AUTOMATED KEY SHARING IN THE AUTHENTICATION PROCESS OF LTE BASE STATIONS

Co-authored by

Student: Babajide Seyi Adegoke

Primary advisor: Fehmi Jafaar

Secondary advisor: Ron Ruhl

Project report
Submitted to the Faculty of Graduate Studies,
Concordia University of Edmonton

In Partial Fulfillment of the
Requirements for the Final
Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton
FACULTY OF GRADUATE STUDIES
Edmonton, Alberta

April 2018

Automated Key Sharing in The Authentication Process of LTE Base Stations

Babajide Seyi Adegoke
Department of Information Systems Security and Assurance Management
Concordia University of Edmonton
Edmonton T5B 4E4, Alberta, Canada
badegoke@student.concordia.ab.ca

Fehmi Jafaar
Department of Information Systems Security and Assurance Management
Concordia University of Edmonton
Edmonton T5B 4E4, Alberta, Canada
fehmi.jafaar@concordia.ab.ca

Ron Ruhl
Department of Information Systems Security and Assurance Management
Concordia University of Edmonton
Edmonton T5B 4E4, Alberta, Canada
ron.ruhl@concordia.ab.ca

***Abstract* – Sensitive information like the International Mobile Subscriber Identity has been a problem on all generations of mobile telecommunication networks, i.e., 2G, 3G and 4G. Many cases of compromising users' privacy in telecom networks have been reported. Cases of rogue base stations capable of tracking, intercepting and collecting the International Mobile Subscriber Identity without the users' knowledge have emerged. The Universal Subscriber Identity Module (USIM) of a mobile phone must reveal its International Mobile Subscriber Identity in plaintext when trying to establish connection with a base station for the first time. The International Mobile Subscriber Identity can be intercepted by attackers and this can amount to a passive or active attack. This paper proposes the use of a pre-shared key in the authentication process of Long Term Evolution (LTE) base stations to local users. This will result in a first hop authentication procedure to verify if the base station is legitimate by the User Equipment, this authentication will protect the International Mobile Subscriber Identity from been sent to a fake base station during the Evolved Packet System Authentication and Key Agreement authentication procedure.**

Keywords – User Equipment, Base station, Pre-shared Key, Authentication, International Mobile Subscriber Identity

I. Introduction

Mobile communication has become an everyday thing and it's playing an irreplaceable role in our lives. It is not only enabling voice communication but it also enables high speed data communication. Millions of smart phones with LTE capabilities are sold every year and are mostly used for browsing the Internet, banking applications and messaging. With the high data throughput in LTE, many subscribers communicate more data than voice which leads to many mobile network operators' data revenues exceeding the voice revenue. Therefore, mobile operators took advantage of their data services and, in addition to being mobile voice carriers, mobile core networks tend to be used as Internet Service Providers (ISP). These investments made by mobile carriers on their IP based infrastructures and services are driven majorly by their subscribers' increasing demand for mobile data communication. Accepting mobile networks as a means for Internet access brings about new IP based vulnerabilities and threats on mobile core networks. Studies on LTE network has shown several vulnerabilities, security threats, security scenarios, security problems and security requirements [4]. One of the vulnerabilities is the IMSI been sent in plaintext by the UE to the base station during the EPS-AKA Authentication Procedure.

The rest of the paper is organized as follows. Section II is the background where the EPS-AKA authentication procedure and its weakness will be discussed. Section III provides an overview of the related works. 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. Finally, Section VI concludes the paper and its future work.

