or 'semi-honest' adversary model used for cryptographic protocols [18].

Active

The active adversary can set up and operate a rogue eNodeB to establish malicious communication with UEs. Capabilities required for active attacks include knowledge of LTE specifications and hardware (USRP) that can be used for impersonating subscriber's serving operator network, and injecting malicious packets to UEs. An active adversary is analogous to the 'malicious' adversary model in cryptographic protocols [18].

IV. Experimental Setup

Software and hardware used in major telecommunication systems have traditionally been proprietary (closed source) and expensive. However recently open source telephony software and low-cost hardware modules have started to emerge. In this section, we explain our experimental setup built using low cost off-the-shelf components and requiring only elementary programming skills with knowledge of LTE specifications. Figure 3 depicts the experimental setup.

Hardware

Hardware components for eNodeB, MME, and UE are needed to build our experimental LTE network. On the network side, we used a USRP B210 device [19] connected to a host laptop (Intel i7 processor & Ubuntu 14.04 OS), acting as an eNodeB. USRP is a software-defined radio peripheral that can be connected to a host computer, to be used by host-based software to transmit/receive data over the air. Even though we utilized USRP B210 which costs around one thousand euros, passive attacks can also be realized practically with more cheaply available radio hardware. For example, RTL-SDR [20] dongles which cost around 15 euros can be leveraged to passively listen over the LTE air-interface. On the UE side, we selected popular LTE-capable mobile phones available in the market. These devices incorporate LTE implementations from four major LTE baseband vendors who collectively account for the vast majority of deployed LTE-capable UEs.

Fig. 3. Experimental setup

A. Passive and semi-passive attack setup

The research test-bed used in performing paging attacks described in [2] was restricted to GSM networks due to the unavailability of any LTE baseband implementations at that time. Today, there are some partial LTE baseband implementations available as open source including `OpenLTE` [21] and `srsLTE` [22], which enabled us to conduct real-time experiments on LTE networks.

Implementation

In order to sniff LTE broadcast channels, we utilized parts of `srsLTE`. It is a free library for software-defined radio mobile terminals and base stations. Currently, the project is developing a UE-side LTE baseband implementation. `srsLTE` uses Universal Hardware Device library to communicate with the USRP B210. Since all the passive sniffing is done in real-time, it is recommended to have a high-speed host (laptop) in order to handle the high (30.72 MHz) sampling rates without data loss and also to maintain constant sync with eNodeBs. In particular, we used the `pdsch-ue` application to scan a specified frequency and detect surrounding eNodeBs. It can listen and decode SIB messages broadcast by eNodeB. Further, we modified `pdsch-ue` to decode paging messages which are identified over-the-air with a Paging-Radio Network Temporary Identifier (P-RNTI). Upon its detection, GUTI(s) and/or IMSI(s) can be extracted out of paging messages.

In semi-passive attack mode, we use Facebook [23], [3] and WhatsApp [4] applications over the Internet, in addition to initiating communication with targets via silent text messages or phone calls.

B. Active attack setup

We built an eNodeB to mount successful active attacks against UEs registered with a real LTE network. In particular,

our eNodeB impersonates a real network operator and forces UEs to attach to it. The process of building such rogue eNodeBs is described below.

Building rogue eNodeB: Generally, UE always scans for eNodeBs around it and prefers to attach to the eNodeB with the best signal power. Hence in IMSI catcher type of attacks [17], rogue eNodeBs are operated with higher power than surrounding eNodeBs. However, in LTE the functionality of the UE may be different in some situations. In particular, when a UE is very close to a serving eNodeB it does not scan surrounding eNodeBs. This allows UEs to save power. Hence to overcome this situation in our active attacks, we exploit another feature named *'absolute priority based cell reselection'*, and introduced in the LTE release 8 specification [24].

The principle of priority-based reselection is that UEs, in the IDLE state, should periodically monitor and try to connect to eNodeBs operated with high priority frequencies [24]. Hence even if the UE is close to a real eNodeB, operating the rogue eNodeB on a frequency that has the highest reselection priority would force UEs to attach to it. These priorities are defined in SIB Type number 4, 5, 6, and 7 messages broadcast by the real eNodeB [5]. Using passive attack setup, we sniff these priorities and configure our eNodeB accordingly.

Further, the rogue eNodeB broadcasts MCC and MNC numbers identical to the network operator of targeted subscribers to impersonate the real network operator. Generally, when UE detects a new TA it initiates a *"TAU Request"* to the eNodeB. In order to trigger such request messages, the rogue eNodeB operates on a TAC that is different from the real eNodeB.

Implementation

The active attack is launched using the USRP B210 and a host laptop which together are running `OpenLTE`. The `OpenLTE` is an open source implementation of LTE specifications and includes an `LTE_Fdd_enodeb` application. Although this application cannot be compared to a full-fledged commercial eNodeB, it has the capability to execute a complete LTE *Attach* procedure. In addition, some functionality of the MME is implemented in `LTE_Fdd_enodeb`. Upon successful completion of *Attach*, `LTE_Fdd_enodeb` can also handle UE-originated services. However, currently it lacks stability. We tested active attacks on UEs with USIMs from three major national-level operators.

Further, we programmed `LTE_Fdd_enodeb` to include LTE RRC and NAS protocol messages to demonstrate active attacks. In addition, we modified the telephony protocol dissector [25] available in Wireshark [26] to decode all messages exchanged between the rogue eNodeB and UE. These modifications are submitted to the Wireshark project and are being merged into the mainstream application.

C. Ethical considerations

Our work reveals vulnerabilities in LTE specifications which are already in use in every LTE-enabled UE worldwide. Further we also encountered several implementation issues in popular smartphones and LTE network configuration issues. Therefore we made an effort to responsibly disclose our work to the relevant standard bodies and affected parties. Our reports were acknowledged by all vendors and network operators we contacted. For those vendors who have a standard responsible disclosure process in place, we followed the process.

We carried out most of the active attacks in a Faraday cage [27] to avoid affecting other UEs. For attacks in real LTE networks, we took care not to interrupt normal service to other UEs in the testing zone. Initially, we determined GUTIs of our test UEs via passive attacks and fed them into our rogue eNodeB. We programmed our rogue eNodeB to accept *"TAU / Attach / Service Requests"* only from these specified GUTIs and to reject all requests from unknown UEs with the EMM reject cause number 12 *"Tracking area not allowed"* [11]. Upon receipt of this message, all UEs other than our test UEs disconnect automatically from our rogue eNodeB.

V. Location Leak Attacks Over Air Interface

In this section, we show how the approximate location of an LTE subscriber inside an urban area can be inferred by applying a set of novel passive, semi-passive, and active attacks. In particular, we track down the location of a subscriber to a cell level (e.g., 2 km^2 area) using passive attacks (L1[4]) and further determine the precise position using active attacks (L3). We first describe the background for the attacks by summarizing the features and aspects of LTE that are used by the attacker. We then characterize preliminary measurements used for realizing the attacks and new techniques for triggering subscriber paging. Finally, we explain the attacks in detail.

A. Attack background

We now describe network configuration issues, subscriber identity mapping technique, and observations about certain LTE network access protocols. We will later make use of all of these aspects in developing our attacks.

Network configuration issues

In LTE, network operators deploy various methods to minimize signaling overhead introduced due to evolution of networks, devices, and smartphone applications [28]. We identify two such deployment techniques relevant to our discussion.

Smart Paging: In GSM, paging messages are sent to an entire location area. Thus it only allows the attacker to locate a subscriber within a large (e.g., 100 km^2) area [2]. However, LTE paging is directed onto a small cell rather than to a large TA. Such Smart Paging allows an attacker to locate an LTE subscriber within a much smaller (e.g., 2 km^2) area which is a typical LTE cell size as observed in our experiments in a major city.

