Securing the Authentication Process of LTE Base Stations

Adegoke Babajide Seyi
Concordia University of Edmonton
Alberta, Canada
badegoke@student.concordia.ab.ca

Fehmi Jafaar
Computer Research Institute of Montreal
Quebec, Canada
fehmi.jaafar@crim.ca

Ron Ruhl
Concordia University of Edmonton
Alberta, Canada
ron.ruhl@concordia.ab.ca

***Abstract* – Securing sensitive information like the International Mobile Subscriber Identity has been a challenge on all generations of mobile telecommunication networks, i.e., 2G, 3G and 4G. In fact, many cases of compromising users' privacy in telecom networks have been reported such as the cases of rogue base stations capable of tracking, intercepting and collecting the sensitive data without the users' knowledge. To overcome these issues, we are proposing in this paper the use of a pre-shared key in the authentication process of Long-Term Evolution (LTE) base stations to local users. We are proposing a first hop authentication procedure to verify if the base station is legitimate by the User Equipment. We simulate our approach using the NetSim simulated environment to show how it is improving the data confidentiality in LTE networks.**

Keywords – The Long-Term Evolution standard, the EPS-AKA Authentication Procedure, User Equipment, base station, pre-shared Key, Authentication, International Mobile Subscriber Identity.

I. INTRODUCTION

Mobile communication technologies are playing an irreplaceable role in our daily activities. They are mainly enabling voice communication and high-speed data communication. In this context, The Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. Much of the LTE standard addresses the upgrading of 3G UMTS to what will eventually be 4G mobile communications technology. Moreover, the majority of the telecommunications companies around the world are adopting the LTE as their 4G wireless standard. Currently, hundreds of millions of smart phones with LTE capabilities are used for browsing the Internet, banking applications, mobile gaming, messaging, etc. Recent studies on LTE network reported concrete case of security vulnerabilities and threats [4, 17, and 18]. For example, a malware may compromise base station operating systems initiating abnormal and undesirable equipment behavior.

Mobile telecommunication networks define several permanent and temporary user identities such as the permanent identities International Mobile Subscriber Identity (IMSI) and International Mobile Station Equipment Identity (IMEI). One of the security vulnerabilities in mobile telecommunication networks is sending the IMSI in plain text by the User Equipment to the base station during the EPS-AKA Authentication Procedure. Indeed, an attacker could use this vulnerability to log user activities, modify the configuration of critical communications gateways, or sniff user traffic and sensitive information. Nevertheless, an attacker can obtain meta-information about the communication process (e.g., when and how often data is transmitted).

In this paper, we are proposing a mitigation of this security vulnerability by using a pre-shared key in the authentication process of LTE networks. We propose the use of a pre-shared key for mutual authentication in the initial authentication process between a User Equipment and LTE base stations. The proposed mutual authentication will aim to authenticate the base station to the User Equipment as legitimate and trusted. This will in turn protect the IMSI been sent during the initial authentication and registration processes of a User Equipment not to be sent to a malicious base station. Moreover, we are showing how to protect the confidentiality of the user information when he is using an equipment in a foreign area through the roaming services (as an attacker may try to exploit the current vulnerability in the LTE networks by pretending to be a roaming base station). We determined the performance of the proposed approach in the NetSim simulated environment. From the simulation results, we observed that the data confidentiality in LTE networks is improved while we are preserving an acceptable range of energy consumption, throughput, and delay.

The rest of the paper is organized as follows: in Section II, we are discussing the EPS-AKA authentication procedure and its weakness. Section III provides an

978-1-7281-7116-6/20/$31.00 ©2020 IEEE

overview of the related work. Section IV outlines the methodology used for the proposed pre-shared key authentication, followed by Section V, which discusses the implementation of the proposed pre-shared key authentication into the LTE network. The empirical study and results are discussed in Section VI. Finally, Section VII concludes the paper and its future work.