II. Background

A. *EPS-AKA Authentication Procedure*

The authentication mechanism used in LTE network is the Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol. The authentication procedure starts after connection has been established between the User Equipment (UE) and the Mobile Management Entity (MME). The MME sends an ID request to the UE via the Evolved Node B (eNB). The UE will respond by sending its International Mobile Subscriber Identity (IMSI) in plain text to the MME. 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 Authentication Center (AuC) in the HSS will increase the sequence number (SQN) and generate a random number (RAND) and an EPS authentication vector (AV). This AV consists of an expected response (XRES), an authentication token (AUTN), a key (KASME) and a random number (RAND). The AuC of the HSS then sends the AV to the MME, the MME will in turn keep the KASME and XRES but will forward the RAND and the AUTN to the UE. The UE will then use the RAND and the AUTN sent to it by the HSS to calculate its own version of AUTN by using its own key (K) and sequence number, the UE will then compare its calculated AUTN with the AUTN received from the MME in order to authenticate the network. If both AUTNs match, the UE will then compute a response (RES) by making use of cryptographic functions with the key (K) and the RAND. A cipher key (CK) and an integrity key (IK) is also computed. The UE will then send the computed response (RES) back to the MME. The MME will in turn compare the XRES in its possession with the RES sent by the UE. If both are equal, we have a mutual authentication. The UE will use the CK and IK to compute KASME in the same way as HSS. Both UE and MME will then be in possession of the same key KASME. The MME will grant the UE access if both XRES and RES are equal, if not access will be denied [3]. Fig 1 below shows EPS-AKA authentication procedure.

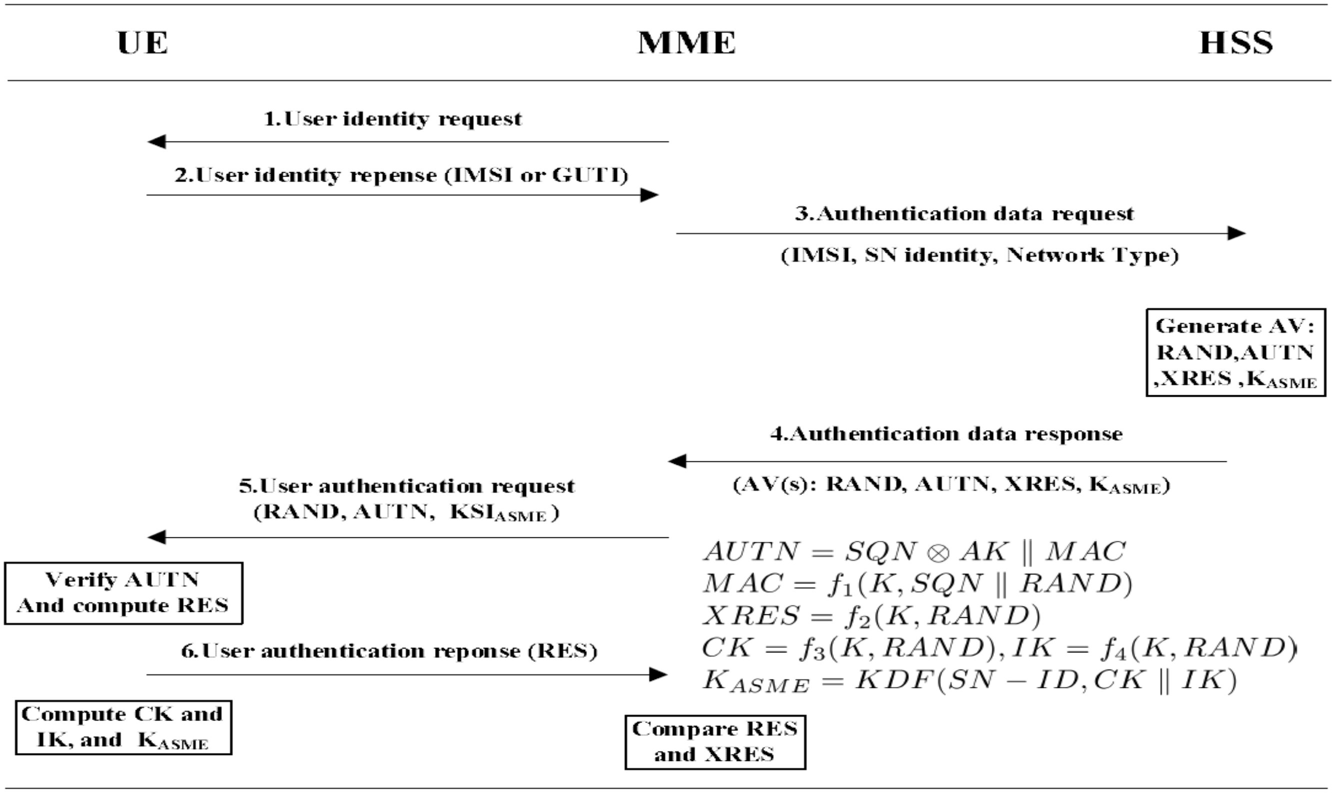
UE
MME
HSS
1.User identity request
2.User identity repense (IMSI or GUTI)
3.Authentication data request
(IMSI, SN identity, Network Type)
Generate AV: RAND,AUTN ,XRES ,K_{ASME}
4.Authentication data response
(AV(s): RAND, AUTN, XRES, K_{ASME})
5.User authentication request (RAND, AUTN, KSI_{ASME})
$AUTN = SQN \otimes AK \parallel MAC$
$MAC = f_1(K, SQN \parallel RAND)$
$XRES = f_2(K, RAND)$
$CK = f_3(K, RAND), IK = f_4(K, RAND)$
$K_{ASME} = KDF(SN-ID, CK \parallel IK)$
Verify AUTN And compute RES
6.User authentication reponse (RES)
Compute CK and IK, and K_{ASME}
Compare RES and XRES