GUTI persistence: Generally a fresh GUTI is allocated in the following situations: (a) when MME is changed due to handover or load balancing, b) during TAU or *Attach* procedure, and c) when network issues NAS *"GUTI reallocation command"*. However, network operators tend to not always change GUTI during the above procedures [29][5]. This allows a passive attacker to track UEs based on their GUTIs.

[4]For the sake of simplicity, we refer location leaks attacks as L1, L2, and L3 whereas DoS attacks as D1, D2, and D3 respectively.

[5]The reason for not changing GUTIs often is to avoid signaling storms in LTE network as described in [29].

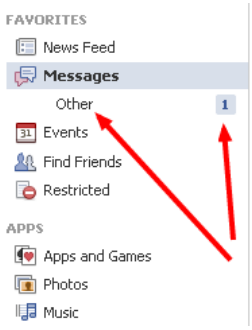

Fig. 4. 'Other' folder in Facebook

Social identity to subscriber mapping

In previous work, phone calls (originating from a landline phone) [2] and silent Short Message Service (SMS) [30] techniques were used to page GSM subscribers thereby mapping TMSIs to their phone numbers. However these methods are not as effective anymore due to the availability of tools to detect such attacks [31], [32]. We now discuss some features in social network messaging applications that can be used to trigger LTE paging requests to devices in which the subscriber has installed the corresponding social network applications.

Facebook 'Other' message folder: Many Facebook [23] users do not know about the *'Other'* message folder (as shown in Figure 4) in Facebook. Normally when a message is received from a Facebook friend, it will be stored in the normal inbox folder of that user. But messages from people who are not in the friend list may be directed to the *'Other'* folder. Further, the user is *not notified* about messages in the *'Other'* folder. In fact, the user himself has to manually check *'Other'* folder to even notice that there are waiting messages. According to Facebook [33], this is intended to protect users against spam. When an LTE subscriber has the Facebook application installed on his LTE device, *all* incoming Facebook messages, including those that end up in the 'Other' folder, trigger a paging request by the network. Other Facebook features, such as repeated friend requests or poking (depending on the user's profile settings) also trigger paging requests. However, in those cases, unlike in the case of messages that end up in the 'Other' folder, Facebook application notifies the user.

WhatsApp 'typing notification': WhatsApp supports a 'typing notification' feature - when someone ('sender') starts composing a message to a person ('recipient') using WhatsApp, the WhatsApp client UI at the recipient shows a notification to the recipient that an incoming message is being typed. If the recipient is using a WhatsApp client on an LTE device, this ends up triggering a paging request.

RRC protocol issues

The LTE RRC protocol includes various functions needed to set up and manage over-the-air connectivity between the eNodeB and the UE as described in [5]. For our attacks, we exploit two of these: network broadcast information and measurement reports sent by UEs to the network.

Broadcast information: In this RRC protocol function, temporary identities associated with UEs (i.e., GUTIs) are transmitted over the air in a broadcast channel. Such broadcast messages are neither authenticated nor encrypted. Hence anyone can decode them with appropriate equipment. Since these broadcast messages are only sent in specific geographical areas, we can use the method described in [2] to reveal the presence of subscribers in a targeted area by exploiting these broadcast messages.

Further, the eNodeB periodically broadcasts SIB messages which carry information for UEs to access the network, perform cell selection, and other information as described in [5]. The attacker can utilize this broadcast information to configure the rogue eNodeB for malicious purposes.

UE measurement reports: In LTE, UE performs network measurements and sends them to the eNodeB in RRC protocol messages when requested. Such UE measurement reports are necessary for network operators to troubleshoot signal coverage issues. In particular, there are two types of UE measurement reports - one sent in *"Measurement Report"* used as part of handover procedure and other one in Radio Link Failure (RLF) report - which are used to troubleshoot signaling coverage. However, since these messages are not protected during the RRC protocol communication, an attacker can obtain these network measurements by simply decoding from radio signals.

We now explain the importance of two RRC protocol messages and measurement information they carry. First, *"Measurement Report"* message is a necessary element during handover procedure in LTE networks. Generally, eNodeB sends a RRC message indicating what kind of information is to be measured in response the UE sends *"Measurement Report"* messages. We discovered that the LTE specification allows sending this message to the UE without AS security context [5]. Second, RLF report is a feature to detect connection failures caused by intra-LTE mobility and inter-system handovers between LTE, GSM, and 3G networks. Upon detection of such events, RLF reports are created by the UE and forwarded to eNodeB when requested. These reports are collected by the Operations, Administration, and Maintenance (OAM) system for troubleshooting. As per the LTE standard specification [5] appendix A.6, the *"UEInformationResponse"* message carrying RLF report should not be sent by the UE before the activation of AS security context. However, we discovered that major LTE baseband vendors failed to implement security protection for messages carrying RLF reports. This suggests that the specification is ambiguous leading to incorrect interpretation by multiple baseband vendors.

In particular, *"Measurement Report"* and *"UEInformationResponse"* messages contain serving and neighboring LTE cell identifiers with their corresponding power measurements and also similar information of GSM and 3G cells. Additionally the message can include the GPS location of the UE (and hence of the subscriber) if this feature is supported. We exploit the above vulnerabilities to obtain power measurements, which we then use to calculate a subscriber's precise location.

B. Initial measurements

We performed a measurement study on LTE networks of three major operators to understand GUTI allocations, Smart Paging, and mapping of tracking area and cell dimensions for

the purpose of examining the feasibility aspects of location leak attacks.

Before measuring GUTI allocations and Smart Paging, we consider the following timing constraints for the paging procedure in LTE. Paging messages are sent only if a UE is in IDLE state. During an active connection, there are no paging messages. According to [13], if the UE remains silent for 10 seconds during a connection, the eNodeB releases the associated radio resources and the UE moves into IDLE state.

GUTI variation: GUTI reallocation depends entirely on operator configuration. We investigated GUTI allocation and reallocation methods used by several operators. Specifically, these experiments verify whether GUTIs are really temporary in practice. We used a Samsung B3740 LTE USB data stick as the UE, since it allows us to view the RRC and NAS messages in Wireshark [34]. The changes in GUTI can be seen in the *"Attach Accept"* or *"TAU Accept"* NAS messages in the Wireshark traces. We identified these NAS messages and recorded GUTIs for every operator for further analysis. In addition, GUTI variation can be verified with engineering mode on few selected handsets, for example LG G3 [35]. Our results in Table I show that GUTI allocation and reallocation mechanisms are similar among all operators. The results are summarized below:

- Periodically (once an hour and once in 12 hours) detaching and attaching the UE while it was stationary resulted in the same GUTI being re-allocated in all three operator networks. A stationary UE did not have its GUTI changed for up to three days or when moving between TAs within the city.
- When UE was moving inside the city for 3 days while remaining attached to the network, no change in GUTI was observed in any operator's network.
- If a UE was completely turned off for one day, a new GUTI was allocated when it was subsequently turned on. In the case of one of the operators, the newly assigned GUTI differed from the old one by only one hexadecimal digit. This implies that GUTIs were not chosen randomly.

Based on above observations we conclude that the GUTI tends to remain the same even if a UE is moving within a city for up to three days. Hence temporary identities are not really temporary in any of the three networks. This allows an attacker to perform passive attacks.