II. Background

A. EPS-AKA Authentication Procedure

The LTE network infrastructure consists of a set of User Equipment, base stations called Evolved NodeB, and the core network for mobility management. The eNodeB are the base stations of the LTE network. They are responsible for radio resource management and user data encryption. The LTE network uses the Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol as the authentication mechanism to enable the base station to verify the identity of a user device. A mutual authentication could be performed using this protocol as both the communicating parties in LTE networks need to confirm each other. In this protocol, the authentication procedure starts after the establishment of a connection between the User Equipment (UE) and the Mobile Management Entity (MME). The Mobile Management Entity sends an ID request to the User Equipment via the Evolved Node B (eNB). The User Equipment will respond by sending its International Mobile Subscriber Identity (IMSI) in plain text to the Mobile Management Entity. The MME will in turn request an Evolved Packet System (EPS) authentication vector (AV) from the Home Subscriber Server (HSS). Based on the IMSI of the UE, the HSS will look up the key (K) and a sequence number associated with that IMSI, the information, location information, and conversation information. An attacker can hide the real User Equipment with this information and can launch attacks on the network [1] [4].

B. EPS-AKA Authentication Weakness

The Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol improve the security and privacy of the LTE network but it still has its weaknesses and vulnerabilities. The main weakness of this protocol is that the International Mobile Subscriber Identity (IMSI) of a User Equipment (UE) is always sent in plain text in order to obtain service. This fact presents a breach of the confidentiality of the user information and can allow hackers to spy on users' cellular networks, modify the contents of their communications, and even reroute users to malicious or phishing websites. Concretely, when a User Equipment registers to the network for the first time, the User Equipment must send its IMSI in plain text, which makes it easy for an attacker to capture the IMSI using an IMSI catcher or a fake base station. With the obtained IMSI, an attacker can gather information which includes the subscriber.

Concretely, a set of researchers from Ruhr-Universität Bochum and New York University Abu Dhabi have developed three novel attacks against LTE technology that allowed them to map users' identity, fingerprint the websites they visit and redirect them to malicious websites by tampering with DNS lookups[1]. In addition, an attacker with a rogue base station can easily exploit the weakness. The attacker simply creates a rogue eNodeB and transmits signals at the same time the real eNodeB does, but with more power. When the User Equipment (UE) attempts to get service for the first time, the UE will be forced to connect to the rogue eNodeB because it has more signal strength thereby prompting the UE to transmit its IMSI in plain text to the rogue eNodeB for authentication. Consequently, the attacker can retrieve the IMSI of the UE which can lead to passive and active attacks [6] [7].

In this paper, we are adopting the shared secret authentication model described in a previous work [8] to enhance the mutual authentication between the UE and the local base stations. The scope of our solution is limited to users and base stations of a network in a specific area or geographical area. Moreover, we will present in this paper an approach to protect the user information in case that he uses an equipment in a foreign area through the roaming services (as an attacker exploit the vulnerabilities in the LTE networks by pretending to be a roaming base station).

III. Related Work

Cao et al. in [2] carried out a survey on the security aspect of the LTE network. An overview of the security functionalities of the network and some vulnerabilities in the security functionalities were listed. A survey on the existing solutions to these problems found that the EPS-AKA authentication mechanism was vulnerable to several kinds of passive and active attacks. In our current paper, we are seeking to add a first hop authentication procedure to the LTE network in order to protect the vulnerability of the EPS-AKA authentication mechanism mentioned in previous work [2]. Shaik et al. [6] analyzed the access network security protocols of LTE networks. Several issues in the LTE security standards and baseband chipsets were discovered by the authors during their analysis and an experimental base station was used to demonstrate how these issues can be exploited. In fact, an experiment was carried out to show active attacks in a Faraday cage in order not to interfere with other phone users. The approach

[1] https://alter-attack.net/

proposed in our current paper aims to face the rogue base station attack mentioned in paper [6].

Donegan [8] discussed the security implications in the LTE architecture and the implementation of IPsec Protocol in the LTE network. The author proposed the adoption of IPsec in LTE to secure the LTE network. First, a detailed discussion about authentication of eNodeBs using PKI and pre-shared keys were elaborated. Then the use of a "shared secret" authentication model for authentication of base stations paper proposed. In our proposed solution, we are adopting on the shared secret authentication model mentioned in [8]. Fortio [11] discussed the security vulnerabilities present in the LTE access network. Norrman et al. [9] studied various cases of users' privacy attacks in telecom networks. Their paper revealed that the IMSI-catcher takes advantage of the increase in operators in the traditional walled-garden trust model of mobile networks and the recovery mechanism to obtain IMSI from mobile devices. The authors proposed a method of protecting the IMSI that requires a pseudonym to be derived locally at the user equipment and the home network without affecting existing Universal Subscriber Identity Modules (USIMs). However, the proposed method does not completely protect the IMSI from curious serving networks because there are other ways IMSI could be obtained by serving networks. The authors also noted that some regulations and laws would render the proposed method illegal in some jurisdictions.