Fig 1: EPS-AKA Authentication Procedure [13]

B. EPS-AKA Authentication Weakness

The Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol improves the security and privacy of the LTE network but it still has its weaknesses and vulnerabilities. The main weakness 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 weakness is a breach of confidentiality code (Disclosure of the user identity) of the information security CIA TRIAD. This happens when a UE registers to the network for the first time, the UE must send its IMSI in plaintext 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 include the subscriber information, location information, and conversation information. An attacker can hide the real UE with this information and can launch attacks on the network [1][4]. Fig 2 below shows the disclosure of a user identity:

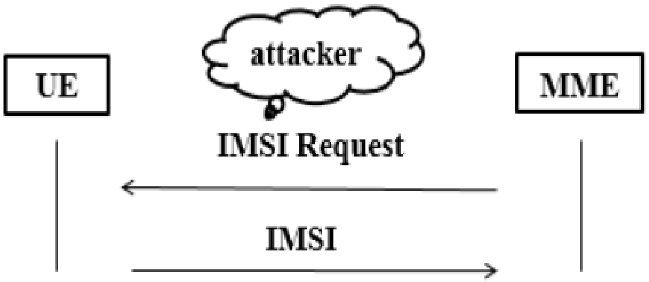

Fig 2: User Identity Disclosure [4]

The weakness described above can easily be exploited by an attacker with a rogue base station. 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. This results in the attacker been able to retrieve the IMSI of the UE which can lead to passive and active attacks [6] [7].

This paper proposes the use of a pre-shared key for mutual authentication in the initial authentication process between a UE and LTE base stations. This mutual authentication will aim to authenticate the base station to the UE as legitimate and trusted. This will in turn protect the IMSI been sent during the initial authentication and registration processes of a UE not to get sent to a malicious base station. This paper will be adopting the shared secret authentication model in [8] for mutual authentication between the UE and the local base stations. The scope of this paper is limited to just users and base stations of a network in a specific area or geographical area. This paper is focused on the UE and the eNodeB of the 4G LTE network architecture as shown in Fig 3 below:

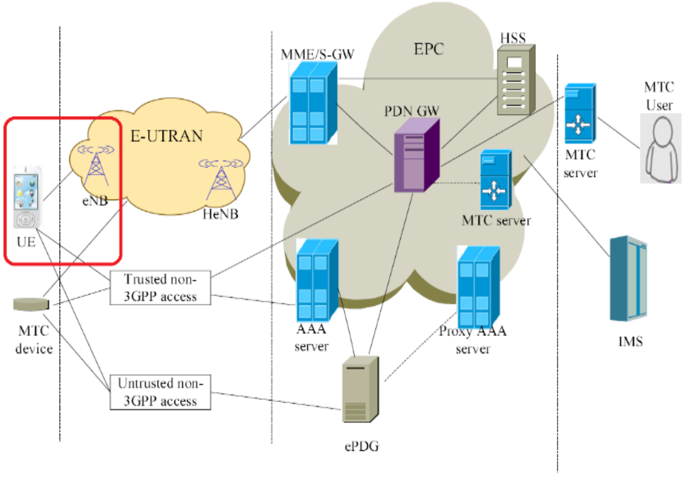

Fig 3: LTE Network architecture [2]

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 was presented, some vulnerabilities in the security functionalities were listed and how these vulnerabilities can be exploited to compromise the network. A survey on the existing solutions to these problems was also carried out. From the survey, the EPS-AKA authentication mechanism, which was able to improve the security in the GSM and UMTS networks by providing mutual authentication and integrity protection, was found vulnerable to several kinds of passive and active attacks. In this 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 paper [2].