Activity	*Smart Paging*		*GUTI changed?*
	on Cell	*on TA*	*(All operators)*
Facebook Message	*Yes*	*No*	*No*
SMS	*Yes*	*No*	*No*
VoLTE call	*No*	*Yes*	*No*
Attach and Detach every 1 hour	-	-	*No*
Attach and Detach every 12 hour	-	-	*No*
Normal TAU procedure	-	-	*No*
Periodic TAU procedure	-	-	*No*

TABLE I: GUTI variations and Smart Paging behavior

Smart Paging: We identified multiple cells in a busy TA for each operator and placed our passive LTE air-interface sniffer within each cell. The test UE was placed in one of the cells and remained stationary for the experiment duration. Table I presents the set of activities performed to trigger paging messages. The results are summarized as follows:

- Paging for Voice Over LTE (VoLTE[6]) call occurs on the entire TA and paging for other IP applications occurs on the last seen cell. This is referred to as application aware paging [16]. Since VoLTE has higher priority and strict timing constraints compared to other data applications, the network pages the complete TA to find the UE quickly.
- When the UE paging is triggered via Facebook or SMS messages, sniffers detected a particular paging message only in the cell where the UE is located (or last seen). This implies that all operators are using Smart Paging.

Mapping tracking area and cell dimensions: It is necessary to have knowledge of the size of LTE tracking areas and cells deployed in a metropolitan city for determining a victim's location. In particular, this knowledge enables an attacker to identify targeted TAs for specific regions and network operators in the city. We created a database that maps Tracking Area Codes (TACs) to GPS coordinates by slowly bicycling through the city. The TACs are periodically broadcast in SIB Type number 1 messages [5]. We logged them using our passive attack setup. Further, in order to determine the surface area covered by a tracking area, we calculated the region covered by the points with the same TAC and the results are plotted in Figure 5. The size of TA inside the city varies from 10 to 30 km^2. According to OpenCellID [36] tracking areas outside the city center cover 80 - 100 km^2. The TAs are smaller in size compared to the GSM location areas plotted by [37] in the same city.

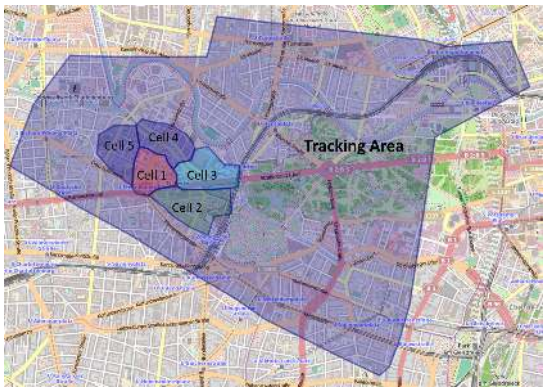

Fig. 5. LTE tracking area and cells of a major operator in a city

Since the granularity we obtain through our attacks is on a cell level, it is important to know cell sizes in LTE network as compared to GSM. Further, this knowledge helps in positioning the rogue eNodeB to maximize the effect of active attacks. In order to plot cell boundaries, we used the

[6]VoLTE stands for voice over LTE and it is for voice calls over an LTE network, rather than the 2G or 3G connections which are usually used.

`cellmapper` [38] Android application which reports the cell ID, eNodeB ID, and Radio Signal Strength Indicator (RSSI) of the cell in real time. Initially, we identified a point with high signal strength (possibly close to the eNodeB) and marked it for the reference. Then we walked in all directions from the reference point till reaching the cell edge. Cell edges are identified when RSSI becomes very poor and the UE triggers a cell change. In this way, we traced the boundaries of the 5 cells and marked them inside the TA as shown in Figure 5. Based on the cell sizes measured, we find out that a major operator implemented micro cells in their LTE infrastructure. Typical size of a micro cell ranges from 200 - 2000 m in radius [39].

C. Passive attack - link subscriber locations/movements over time (L1)

In passive attack mode, attacker's objective is to collect a set of IMSIs and GUTIs which can be used for two purposes. One is to verify subscriber's presence in certain area, and other is to reveal his past and future movements in that area. To achieve this, we sniff over the LTE air interface and decode broadcast paging channels to extract IMSIs and GUTIs. These identities can be collected in locations such as airports or subscriber's home or office. The attacker needs to map IMSI or GUTI associated with a particular subscriber to reveal his/her presence in that area. Since GUTI is persistent for several days in our experiments (see Section V-B), its disclosure makes the subscriber's movements linkable. The mapping between GUTI and IMSI is possible using semi-passive attacks.

D. Semi-Passive attack - leak coarse location (L2)

The objective of the semi-passive attack is to determine the presence of a subscriber in a TA and further, to find the cell in which the subscriber is physically located in. In particular, we demonstrate the use of novel tracking techniques to initially determine the TA and then exploit Smart Paging to identify a cell within that TA.

Determining tracking area and cell ID

We use following two methods to generate signaling messages for performing the attack.

Using VoLTE calls: We placed 10 VoLTE calls to the victim. The VoLTE call connection times are very short at around 3 seconds according to previous work [40]. Hence, the attacker has to choose the call duration so that it is long enough for a paging request to broadcast by the eNodeB but short enough to not trigger any notification on the UE's application user interface. As explained earlier, VoLTE has high priority and therefore its paging requests are broadcast to all eNodeBs in a TA. Hence it is sufficient to monitor any single cell within the TA for paging messages. The observed GUTIs undergo a set intersection analysis where we apply the method proposed by Kune et.al [2] to reveal the mapping between the GUTI and phone number of the subscriber. Once successful, the presence of the subscriber is confirmed in that TA.

Using social network and applications: Social identities are a compelling attack vector because mobile subscribers nowadays use mobile phones for accessing popular social networks and instant messaging applications. The primary intention of the attacker is to trigger paging requests via social identities without LTE subscribers being aware of it. For triggering paging messages, various mobile applications can be used. Due to popularity and size of user base we chose Facebook and WhatsApp applications for our experiments. However tracking subscribers using social applications is not as effective as using VoLTE calls.

We used Facebook messages as described in Section V-A to trigger Smart Paging to localize the target subscriber to a specific cell. Similar to VoLTE calls, we send 10-20 messages to the subscriber via Facebook and do the set intersection analysis to link GUTIs to Facebook profiles. If the mapping is successful in a particular cell where the attacker is, the presence of the subscriber is confirmed. Otherwise the attacker needs to move to other cells and repeat the same procedure. The attacker can also place passive sniffers in every cell to speed up the localization procedure. However, this is expensive. The subscriber's presence is successfully determined in a cell a cell that is typically of size 2 km^2, i.e. much smaller than a GSM cell.

We also used WhatsApp similarly to exploit its "typing notification" feature. In this case, the attacker requires the phone number to identify the subscriber on WhatsApp. In addition, the victim's privacy settings must allow the attacker to view the victim's WhatsApp profile. First, the attacker sends a message to the target recipient. Once it is received, the recipient's WhatsApp application will list it in the inbox. For the attack to succeed, it is essential that the recipient does not block or delete the attacker's contact. Later, the attacker opens his active chat window corresponding to the recipient and composes a message but does not send. Due to the "typing notification" feature, the recipient can see that the attacker is typing in the chat window. During this procedure, network triggers paging request destined for recipient's LTE devices.

E. Active attack - leak fine-grained location (L3)

Once the attacker determines a TA and cell where the subscriber is present, the next goal is to find his/her location more precisely. We now demonstrate two methods in which the attacker exploits a specification and an implementation vulnerability to this end.