Cichonski and Franklin [12] discussed how rogue base station attacks are used to track devices and identity of users to perform a Man-the-Middle attack. They suggested the use of temporary identities by the UE and the use of IMSI-catcher-catcher during transmission as possible mitigation to this problem. Jimenez et al. [10] discussed the privacy issues related to the disclosure of the IMSI in the Radio Interface while it is being transmitted to establish a connection. Their paper proposed a solution for enhancing the privacy of IMSI in 5G systems. The authors presented a method in which the IMSI was encrypted by employing public-key cryptography. In this paper, we are also seeking to enhance the privacy of the IMSI by proposing a first hop authentication procedure in LTE networks. Ramadan et al. [14] surveyed works on the security of GSM, CDMA, and LTE cellular systems using PKI. They presented the security issues for each generation of mobile communication systems, then studied and analyzed the proposed schemes and gave some comparisons. The authors noted that these generations have many vulnerabilities, and huge security work is involved to solve such problems. The paper classified the mobile communication security schemes according to the techniques used for each cellular system and covered some of the PKI-based security techniques such as authentication, key agreement, and privacy preserving. Their paper explained the authentication mechanism in all generation of mobile communication which gives us insight on how to incorporate authentication in this paper.

Mavoungou et al. [15] discussed the evolution of mobile technology, the vulnerabilities and threats that come with this evolution, which can be used to launch attacks on different network components, such as the access network and the core network. Their paper reviewed the main security issues in the access and core network (vulnerabilities and threats) and provided a classification and categorization of attacks in the mobile network. The paper presented in addition countermeasures and mitigation solutions of these attacks. We explored some of the mitigation mentioned in paper [15] in our current work. Ney et al. [19] designed SeaGlass as a cost-effective approach to surface anomalies in mobile networks such as LTE networks with low false-positive rates. The authors showed that SeaGlass is capable of detecting anomalies across a wide variety of signature classes, potentially caused by actual cell-site simulators. Dabrowski et al. [16] focused on all generations of mobile telecommunication networks 2G and 3G/4G. The paper's main aim was to provide a solution to the oldest practical attack against 3GPP networks, IMSI catching. The authors revealed that the IMSI catching is mostly related to the issue of location privacy. The paper took a deep look at 3GPP networks' relevance to IMSI catching problem with the focus on the identification and authentication procedures. The authors proposed a solution of replacing IMSI with a changing pseudonym. Thus, only the USIM's home network can link to the USIM's identity.

IV. METHODOLOGY

Our proposed solution seeks to protect the IMSI, which can be intercepted in transmission by an attacker during the EPS-AKA authentication procedure. The attacker creates a rogue base station that transmits signals as a real base station does, but the rogue base station transmits signals with more power when it is physically proximate to a User Equipment (UE). The hardware necessary to construct these rogue base stations are available and inexpensive, while the software required to operate them open source and freely available. A User Equipment always connects to the base station with the most powerful signal in an attempt to get service for the first time. Thus, the UE will be forced to connect to the rogue base station because it has more signal strength [6]. Our proposed solution uses a pre-shared key for authenticating a base station in the first hop of the initial registration of a UE as below:

STEP 1: A pre-shared key will be generated by the network operator. With this pre-shared key installed on both the Universal Subscriber Identity Modules and the base stations, a first-hop authentication procedure to authenticate if the base station can be trusted for service will take place anytime the User Equipment wants to

register for the first time before proceeding to send its IMSI to the base station for service. The base station authentication procedure will start with the User Equipment sending the base station a challenge in form of a random number. This random number is encrypted with the network operators pre-shared key (PSK) installed in the Universal Subscriber Identity Modules.

STEP 2: The random number encrypted is sent to the network operator's PSK as challenges created by the User Equipment to identify legitimate base stations from rogue base stations.

STEP 3: The challenge sent by the User Equipment will require the base station to decrypt the random number with its own network operator's pre-shared key (PSK). Then, the base station has to add a number specified by the User Equipment to the random number to generate an answer to the challenge sent by the User Equipment (The number 1 will be used in this case in order to simplify the explanation of our approach).