Shaik et al in [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. The issues discovered by the authors allowed attackers to mount a rogue base station to track LTE subscribers and deny them services. An experiment was carried out to show active attacks in a faraday cage in order not to interfere with other phone users. They also made sure services were not interrupted to normal users while carrying out passive attacks. The rogue base station attack mentioned in paper [6] is what this paper is seeking to protect LTE users against.

Donegan in [8] discussed security implications in the LTE architecture and the implementation of IPsec Protocol in the LTE network. The author also discussed the adoption of IPsec in LTE to secure the LTE network. A detailed discussion about authentication of eNodeBs using PKI and pre-shared keys was done in the paper. The paper proposed the use of a “shared secret” authentication model for authentication of base stations. This paper will be adopting and basing its proposed solution on the shared secret authentication model mentioned in [8].

Fortio in [11] discussed the security vulnerabilities present in the LTE access network. The paper evaluated the introduction of IPsec in the LTE access network. IPsec in LTE access network was studied and analyzed the impact in the LTE architecture and performance. One of the impact of IPsec in the LTE access network is the eNodeB certificate-based authentication which uses digital signature with asymmetric keys and requires implementations of a Public Key Infrastructure (PKI) for SecGW and eNodeB public keys certificate issuing. The paper concluded after laboratory tests that IPsec in LTE had marginal impact on network performance, but considered quite acceptable taking into account the added value in network security and in the carried services. In this paper, we are seeking to authenticate the eNodeB as a proposed solution to rogue eNodeB attacks and paper [11] gives an insight on authentication of eNodeB.

Norrman et al in [9] studied various cases of users’ privacy attacks in telecom networks. The 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. This method requires a pseudonym to be derived locally at the user equipment and the home network without affecting existing Universal Subscriber Identity Modules (USIMs). This method presented protects the IMSI from passive and active IMSI-catchers as well as honest but curious serving networks. The authors revealed that the proposed method has its limitation, the method does not completely protect the IMSI from curious serving networks because there are other ways IMSI could be obtained by serving networks but it does protect IMSI against passive and active attackers. The authors also noted that some regulations and laws would render the proposed method illegal in some jurisdictions. In this paper, we are seeking to propose a new approach from the one in paper [9] to tackle the problem of IMSI catchers in LTE networks.

Cichonski and Franklin in [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. In this paper, we explore some of the suggestions made in paper [12] on how to mitigate rogue base station attacks.

Jimenez et al in [10] discussed the privacy issues related to the disclosure of the IMSI in the Radio Interface while it is being transmitted to establish connection. The main goal of their paper was to efficiently protect the IMSI in the Radio Interface, while transmitting it to those network nodes that need it for operation. Their paper proposed a solution for enhancing the privacy of IMSI in 5G systems. The proposed solution was derived based on preliminary analysis of related works, the authors decided to suggest and implement 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 in [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 more on authentication in all generation of mobile communication which gives insight on how to incorporate authentication in this paper.

Mavoungou et al in [15] discussed the evolution of mobile technology, the vulnerabilities and threats that comes 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 mobile network. The paper also analyzed major attacks on 4G mobile networks and corresponding countermeasures and mitigation solutions. We explored some of the mitigations mentioned in paper [15] in this paper.

Dabrowski et al in [16] focused on all generations of mobile telecommunication networks 2G and 3G/4G. The paper took a brief look at the background and description of IMSI catching but focused mainly on the act of gathering IMSI numbers from airwaves (passive or active). The paper's main aim was to provide a solution to the oldest practical attack against 3GPP networks, IMSI catching. The paper revealed 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 main focus on the identification and authentication procedures. The paper proposed a solution of replacing IMSI with a changing pseudonym that only the USIM's home network can link to the USIM's identity. Their paper provided more information for this paper about IMSI catching in all generations of mobile telecommunications.