1. Via measurement reports: We consider a subscriber who is initially attached to a legitimate eNodeB. The attacker forces him/her to attach to a rogue eNodeB by applying the techniques mentioned in Section IV-B. The subscriber's UE completes RRC connection procedures and initiates a *TAU* procedure with attacker's rogue eNodeB. Next, UE enters into CONNECTED state. The attacker creates a *"RRC Connection Reconfiguration"* message with different cell IDs (possibly 3 or more neighbor cells) and necessary frequencies, and sends it to the UE without any protection. After receiving this unprotected message, UE computes the signal power from neighboring cells and frequencies and sends an unprotected *"Measurement Report"* message to the rogue eNodeB.

If the UE supports *'locationInfo-r10'* feature [5], it includes its GPS coordinates in the measurement report. This feature is not yet widely supported by current smartphones - however one of our test phone exhibited this behavior.

2. Via RLF reports: In this attack, two rogue eNodeBs are operated in the same cell where the subscriber is present. Initially eNodeB 2 is OFF and eNodeB 1 ON to create a RLF scenario to the UE. The UE initiates connection to eNodeB 1 and enters into CONNECTED state as shown in Figure 6. We turn OFF eNodeB 1 upon receiving a TAU request from the UE. At the same time, eNodeB 2 is turned ON. Meanwhile UE detects that it has lost sync with the eNodeB 1 and starts RLF timer (T310).

When the RLF timer expires, UE creates a RLF report [5] and goes into IDLE mode. In this mode, UE starts cell selection procedure as specified in [12] to attach to eNodeB 2. As before, UE enters the CONNECTED state with eNodeB 2 and indicates the availability of RLF report in a TAU message. Upon receiving this message, the attacker sends an unprotected *"UEInformationRequest"* message to UE from eNodeB 2, thereby requesting UE to send RLF report to eNodeB 2 in response. As a result, UE sends the resulting response in an unprotected *"UEInformationResponse"* message containing the RLF report. This report contains failure events and specifically signal strengths of neighboring eNodeBs.

In addition, according to the LTE specification [41], RLF report can include GPS coordinates [5] of UE at the time it experienced the radio failure. As before, this feature is not widely implemented yet.

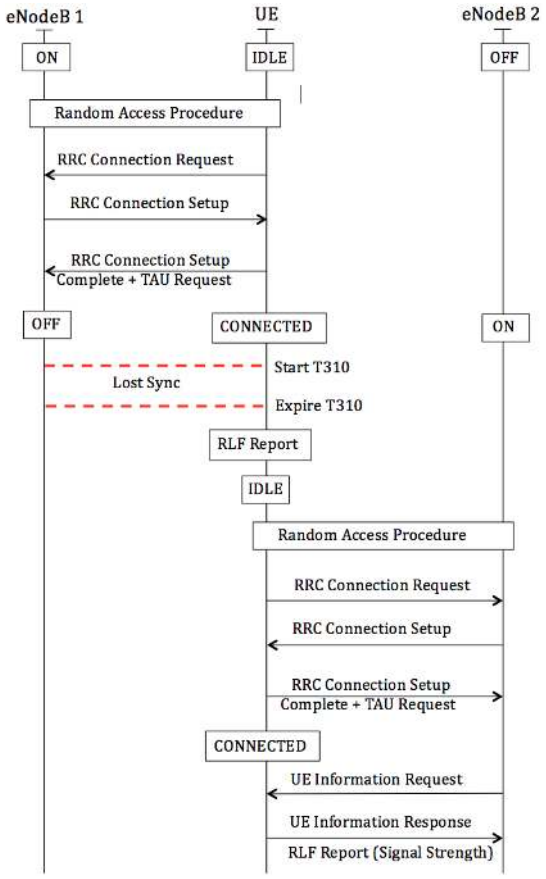

Fig. 6. Retrieving RLF report from UE (L3)

Determining subscriber's precise location

Aforementioned measurement and RLF reports provide signal strengths allowing the active attacker to calculate distance between the UE and the rogue eNodeB. This calculation is performed using a trilateration technique as described in [42]. Figure 7 shows how this technique is used to determine subscriber's location. The distance estimates are calculated as d1, d2, and d3 for three neighboring base stations. The zone of intersection point of three circles is subscriber's approximate location in a cell. However, if *'locationInfo-r10'* feature is supported in measurement and RLF reports, accurate location can be determined using GPS coordinates.

Fig. 7. Determining subscriber's precise location using trilateration (L3)

VI. DoS Attacks on LTE Air Interface

In this section, we demonstrate how an attacker can exploit two LTE specification vulnerabilities to deny LTE, and also GSM and 3G network services to subscribers. First, we describe the attack background and present three types of persistent DoS attacks labeled D1, D2, and D3. Later, we discuss their impact on LTE subscribers and operator services.

A. Attack background

We exploit the EPS Mobility Management (EMM) protocol messages which are required for control of UE mobility in LTE networks. In particular, we exploit two functions of EMM messages described below.

1. TAU procedure: One of the main function of EMM protocol messages is to inform the network about UE's present location in the serving area of the operator. This allows the MME to offer network services to the UE, e.g., when there is a incoming call. For this purpose, UE notifies the MME of its current TA by sending a *"TAU Request"* message and also includes its network modes. Generally, UE operates in various network modes for voice and data connections as stated in [11], but for this work we focus only on two modes: i) EPS services (i.e., LTE services), ii) both EPS and non-EPS (i.e., GSM or 3G) services. During a *TAU* procedure, the UE and MME agree on one of these modes depending on the type of subscription (for example, USIM is subscribed for LTE services), and network capabilities supported by the UE and by the operator in a particular area.

During *TAU* procedure the network may deny some services to UEs, for example if the subscriber's USIM is not authorized for LTE services or if the operator does not support certain services in the serving area. The LTE specification [11] defines certain EMM procedures to convey such denial messages to UEs. Specifically, these are sent in *"TAU Reject"* messages which are not integrity protected.

2. LTE Attach procedure: During an *Attach* procedure, UE sends a list of its capabilities to the network in an *"Attach Request"* message. In particular, these capabilities include supported networks (such as LTE, GSM or 3G), security algorithms, and other features as defined in [11]. However, these capabilities are sent unprotected and hence, the list can be altered by an attacker. To protect against MiTM attacks, the LTE security architecture mandates reconfirmation of previously negotiated security capabilities after the AKA procedure [10]. In particular, the network sends an integrity-protected message including the list of supported security algorithms previously received from the UE. However, there is no similar confirmation for UE's network capabilities.

B. Downgrade to non-LTE network services (D1)

We identify a vulnerability in the LTE specification which enables the following DoS attacks D1. We exploit the fact that certain *"TAU Reject"* messages sent from the network are accepted by UEs without any integrity protection. In particular, there is no need of mutual authentication and security contexts between the UE and network for accepting such reject messages. Note that, the attacker does not need any security keys to send *"TAU Reject"* messages. Hence, the attacks can be targeted towards any LTE subscribers within the range of the rogue eNodeB. Similar types of attacks are also possible with *"Service Reject/ Attach Reject"* messages.

As shown in Figure 8, the UE sends *"TAU Request"* message to attacker's rogue eNodeB. Note that as the UE is attached to the real network, this message can be integrity protected using the existing NAS security context. However, according to LTE specification [11](section 4.4.5), this message is not encrypted. As a result, rogue eNodeB decodes it and responds with a *"TAU Reject"* message. The attacker includes EMM cause number 7 *"LTE services not allowed"* into this message. As no integrity protection is required, the victim's UE accepts the message. The UE proceeds to act on the indicated rejection cause by deleting all existing EPS contexts associated with the earlier (real) network.

As a result, UE updates its status to *"EU3 ROAMING NOT ALLOWED"*[7] and considers the USIM and hence the UE as invalid for LTE services until it is rebooted or USIM is re-inserted. Further, UE does not search for or attach to legitimate LTE networks even if they are available in that area, causing a denial of service. However, if supported, the UE searches for GSM or 3G network in the same area to gain network services. By downgrading subscribers, an attacker could attempt to launch known 2G or 3G attacks, besides loss of LTE services.