STEP 4: The base station will then proceed to add 1 to the random number and encrypt the calculated answer to the challenge with its PSK before proceeding to send it back to the User Equipment.

STEP 5: The base station will send back an encrypted answer to the User Equipment (in our scenario, the encrypted number will contain the random number +1).

STEP 6: The User Equipment decrypts this answer. If the answer is correct, the User Equipment will authenticate the base station as trusted and legitimate and will proceed to send its IMSI to the base station for network service.

STEP 7: The User Equipment authenticates the base station is legitimate and can be trusted for connection.

Implementing the proposed pre-shared key model as part of the LTE authentication procedure will give rise to a first-hop eNodeB authentication procedure before proceeding to a second-hop mutual authentication procedure, which is the EPS-AKA Authentication procedure. The first hop eNodeB authentication procedure is a one-way authentication procedure where only the UE authenticates the eNodeB while the second hop mutual authentication procedure (EPS-AKA authentication procedure) is a two-way authentication procedure where both the User Equipment and eNodeB authenticate each other in order for the User Equipment to get service. The home network provider will generate a pre-shared key automatically to be distributed and installed on both the Universal Subscriber Identity Modules and base stations. A single pre-shared key will be used because the memory capacity of a Universal Subscriber Identity Module may not be able to store thousands of keys required to authenticate base stations of a network provider. This single pre-shared key has to be installed on the Universal Subscriber Identity Modules and all the base stations of the network provider. In addition, we propose to change regularly this shared key by automatically updating the Universal Subscriber Identity Modules and the base stations.

V. DISCUSSION

First, we notice that a computer-network authentication protocol that works on the basis of tickets, e.g. Kerberos, can allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. However, such protocol requires continuous availability of a central server. Thus, when the central server is down, new users cannot log in. In addition, a computer-network authentication protocol that works based on tickets have strict time requirements, which means the clocks of the involved hosts must be synchronized within configured limits. The tickets have a time availability period and if the host clock is not synchronized with the central server clock, the authentication will fail.

Second, the main purpose of the proposed pre-shared key authentication procedure between the User Equipment and the base stations is to provide the needed privacy to local users as they connect to the LTE networks. Our proposed approach will protect users in a specific geographical area or country from sending their IMSI to a fake base station. In case that the users leave the country of their home network and they try to roam with a foreign network, they may become vulnerable to fake base stations located in other countries. Indeed, the pre-shared key on the User Equipment is only restricted to its home network. In fact, the roaming service refers to the ability for a user to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when traveling outside the geographical coverage area of the home network, by means of using a visited network.

To face the case where an attacker will try to exploit a security vulnerability related to roaming services in current LTE network (by pretending to be a roaming base station), someone may propose that the home network place a roaming restriction on the User Equipment. This roaming restriction will make sure the User Equipment does not establish connection with any other network or foreign network order than its home network. However, this restriction can be lifted if the user wants it lifted. Concretely, the foreign network will be responsible for contacting the UE's home network for the UE's PSK once it has received the encrypted challenge from a foreign User Equipment. The PSK received by the foreign network will be discarded to make a connection between the User Equipment and the foreign network. Once the User Equipment has successfully registered to the foreign network, it will automatically establish a connection with any of the foreign network's base stations nearest to it without having to request for service from the UE's home

network. In the following, we are detailing our proposed method to lift roaming restriction:

STEP 1: Mobile users must notify the home network of their intention to travel out of service area and request that the roaming restriction be lifted.

STEP 2: The home network will proceed to lift the roaming restriction placed on the User Equipment and will save the information related the user and the visited area.

STEP 3: Once the mobile user is out of the home network's area, the User Equipment requests roaming services by sending an encrypted challenge with the Mobile County Code (MCC) and the Mobile Network Code (MNC) of its home network to the foreign network's base station.

STEP 4: The foreign network's base station will use the MCC and MNC sent to it by the User Equipment to identify the UE's home network. Once identified, the foreign network will contact the UE's home network and request for the PSK to decrypt and solve the challenge.

We suppose the existence of an agreement between the foreign network and the UE's home network to share roaming services as well as authentication information.

STEP 5: Upon receiving the request, the UE's home network will verify if the foreign network is real before proceeding to send the PSK to the foreign network.