IV. Methodology

The methodology in this paper 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 at the same time the real base station does, but the rogue base station transmits signals with more power. A User Equipment (UE) always connects to the base station with the most powerful signal in an attempt to get service for the first time, the UE will be forced to connect to the rogue base station because it has more signal strength thereby prompting the UE to transmit its IMSI in plain text to the rogue base station for authentication. This results in the attacker been able to retrieve the IMSI of the UE [6].

The methodology in this paper uses a pre-shared key for authenticating a base station in the first hop of the initial registration of a UE. The purpose of using a pre-shared key is to provide authentication of the base station by the UE. A pre-shared key is a shared secret agreed on by two parties and is shared between them to communicate via a secure channel. A pre-shared key is used for authentication and during security negotiation between two parties, information is encrypted before transmission using the shared key, and decrypted on the receiving end using the same key. If the receiver can decrypt the information, identities are considered authenticated. Below is a diagram and a step-by-step description of how the research objective will be achieved using pre-shared key

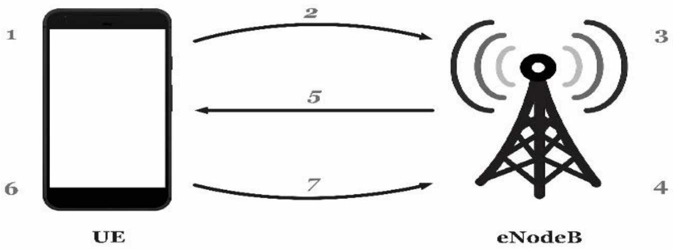

Fig 4: Overview of the Pre-shared key model deployment in base station authentication

STEP 1: A pre-shared key will be generated by the network operator; this pre-shared key will be installed in the USIM and into the LTE base stations using an automated method. With this pre-shared key installed on both the USIM 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 UE 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 UE sending the base station a challenge in form of a random number. This random number is encrypted with the network operator's pre-shared key (PSK) installed in the USIM.

STEP 2: Random number Encrypted with the network operator's PSK

STEP 3: The base station will accept the challenge sent by the UE. This challenge sent by the UE will require the base station to decrypt the random number with its own network operator's pre-shared key (PSK) and then adding any number specified by the UE to the random number to generate an answer to the challenge sent by the UE (The number 1 will be used in this case).

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 UE.

STEP 5: Encrypted answer been sent back to the UE (Random number +1).

STEP 6: This answer will in turn be decrypted by the UE, if the answer is right, the UE 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 UE authenticates the base station is legitimate and can be trusted for connection.

V. Discussion

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. A pre-shared key will be generated automatically by the home network provider. The pre-shared key is distributed and installed on both the USIM and base station. A single pre-shared key will be used because the memory capacity of a USIM may not be able to store thousands of keys required to authenticate base stations of a network provider. This single pre-shared key will be installed on the USIM and all the base stations of the network provider. This shared key will also be changed regularly by automatically updating the USIM and the base stations. This regular key change is done for security purposes.

On registering the UE to the home network and for the UE to get service, it initiates a first hop eNodeB authentication procedure to verify if the base station it's trying to connect to is legitimate before sending its IMSI to the base station for a second hop mutual 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 UE and eNodeB authenticates each other in order for the UE to get service. A step by step explanation of the proposed authentication procedure is done below:

1. The UE sends a RRC connection request (Radio Resource Control) to the MME.

2. The MME will respond to the UE by sending a user identity request to the UE.

3. Once the User Equipment (UE) receives the user identity request, it initiates a first hop eNodeB authentication procedure by creating a challenge (Adding a specific number to the random number) by selecting a random number and encrypting it with the network provider's generated pre-shared key installed in its USIM (E_{PSK} (RAND)). The UE sends this encrypted random number to the Evolved Node B (eNodeB) along with the challenge for it to add a specific number to the random number.

4. The eNodeB will accept this challenge by decrypting the random number with the network provider's generated pre-shared key installed into it (D_{PSK} (RAND)). The eNodeB will proceed to solve the challenge by adding the specific number to the random number. The eNodeB will proceed to encrypt the answer to this challenge with its pre-shared key (E_{PSK} (RAND + 1)) and send it back to the UE.