[7]It means that last *TAU* procedure was correctly performed, but reply from the MME was negative due to roaming or subscription restrictions.

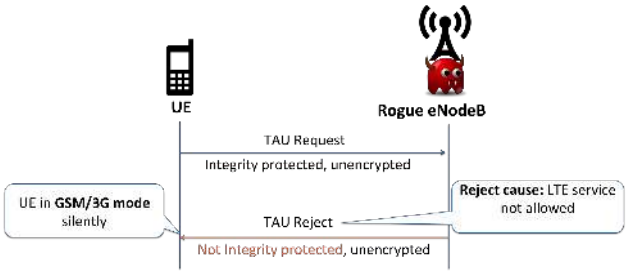

Fig. 8. DoS attack - denying LTE network services (D1)

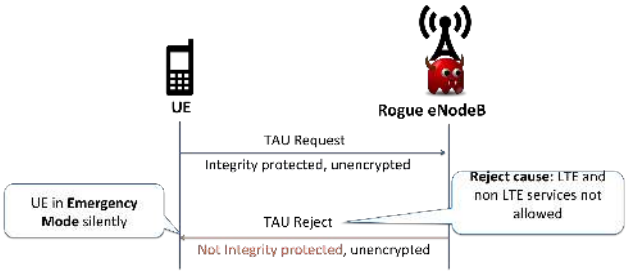

Fig. 9. DoS attack - denying all mobile network services (D2)

C. Denying all network services (D2)

D2 is similar to D1 but the result is different. The UE initiates TAU request procedure and rogue eNodeB responds with a TAU Reject message with the cause number 8 which is *"LTE and non-LTE services not allowed"*. After receiving this message, the UE sets LTE status to *"EU3 ROAMING NOT ALLOWED"* and considers USIM invalid for the network until it is rebooted or USIM is re-inserted. Further, it enters the state EMM-DEREGISTERED: UE's location is unknown to the MME and is not reachable for any mobile services. As a result, UE does not attempt to attach to LTE, GSM, or 3G networks for normal services even if networks are available. The UE remains in the EMM-DEREGISTERED state even it moves to a new TA or even to a new city, thereby causing a persistent denial of service. Signaling messages exchanged between the UE and the rogue eNodeB are shown in Figure 9.

D. Denying selected services (D3)

In this attack, the active attacker modifies messages exchanged between the eNodeB and UE. However, note that this attack was not performed during our experiments due to unavailability of UE baseband software.

The UE initiates an *"Attach Request"* message to the eNodeB and this message is intercepted by the attacker. The message contains *"Voice domain preference and UE's usage setting"* which informs the network about UE's voice calling capabilities. The attacker removes these capabilities from this unprotected message and adds *"Additional update type - SMS only"* before forwarding it to the network. The network accepts this message and executes AKA protocol with the UE to complete *Attach* procedure. However at this step, the MME configures UE's profile with the received (modified) capabilities, thereby allowing only SMS and data services. When there is an incoming call for UE, the MME rejects it and informs the cause to the subscriber who is calling. On the other hand, if UE tries to make an outgoing voice call, the network

rejects this request and informs the cause. This is an example of a bidding down attack. The denial is persistent since the attack is effective even after the attacker has moved away. However, the user can recover from the attack by restarting the UE or moving to another TA. 3GPP specifications does indeed mention a timer (T3245) that a UE can use to recover from EMM DISCONNECTED state [43]. However, the use of this timer is optional (none of the devices we tested implement this timer). The default timer value (24-48 hours) is too large in the case of DoS attacks.

E. Impact on end-users and operators

Unlike the LTE jamming DoS attacks described in [44], our attacks are against UEs in a certain area instead of against LTE networks. A successful attack would deny the target UE from utilizing network services. Typically, the UE remains in non-service state for some time period even if the attacker shuts down his rogue eNodeB or moves away from attacking area. Consequently, this attack is more serious than other types of DoS attacks (for example jamming and RACH flood [45] that are difficult to prevent). Impact of these attacks are as follows:

- Subscriber's UE may not alert the user about the unavailability of legitimate services. However, depending on the alert notification capabilities provided by application layer of various mobile operating systems installed on the UE, the subscriber could be notified of limited services or no network connectivity status. We noticed that there is no standard approach across different mobile operating systems to indicate the type of active network mode (e.g., 2G/GSM, 3G, LTE) to the user.
- Subscribers will not be able to receive or make normal calls and data connections. Hence, a significant loss is incurred to both network operators and their subscribers. Network operators are not able to offer services since subscribers are unavailable technically and no billing would occur.
- UE can still make emergency calls. However, emergency calls are not possible when UE is attached to a rogue eNodeB.
- LTE-capable M2M devices which are not attended by technicians on a daily basis could be blocked out from network services for a long time. This is due to the fact that M2M devices need to be rebooted or USIM needs to re-inserted to recover from the attacks.

VII. Attack Feasibility and Amplification

In this section, we discuss the feasibility of both location leak and DoS attacks against popular LTE smartphones and methods to amplify the coverage range of our attacks.

Several of the vulnerabilities we exploited are in the LTE specifications rather than in the UE's baseband software. Therefore, all LTE-capable UEs conforming to these specifications are affected. For evaluation, we selected popular smartphones incorporating baseband implementations from top vendors who dominate the market share worldwide [46]. We successfully verified that all these phones are vulnerable to our attacks. In addition, all UEs have the implementation vulnerability leading to attack L3.

We further investigated on how UEs recover from DoS attacks. We found out that all UEs recover after rebooting or re-inserting the USIM. Additionally, UEs having baseband from most vendors can recover by toggling the flight mode.

Attack amplification: Related to our passive attacks, we determined the average cell radius of a major operator in a city is 800 meters for the 2.6 GHz and 1 km for the 800 MHz frequency band. The USRP B210 used for our attacks has a maximum output power of 20dbm (100mW) [47] with a coverage range of 50 to 100 meters. However, the signal coverage area can be increased with a suitable power amplifier. Specifically, based on the COST 231 radio propagation model [48], we calculated that by mounting a USRP at a height of 10m (e.g., on a street lamp) and amplifying the power by 10 dB, it is possible to deny LTE and non-LTE services for every subscriber in a cell. For a reference, `OpenBTS` projects [49], [50] use USRPs to provide GSM coverage in rural areas with $>$2 km coverage with an external power amplifier and antenna. Similarly, signal coverage area of our rogue eNodeB could be increased to demonstrate feasibility of the attack.

VIII. Security Analysis

In this section, we discuss vulnerabilities discovered in the specifications and their impact on LTE security. We explain the background behind the vulnerabilities by considering various trade-offs between security and criteria like availability and performance. We show that the equilibrium points in the trade-offs have shifted today compared to where they were when the LTE security architecture was being designed. We also discuss countermeasures for the vulnerabilities that made our attacks possible. Table II summarizes our analysis.

A. Possible trade-offs

Security vs Availability: We demonstrated a vulnerability in the LTE RRC protocol specification that allows the adversary to obtain unprotected measurement reports from UEs (L3). We consider the following two angles to explain the trade-off. On one hand, in some cases network operators require unprotected reports for troubleshooting purposes. In particular, if the UE is not able to establish connection with the eNodeB then it may be necessary to send measurement reports without protection in order allow the network to identify technical reason behind the fault. This seems to be the reasons behind the note in LTE RRC specification which points out that the 3GPP Radio Access Network (RAN2) working group decided to permit UEs to send reports even without security activation [5]. On the other hand, during the design work for the LTE security architecture, the 3GPP security working group (SA3) suggested that all RRC protocol messages should be sent in encrypted form [51]. Hence, the vulnerability in RRC protocol specification is a conscious exception to this security design guidance [5]. Clearly, 3GPP has concluded that in this particular case the requirement of having network availability all the time to all UEs outweighs security concerns related to subscribers' privacy.