STEP 6: Once the foreign network receives the PSK, the base station will proceed to decrypt the challenge with the PSK, solve that challenge before encrypting the answer to this challenge with the PSK. This encrypted answer will then be sent back to the User Equipment.

STEP 7: Upon receiving the encrypted answer, the User Equipment will decrypt it with its PSK. The User Equipment will compare the answer sent with the calculated value that it has. If the two values are equal, the User Equipment will proceed to authenticate the base station before proceeding the using of the foreign network's base station service.

VI. Empirical Evaluation

We evaluated the efficiency of our proposed approach by performing an empirical study and measuring a set of performance metrics such as Throughput, Data Confidentiality, Delay, and Energy Consumption. We used the NetSim simulated environment. NetSim is a leading network simulation software for protocol modeling and simulation. During the evaluation of our approach, NetSim allowed us to analyze its efficiency using a set of metric performance. Throughput is measured by calculating the amount of data transferred per unit time between the User Equipment and the base station. The data confidentiality is the percentage of protecting the confidentiality of data over a total number of the connected equipment and the base stations. Delay is the average time taken by the User Equipment to access the particular message from the base station. The Energy Consumption is calculated as an average energy consumed by the User Equipment in the network to subscribe to a base station.

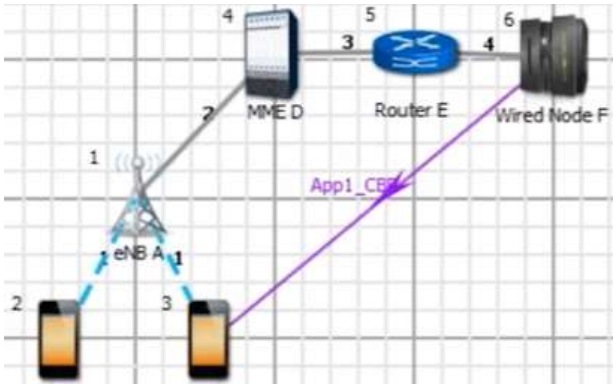

Fig 1: The simulation of LTE networks using NetSim[2]

First, we created a simulated LTE network using NetSim's GUI. Then, we run the Discrete Event Simulation (DES) through the GUI to log packet traces that reports parameters (such as arrival time, queuing time, payload, overhead, error, etc.) for every packet as it flows through the simulated network. In addition, we recorded event traces, which logs every single event in the simulated network with associated information like time-stamp, Event ID, Event Type, etc. Finally, we studied a variety of metrics such as the throughput, delay, data confidentiality, and energy consumption.

TABLE I. Simulation Model Parameters

SIMULATOR PARAMETERS	
Simulators	Parameters
Number of base stations	4
Number of UE	40
Channel Bandwidth (MHz)	5
Transmission Bandwidth Configuration NRB : (1 resource block = 180 kHz in 1 ms TTI)	75
Peak data rate	75 Mbps (20 MHz bandwidth)
Simulation Time	3600 Seconds

Table I summarized the details of empirical study. The results collected from simulated LTE networks are highlighting the following points:

[2] https://www.tetcos.com/netsim-acad.html

1. The Throughput: the average throughput with a simulated LTE network that implements our approach was 0.08 % more than the Throughput with a standard LTE network. This observed increase of throughput is due to the added authentication procedure but it remains acceptable.
2. Delay: we observed that a standard LTE network delivers messages in 1.5 ms, whereas the simulated LTE network that implements our approach delivers the messages in 1.6 ms.
3. Data Confidentiality: the percentage of protecting the confidentiality of data a simulated LTE network that implements our approach is improved by 15%, in comparison with the standard LTE network.
4. Energy Consumption: the average energy consumption of user equipment in a simulated LTE network that implements our approach increases by 0.7% more than the average energy consumption of user equipment with a standard LTE network. Once more, this observed increase is due to the added authentication procedure but it remains acceptable.

Based on this empirical evaluation using the NetSim simulated environment, we can conclude that our proposed approach increases the protection of sensitive data of users while preserving an acceptable performance in comparison with a standard LTE network.