5. The UE will in turn decrypt the answer with its pre-shared key (D_{PSK} (RAND + 1)). Once decrypted, the UE will carry out a calculation to arrive at the random number it sent to the eNodeB. The UE will compare the answer it arrived at with the initial random number it sent to the eNodeB (RAND + 1 – 1 = RAND). If the answer calculated by the UE is the same as the random number, the UE authenticates the eNodeB as legitimate and proceed to initiate the second hop mutual authentication procedure.

6. To start the second hop mutual authentication procedure, the UE will encrypt the IMSI with its PSK and send it to the eNodeB. The eNodeB will in turn decrypt the IMSI with its own PSK before sending it to the MME in plaintext in order to obtain service.

In figure 5, we present a diagram of the proposed authentication procedure:

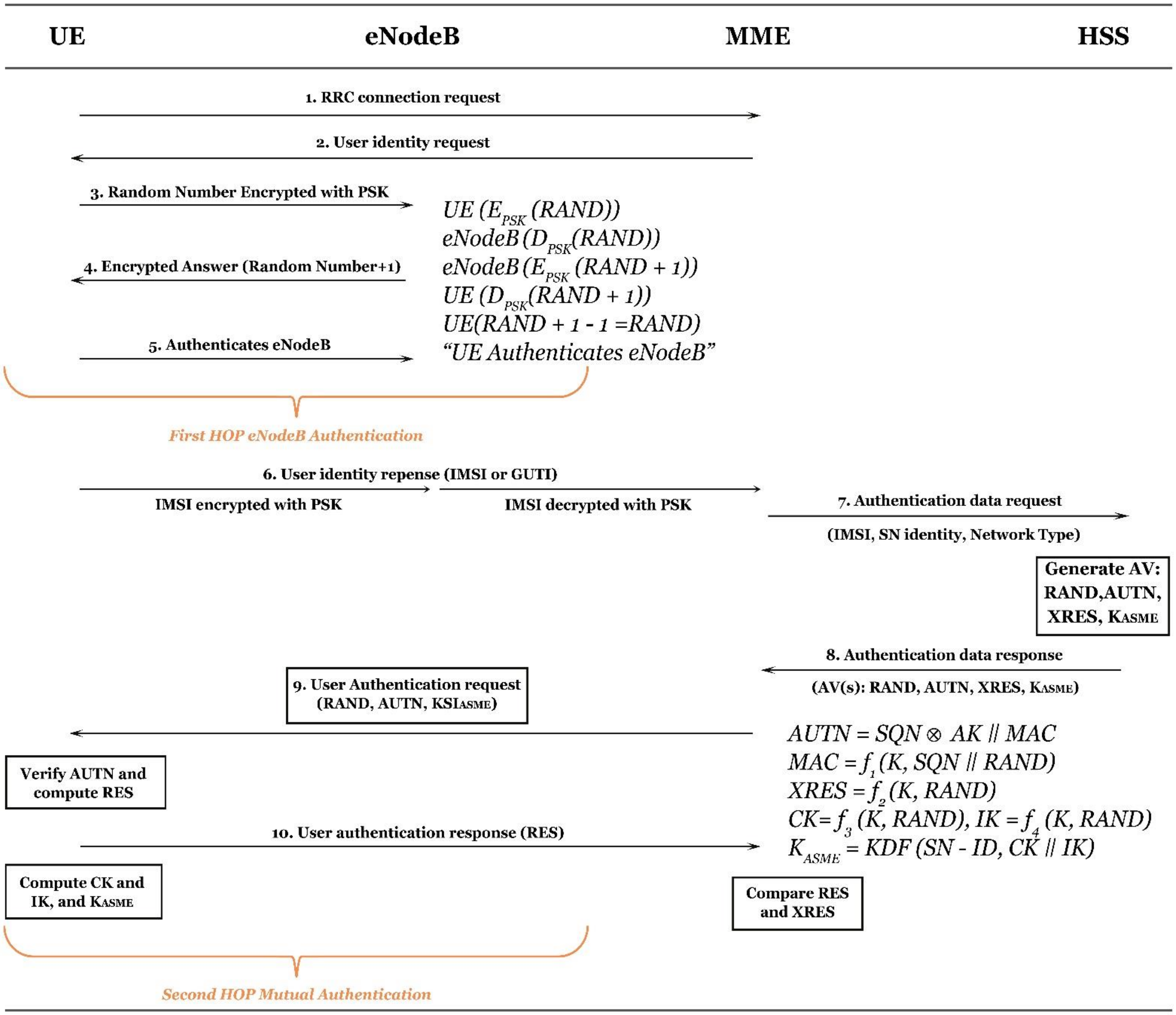
UE
eNodeB
MME
HSS
1. RRC connection request
2. User identity request
3. Random Number Encrypted with PSK
UE (E_PSK (RAND))
eNodeB (D_PSK(RAND))
4. Encrypted Answer (Random Number+1)
eNodeB (E_PSK (RAND + 1))
UE (D_PSK(RAND + 1))
UE(RAND + 1 - 1 =RAND)
5. Authenticates eNodeB
"UE Authenticates eNodeB"
First HOP eNodeB Authentication
6. User identity repense (IMSI or GUTI)
IMSI encrypted with PSK
IMSI decrypted with PSK
7. Authentication data request
(IMSI, SN identity, Network Type)
Generate AV: RAND,AUTN, XRES, KASME
8. Authentication data response
(AV(s): RAND, AUTN, XRES, KASME)
9. User Authentication request (RAND, AUTN, KSIASME)
AUTN = SQN ⊗ AK || MAC
MAC = f_1 (K, SQN || RAND)
XRES = f_2 (K, RAND)
CK= f_3 (K, RAND), IK = f_4 (K, RAND)
K_ASME = KDF (SN - ID, CK || IK)
Verify AUTN and compute RES
10. User authentication response (RES)
Compute CK and IK, and KASME
Compare RES and XRES
Second HOP Mutual Authentication