Security vs Performance: We observed that UEs are required to reboot or re-insert USIM after DoS attacks in order to

regain network services. This behavior, exhibited by all LTE devices we tested, is according to the LTE specification. Since the network denies services for valid reject causes described in [11], the UE restricts itself from re-initiating LTE (or any mobile network) *Attach* procedure in order to conserve battery power. In addition, frequent unsuccessful *Attach* requests from UEs would increase signaling load on the network. These are the reasons why the LTE specification requires the UE to reboot or re-insert USIM to recover from reject messages. This preference of performance over security leaves LTE subscribers vulnerable to the DoS attacks (D1 & D2).

As another example, during *Attach*, UE's security capabilities are sent back to it for confirmation after security activation in order to protect against bidding down attacks. This is an application of the well-known 'matching history' principle used in security protocol design [52]. However, UE's network capabilities are not protected in similar manner, enabling a different type of bidding down attack (D3). The reason for not applying the matching history principle to all negotiated parameters, as discussed in VI-A, indicates another trade-off where added security has not outweighed performance loss due to the full application of the matching history principle. To apply the matching history principle to all parameters would have required the inclusion of a cryptographic hash of all the parameters, instead of the parameters themselves. However, confirming only the security information capabilities, which take up much less space (only a few bits) compared to a full cryptographic hash, minimizes the overhead in signaling.

A third example we observed is that in some operator networks, GUTIs are not changed even after three days of usage (L1). LTE specifications do not mandate any GUTI reallocation frequency, leaving it to as a policy decision to operators. One possible reason for the low GUTI-change frequency is the operators' wish to reduce signaling overhead by trading off privacy.

Security vs Functionality: Our attacks that leak coarse-grained location information by using social network messaging services (L2) is an example of the tension between security and functionality. The introduction of TCP/IP based data communication on top of mobile communication infrastructures has greatly expanded the functionality that third party developers can build for these networks. But such a flexible software architecture makes it harder to avoid or detect the type of vulnerability that led to this attack. Furthermore, even if individual app developers would fix their applications (e.g., Facebook could change the application architecture of their Messenger application to ensure that messages that end up in the "Other" box do not trigger paging requests), other application developers may make similar mistakes. To avoid such vulnerabilities in a modern mobile communication system like LTE, it would require significant developer outreach and education to help them design and build mobile optimized applications [53].

Summary: The design philosophy of LTE security required leaving some safety margin in security mechanisms in order to protect against changes in trade-offs. However, in the above cases the safety margins turn out to be too narrow. As a general learning on an abstract concept level, it would be better to include agility in the security mechanisms instead of a rigid safety margin. The forthcoming fifth generation (5G) technology will offer better possibilities to engineer agility and flexibility for security because software defined networking and cloud computing are among the key concepts of emerging 5G architectures.

3GPP follows the good practice of documenting exceptions when specification needs to deviate from the general security design principles recommended by the security working group (as was the case with L3 or D1/D2/D3). We recommend further that each such exception should also trigger an analysis of its implications. For example, if an exception is made to forego integrity protection for a denial message from the network, then the standards group should consider what happens and how to recover if the denial message contains incorrect information.

B. Countermeasures and discussion

We now discuss potential countermeasures against attacks demonstrated in earlier sections. In particular, we identify protocol-level and operational fixes that can be implemented by baseband vendors and mobile network operators. Some of these countermeasures are much more straight-forward than others. Similarly, some of our proposals may cause hidden dependencies and more changes may be needed in the networks than what is apparent from our descriptions.

Protection against location leaks: LTE broadcast information include subscriber identities which enable tracking of UEs (L1 and L2). The broadcast information must be sent in unprotected messages from LTE system design perspective. There are two solutions to avoid UEs being tracked. One solution is to protect broadcast messages using a public key mechanism but this requires relatively big changes in LTE protocols. According to [54], 3GPP decided against usage of public key mechanisms because its implementation cost was deemed too high. However, our findings may have changed the equilibrium in this trade-off. Consequently, a scheme where public/private keys are used only for network elements could possibly be justified now. Messages from the network could be signed by using a public key digital signature mechanism; UEs would then be able to verify the authenticity of such messages. This would prevent rogue network elements from sending false information, e.g., false messages indicating radio link failures (L3). Messages towards the network could be encrypted using the public key of the serving operator; UEs would not need to send their identities in the clear to initiate network *Attach* procedure. It is not easy to protect paging messages with public key mechanisms, even if we would have public keys for UEs because UEs would have to try to decrypt all paging messages. All these proposed fixes require ensuring global availability and verifiability of public keys of network components (such as eNodeB).

The second solution is more realistic as it does not require change in protocols. Network operators would simply re-allocate GUTIs often enough to avoid tracking. One of the national operators to whom we reported our findings, acknowledged the feasibility of our attacks and already configured their networks to prevent tracking based on GUTIs. This solution would protect against passive attacks (L1). A certain degree of protection against semi-passive adversaries could be achieved by making the adversary's actions more visible to the subscriber. There are already such tools [31], [32] available

Attack		Adversary	Vulnerability		Potential fix
Group	Description	Type	Type	Possible trade-off	
Location Leak	Link location over time (L1)	Passive	Underspecification	(Perceived) security vs availability	Policy to guarantee GUTI freshness
	Leak coarse-grained location (L2)	Semi-passive	Application software architecture	Security vs functionality	Tools like Darshak [31] & SnoopSnitch [32] to visualize suspicious signaling to subscribers
	Leak fine-grained location (L3)	Active	Specification & implementation flaw	(Perceived) security vs availability	Network authentication for requests; ciphering for responses
Denial of Service	Downgrade to non-LTE services (D1)	Active	Specification flaw	Security vs performance	Timer-based recovery
	Deny all services (D2)	Active	Specification flaw	Security vs performance	Timer-based recovery
	Deny selected services(D3)	Active	Specification flaw	Security vs performance	Extend "matching conversation" check to more (all) negotiation parameters

TABLE II: LTE attacks, vulnerability analysis, and fixes

but the challenge is in making them usable and useful to all types of subscribers. LTE specification vulnerability regarding UEs sending measurement reports without integrity protection needs to be addressed by the 3GPP security group in order for all baseband vendors to eventually implement the fix in their products. The simplest solution is to transmit measurement reports only after setting up the security context.

Protection against DoS: The specification vulnerabilities responsible for DoS attacks based on *TAU* procedure (D1 and D2) can be fixed without changes in the protocol itself. The 3GPP SA3 group may propose a new mechanism based on a counter or timer value to recover from DoS attacks. If the UE is detached from the network for a certain duration as a result of a *TAU* reject messages, it should reset the configuration settings in the USIM or baseband to re-attach itself with the network without bothering the user, i.e., without having to reboot or require re-insertion of USIM. If there is an infrastructure to support distribution of operator public keys, *TAU* reject messages could be signed by the network and verified by UEs.

Next, we discuss protection against DoS stemming from bidding down attacks (D3). During an *Attach* procedure, the UE's network and security capabilities are sent to the network. The attacker can modify this list to downgrade capabilities reported by the UE and and forward it to the network. To protect against such modification, both 3G and LTE contain the partial 'matching history' mechanism discussed above. This allows UE to check that its original list of security capabilities are identical with the ones received by the network. We argue that similar protection for network capabilities is required due to the fact that the DoS attack has a persistent nature. This would of course require change in the LTE protocols. Again, with the use of operator public keys, it would be possible to use digital signatures to protect lists of capabilities broadcast by the network. Alternatively, the negotiation of network capabilities could be done after AKA is successfully completed.

IX. Related work

In this section, we describe related work in GSM, 3G, and LTE air-interface security area. Previous works have reported attacks against 2G and 3G access network protocols [2], [55], core network protocols [56], [57], [58], [59], as well as services [60]. In passive attacks, Kune et al. [2] showed that despite the use of temporary IDs, the location of a subscriber's UE in a GSM network can be leaked. In specific, it was shown that an attacker can check if a UE is within a small area, or absent from a large area, without subscriber's awareness. However, their location leaks granularity is lower and it is improved with our attacks on LTE networks. The 3GPP discuss a set of threats exposed in E-UTRAN [51] during LTE security study. However, the attacks we presented are not identified by the study. In active attacks, the authors in [61] present a method to determine the presence of a subscriber in a particular area by exploiting a vulnerability in 3G AKA protocol. By leveraging a rogue eNodeB (femtocell), previously captured authentication parameters are replayed to the UE and the presence is confirmed based on the response from the phone. However their attack cannot reveal approximate location of the UE in a given area.

In DoS attacks, the authors in [44] describe that unauthenticated attach requests sent from a compromised UE/eNodeB to flood the MME and in turn to the HSS, leading to a DoS attack. However their DoS attacks are against the network and not against LTE subscribers. Through simulations the authors in [62] show that Botnets can cause DoS attacks by exhausting subscriber traffic capacity over the air interface. A proof of concept paper by P. Jover et al. [63] provides an overview of new effective attacks (smart jamming) that extend the range and effectiveness of basic radio jamming. However according to [54], both aforementioned flooding and jamming attacks are non-persistent DOS attacks hence not considered as a threat to address in the LTE architecture. In contrast, our DoS attacks are persistent and targeted towards the UE (subscribers). LTE security architecture and a detailed list of security vulnerabilities existing in the LTE networks have been presented in [64]. Our attacks are not presented in this survey. Two recent papers [65], [66] discuss resource stealing and DoS attacks against VoLTE, whereas our focus is against LTE access network protocols. To the best of our knowledge, there was no previous work evaluating practical attacks on LTE access networks in the literature.

X. Conclusion

We have shown that the vulnerabilities we discovered in LTE access network protocols lead to new privacy and availability threats to LTE subscribers. We demonstrated that our attacks can be mounted using open source LTE software stack and readily available hardware at low cost. The need for engineering the correct trade-offs between security and other requirements (availability, performance, and functionality) led to the vulnerabilities in the first place. Such trade-offs are essential for the success of any large-scale system. But the trade-off equilibrium points are not static. We recommend that future standardization efforts take this into account.

Impact: We followed standard responsible disclosure practices of all affected manufacturers. We also notified affected operators as well as the standards body (3GPP). All four

manufacturers acknowledged our report. Two of them have already released patches [67], [68]. Two of three operators have fixed the configuration issues in their networks. 3GPP has initiated several updates to the LTE specifications to address the issues we raised [69]. Up-to-date information about impact may be found in the arXiv report version of this paper [6] and on our project website[8].

Acknowledgments: This work was supported in part by the Intel Collaborative Research Institute for Secure Computing[9], Academy of Finland ("Cloud Security Services" project #283135) and Deutsche Telekom Innovation Laboratories (T-Labs)[10]. T-Labs, Aalto University, and Huawei provided test devices used in our experiments. We thank Stefan Schröder, Peter Howard, Steve Babbage, Günther Horn, Alf Zugenmeier, Silke Holtmanns, and the anonymous reviewers for their thoughtful feedback on previous versions of this paper.

REFERENCES

[1] ABI. LTE Subscriber Base to Grow to 1.4 Billion Globally by Year-end 2015 . [Online]. Available: https://www.abiresearch.com/press/lte-subscriber-base-to-grow-to-14-billion-globally/

[2] N. H. Foo Kune, John Koelndorfer and Y. Kim, "Location leaks on the GSM air interface," in *19th Network and Distributed System Security Symposium*, 2012.

[3] Facebook Inc. Facebook Messenger. [Online]. Available: https://www.messenger.com/features

[4] WhatsApp Inc. WhatsApp Messenger. [Online]. Available: http://www.whatsapp.com

[5] 3GPP. TS 36.331. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification. [Online]. Available: http://www.3gpp.org/dynareport/36331.htm

[6] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, Jean-Pierre Seifert. Practical attacks against privacy and availability in 4G/LTE mobile communication systems . [Online]. Available: http://arxiv.org/abs/1510.07563

[7] 3GPP. Characteristics of the Universal Subscriber Identity Module (USIM application) 3GPP TS 31.102 version 12.5.0 Release 12. [Online]. Available: http://www.3gpp.org/dynareport/31102.htm

[8] 3GPP. Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 12.5.0 Release 12). [Online]. Available: http://www.3gpp.org/dynareport/23003.htm

[9] 3GPP. Network Architecture ; Specification 3GPP TS 23.002 version 12.7.0 Release 12. [Online]. Available: http://www.3gpp.org/DynaReport/23002.htm

[10] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects. Universal Mobile Telecommunications System (UMTS); LTE; System Architecture Evolution (SAE); Security architecture; (3GPP 33.401 version 12.14.0 Release 12). [Online]. Available: http://www.3gpp.org/dynareport/33.401.htm

[11] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 Specification 3GPP TS 24.301 version 12.8.0 Release 12. [Online]. Available: http://www.3gpp.org/dynareport/24301.htm

[12] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; evolved universal terrestrial radio access (E-UTRA); user equipment (UE) procedures in idle mode; Specification 3GPP TS 36.304 version 12.4.0 Release 12. [Online]. Available: http://www.3gpp.org/dynareport/36304.htm

[13] 3GPP. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); overall description; stage 2, Specification 3GPP TS 36.300 version 12.4.0 Release 12. [Online]. Available: http://www.3gpp.org/dynareport/36300.htm

[14] Melih Tufan. Packet Networks Portfolio. [Online]. Available: http://www.ericsson.com/ericsson/investors/doc/2011/ap_forum/ericsson_apac_forum_150911_packet_networks.pdf

[15] David Nowoswiat. Managing LTE core network signaling traffic. [Online]. Available: http://www2.alcatel-lucent.com/techzine/managing-lte-core-network-signaling-traffic/

[16] Nokia Networks. Voice over LTE (VoLTE) Optimization. [Online]. Available: http://networks.nokia.com/sites/default/files/document/nokia_volte_optimization_white_paper_071114.pdf

[17] D. Strobel, "IMSI catcher," *Chair for Communication Security, Ruhr-Universität Bochum*, p. 14, 2007.

[18] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2004.