VII. CONCLUSION AND FUTURE WORK

Securing the privacy of telecommunication users is of major importance as major attacks have and can be carried out with the exposure of the IMSI. In this paper, we proposed the deployment of the pre-shared key authentication between the UE and the base station as a first-hop authentication mechanism before the EPS-AKA authentication mechanism is to prevent the exploitation of IMSI in LTE networks. Moreover, we showed how pre-shared key authentication could be deployed globally and not restricted to certain geographical areas. We simulated and compared the performance of our proposed approach using the NetSim simulation environment. From the simulation results, we observed that the data confidentiality of the data transported through the LTE network is improved. Future work includes the specification of a mechanism to overcome other security challenges in LTE networks such as the DNS spoofing attack, which is an active security attack that allows an attacker to perform man-in-the-middle attacks to intercept communications and redirect the victim to a malicious website.

REFERENCES

[1] O.E. Ekene, R. Ruhl and P. Zavarsky, "Enhanced user Security and Privacy Protection in 4G LTE Network," IEEE 40TH Annual Computer Software and Applications Conference, pp. 443-448, 2016.

[2] J.Cao, M, Ma, H.Li, Y.Zhang and Z. Luo, "A Survey On Security Aspects for the LTE and LTE-A Networks," IEEE Communications Surveys & Tutorials Vol. 16. No. 1, pp. 283-302, 2014.

[3] M.A. Abdrabou, A.D.E. Elbayoumy and E.A. El-Wanis, "LTE Authentication Protocol (EPS-AKA) Weakness Solution," IEEE Seventh International Conference on Intelligent Computing and Information Systems, 2015

[4] M. Ogul and S. Baktur, "Practical Attacks on Mobile Cellular Networks and Possible Countermeasures," Future Internet, vol. 5, no. ISSN 1999-5903, pp. 474-489, 30 September 2013.

[5] H.T. Loriya, A. Kulshreshta and D.R. Keraliya, "Enhancement of user Identity Security in Authentication and Key Agreement Protocol for Wireless Communication Network," 2017

[6] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi and J.P. Seirfert "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," 2016. [Online]. Available: https://arxiv.org/pdf/1510.07563, pp. 1-16

[7] S. Barakovic, E. Kurtovic, O. Bozanovic and J.B. Husic, "Security Issues in Wireless Networks: An Overview," 2016

[8] P. Donegan, "Authentication as a Service for LTE Base Stations" Symantec White Paper, pp. 1-10, 2012.

[9] K. Norrman, M. Naslund and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks" 2016. [Online]. Available: https://pdfs.semanticscholar.org/2161/d05e5858f3144948be8242d25a8711b696f9.pdf

[10] E.C. Jimenez, C. Schaefer and M. Naslund, "Encrypting IMSI to Improve Privacy in 5G Networks," 2017.

[11] R.Fortio, "Analyses and implementation of IPsec protocol in the LTE access network," 2016. [Online]. Available: https://fenix.tecnico.ulisboa.pt/downloadFile/844820067123704/Dissertacao_IPsec_LTE_RuiFortio_n68343_V1.0_ResumoAlargado_EN.pdf, pp. 1-10

[12] J.Cichonski and J.Franklin, "LTE Security – How Good Is It?," RSA Conference, 2015

[13] S. Hussein, "Lightweight Security Solutions for LTE/LTE-A Networks," 2014.

[14] M. Ramadan, G. Du, F. Li and C. Xu, "A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems," 2016. [Online]. Available: http://www.mdpi.com/2073-8994/8/9/85/htm

[15] S.Mavoungou, G. Kaddoum, M. Taha and G. Matar, "Survey on Threats and Attacks on Mobile Networks," IEEE Access Special Section On Security In Wireless Communications And Networking, pp. 4543-4572, 2016

[16] A. Dabrowski, N. Pianta and T. Klepp, "IMSI-Catch Me If You Can: IMSI-Catchers-Catchers," 2014.

[17] Cichonski, Jeffrey, Joshua Franklin, and Michael Bartock. LTE architecture overview and security analysis. No. NIST Internal or Interagency Report (NISTIR) 8071 (Draft). National Institute of Standards and Technology, 2016.

[18] Bartock, Michael, Jeffrey Cichonski, and Joshua Franklin. "LTE security—How good is it?." NIST, Gaithersburg, MD, USA, Tech. Rep 3 (2015).

[19] P. Ney, I. Smith, G. Cadamuro, and T. Kohno, "SeaGlass: Enabling City-wide IMSI-Catcher Detection," Privacy Enhancing Technologies (PETS), vol. 2017, no. 3, pp. 39–56, 2017.