Fig 5: Proposed Authentication Procedure

In step 6 of the above implementation, encrypting the IMSI with the UE's PSK before sending it to the eNodeB will prevent any form of passive attack. If the attacker is unable to pretend as a fake base station in order to capture the IMSI, the attacker can decide to listen to the traffic between the UE and the eNodeB during the second hop mutual authentication in order to capture the IMSI if it's been sent in plaintext. Once the encrypted IMSI is safely through to the eNodeB, it is decrypted with the eNodeB's PSK before been sent to the MME. Sending the decrypted IMSI the rest of the way is because the rest of the LTE network is a trusted area for the IMSI to be transmitted in plaintext.

The main purpose of the proposed pre-shared key authentication procedure between the UE and the base stations is to provide the needed privacy to local users as they connect to the LTE networks. This proposal will only protect users in a specific geographical area or country from sending their IMSI to a fake base station, the moment the users leave the country of their home network and they try to roam with a foreign network, they become vulnerable to a fake base station because the pre-shared key on the UE is only restricted to its home network. In the case where an attacker will try to exploit this vulnerability by pretending to be a roaming base station, this paper proposes that the home network place a roaming restriction on the UE. This roaming restriction will make sure the UE doesn't 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. A proposed method on how this restriction can be lifted and the UE will roam successfully to a foreign network is explained below followed by a sequence diagram showing this method:

A. Proposed Method To Lift Roaming Restriction

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.

2. The home network will proceed to lift the roaming restriction placed on the UE.

3. Once the mobile user is out of the home network's service area, the UE will request to roam by sending an encrypted challenge with the Mobile Country Code (MCC) and the Mobile Network Code (MNC) of its home network to the foreign network's base station.

4. For the foreign network's base station to be able to decrypt and solve the challenge sent to it by the UE, it'll require the PSK of the UE's home network to do this. The foreign network's base station will use the MCC and MNC sent to it by the UE 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.

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.

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

7. Upon receiving the encrypted answer, the UE will decrypt this answer with its PSK. The UE will compare the answer sent with the calculated value it has, if they are the same, the UE will proceed to authenticate the base station before proceeding to roam to the foreign network's base station for service. In Figure 6, we present this proposed method using a sequence diagram.