[19] Ettus. USRP B210. [Online]. Available: http://www.ettus.com/product/details/UB210-KIT

[20] Osmocom. RTL-SDR. [Online]. Available: http://sdr.osmocom.org/trac/wiki/rtl-sdr

[21] Ben Wojtowicz. OpenLTE Project Homepage. [Online]. Available: http://openlte.sourceforge.net/

[22] srsLTE. Open source 3GPP LTE library. [Online]. Available: https://github.com/srsLTE/srsLTE

[23] Facebook Inc. Facebook Mobile. [Online]. Available: https://www.facebook.com/mobile/

[24] 3GPP. TS 36.133. Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management; Version 8.23.0; Release 8. [Online]. Available: http://www.3gpp.org/dynareport/36133.htm

[25] Osmocom Project. What is GSMTAP? [Online]. Available: http://bb.osmocom.org/trac/wiki/GSMTAP

[26] Wireshark - network protocol analyzer. [Online]. Available: https://www.wireshark.org/

[27] Gamry Instruments. The Faraday Cage: What is it? How does it work? [Online]. Available: http://www.gamry.com/application-notes/instrumentation/faraday-cage/

[28] Nokia Blog. A signaling storm is gathering Is your packet core ready? . [Online]. Available: https://blog.networks.nokia.com/mobile-networks/2012/12/05/a-signaling-storm-is-gathering-is-your-packet-core-ready/

[29] Stoke. Charting the Signaling Storms. [Online]. Available: http://www.slideshare.net/zahidtg/charting-the-signaling-storms-stoke

[30] K. Nohl and S. Munaut, "Wideband GSM sniffing," in *27th Chaos Communication Congress*, 2010. [Online]. Available: http://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html

[31] Udar Swapnil. Darshak Framework. [Online]. Available: https://github.com/darshakframework/darshak

[32] SR Labs. SnoopSnitch. [Online]. Available: https://opensource.srlabs.de/projects/snoopsnitch

[33] David Pogue. Two Tips for Facebook Users. [Online]. Available: http://pogue.blogs.nytimes.com/2013/07/18/two-tips-for-facebook-users/?src=twr&smid=tw-nytimes&_r=0

[34] Ramtim Amin. 4G Wireshark dissector for Samsung USB stick. [Online]. Available: http://labs.p1sec.com/2013/08/18/4g-wireshark-dissector-based-on-samsung-usb-stick/

[35] XDA-Developers. LG G3 Field Test Mode. [Online]. Available: http://forum.xda-developers.com/lg-g3/general/lg-g3-field-test-mode-how-to-check-lte-t3128275

[36] ENAiKOON. OpenCellID. [Online]. Available: http://opencellid.org/

[37] N. Golde, K. Redon, and J.-P. Seifert, "Let me answer that for you: Exploiting broadcast information in cellular networks," in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 33–48. [Online]. Available: http://dl.acm.org/citation.cfm?id=2534766.2534770

[38] Cell Mapper. [Online]. Available: https://play.google.com/store/apps/details?id=cellmapper.net.cellmapper

[8] http://se-sy.org/projects/netsec/lte/

[9] http://www.icri-sc.org/

[10] http://www.laboratories.telekom.com/public/english/

[39] JPL Wireless communications. Cell Sizes. [Online]. Available: http://www.wirelesscommunication.nl/reference/chaptr04/cellplan/cellsize.htm

[40] Signals Research Group. VoLTE Performance Analysis. [Online]. Available: http://www.signalsresearch.com/Docs/LTE%20NA%202014%20VoLTE%20Results%20-%20SRG%20Presentation.pdf

[41] 3GPP. Universal Terrestrial Radio Access (UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRA); Radio measurement collection for Minimization of Drive Tests (MDT); Overall description; Stage 2. [Online]. Available: http://www.3gpp.org/DynaReport/37320.htm

[42] J. Caffery and G. Stuber, "Overview of radiolocation in CDMA cellular systems," *Communications Magazine, IEEE*, vol. 36, no. 4, pp. 38–45, Apr 1998.

[43] 3GPP. Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. [Online]. Available: http://www.3gpp.org/dynareport/24008.htm

[44] R. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, June 2013, pp. 1–9.

[45] Osmocom. RACH flood DoS. [Online]. Available: http://security.osmocom.org/trac/ticket/1

[46] IDC. Smartphone Vendor Market Share, Q1 2015 . [Online]. Available: http://www.idc.com/prodserv/smartphone-market-share.jsp

[47] Matt Ettus. Ettus Research update. [Online]. Available: http://static1.1.sqspcdn.com/static/f/679473/23654458/1381240753367/grcon13_ettus_products.pdf?token=ldHVQF0yAdZLWvdjhPjqLtrhB9I%3D

[48] Y. Singh, "Article: Comparison of Okumura, Hata and COST-231 Models on the Basis of Path Loss and Signal Strength," *International Journal of Computer Applications*, vol. 59, no. 11, pp. 37–41, December 2012, full text available.

[49] Jim Forster. OpenBTS and Range Networks. [Online]. Available: http://www.mastel.or.id/files/Open%20BTS_Jim%20Foster.pdf

[50] UmTRX. Open source, cost optimised and future-proofing flexibility. [Online]. Available: http://umtrx.org/about/

[51] 3GPP. Rationale and track of security decisions in Long Term Evolved(LTE) RAN / 3GPP System Architecture Evolution (SAE (Release 8), TR 33.821 V1.1.0. [Online]. Available: http://www.3gpp.org/DynaReport/33821.htm

[52] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des. Codes Cryptography*, vol. 2, no. 2, pp. 107–125, Jun. 1992. [Online]. Available: http://dx.doi.org/10.1007/BF00124891

[53] GSMA. GSMA Announces New Initiatives Focusing On Creating More Efficient Mobile Applications . [Online]. Available: http://www.gsma.com/newsroom/press-release/gsma-announces-new-initiatives-focusing-on-creating-more-efficient-mobile-applications/

[54] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE security*. John Wiley & Sons, 2012.

[55] P. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007, pp. 1289–1297.

[56] N. Golde, K. Redon, and R. Borgaonkar, "Weaponizing femtocells: The effect of rogue devices on mobile telecommunications," in *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012*, 2012. [Online]. Available: http://www.internetsociety.org/weaponizing-femtocells-effect-rogue-devices-mobile-telecommunications

[57] P. Traynor, P. McDaniel, and T. La Porta, "On attack causality in internet-connected cellular networks," in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, ser. SS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 21:1–21:16. [Online]. Available: http://dl.acm.org/citation.cfm?id=1362903.1362924

[58] R. Racic, D. Ma, H. Chen, and X. Liu, "Exploiting opportunistic scheduling in cellular data networks," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2008, San Diego, California, USA, 10th February - 13th February 2008*, 2008. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/08/papers/21_exploiting_opportunistic.pdf

[59] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. D. McDaniel, and T. F. L. Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009*, 2009, pp. 223–234. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653690

[60] W. Enck, P. Traynor, P. McDaniel, and T. F. L. Porta, "Exploiting open functionality in sms-capable cellular networks," in *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005*, 2005, pp. 393–404. [Online]. Available: http://doi.acm.org/10.1145/1102120.1102171

[61] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New privacy issues in mobile telephony: Fix and verification," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 205–216. [Online]. Available: http://doi.acm.org/10.1145/2382196.2382221

[62] J. Jermyn, G. Salles-Loustau, and S. Zonouz, "An Analysis of DoS Attack Strategies Against the LTE RAN," in *Journal of Cyber Security, 3(2):159–180*, 2014.

[63] A. R. R. Piqueras Jover, Joshua Lackey, "Enhancing the security of lte networks against jamming attacks," in *EURASIP Journal on Information Security*, 2014.

[64] M. Ma, "Security Investigation in 4G LTE Networks," in *IEEE GLOBECOM*, 2012.

[65] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, "Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, 2015, pp. 328–339. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813718

[66] C. Li, G. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, 2015, pp. 316–327. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813618

[67] Huawei-PSIRT. Security Advisory - UE Measurement Leak. [Online]. Available: http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-459832.htm

[68] Qualcomm. Qualcomm Product Security . [Online]. Available: https://www.qualcomm.com/connect/contact/security/product-security/hall-of-fame

[69] 3GPP SA3. WG3-Security Anaheim Meeting . [Online]. Available: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_81_Anaheim/Docs/S3-152498.zip