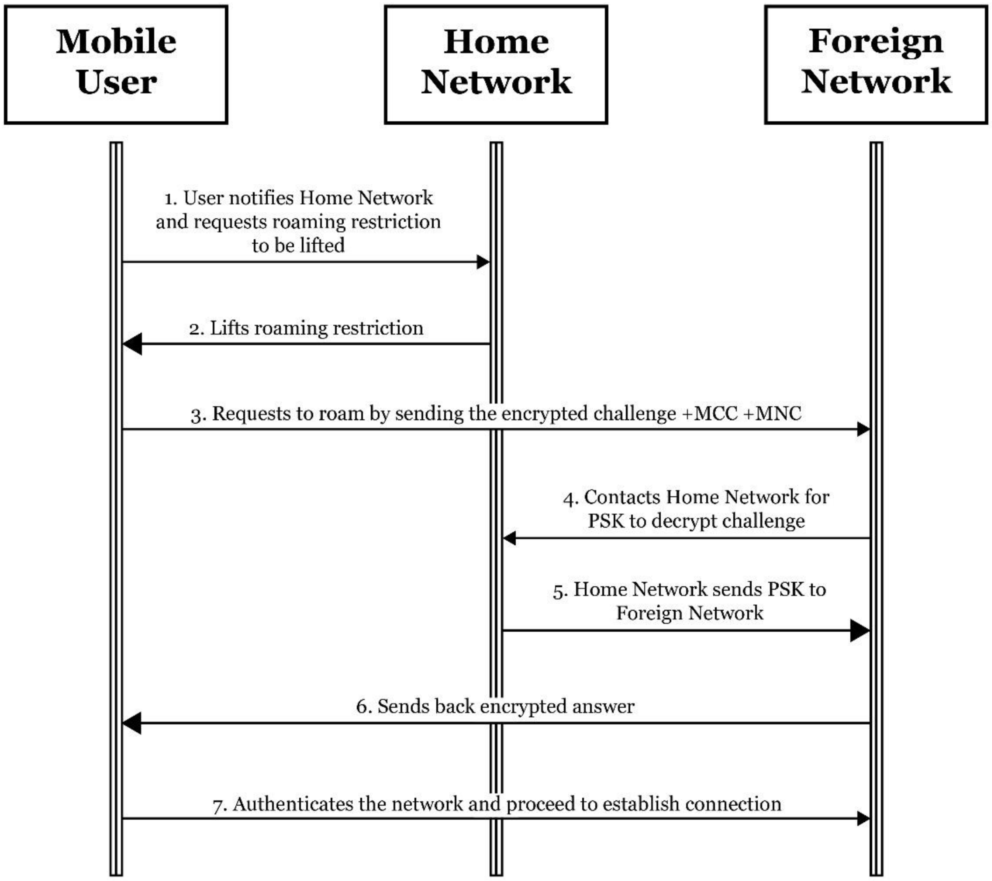
Mobile User
Home Network
Foreign Network
1. User notifies Home Network and requests roaming restriction to be lifted
2. Lifts roaming restriction
3. Requests to roam by sending the encrypted challenge +MCC +MNC
4. Contacts Home Network for PSK to decrypt challenge
5. Home Network sends PSK to Foreign Network
6. Sends back encrypted answer
7. Authenticates the network and proceed to establish connection

Fig 6: A Sequence Diagram Showing the Proposed Method

The method above will ensure that the UE successfully roam to a legitimate foreign network. This method doesn't require the UE to have the PSK of the foreign network it's trying to connect to, 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, the UE's MCC and MNC. The PSK received by the foreign network will be discarded immediately connection has been established between the UE and the foreign network. Once the UE has successfully register to the foreign network, the UE will always automatically establish connection with any of the foreign network's base station nearest to it without having to request for service.

VI. 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. The IMSI been a delicate information that an attacker can use to monitor users, impersonate legitimate users and thereby carrying out attacks for unauthorized usage of network. 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, as it ensures the security and privacy of telecommunication users without negatively affecting the functionality, Quality of Service (QoS), and performance of the network. More work need to be done to figure out how the pre-shared key authentication can be deployed globally and not restricted to certain geographical areas. The proposed pre-shared key authentication also needs to be evaluated to validate the applicability to the LTE network in the future.

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. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1095875/FULLTEXT01.pdf

[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. [Online]. Available: https://www.researchgate.net/publication/279263961

[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. [Online]. Available: https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf