Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

11th International Conference
on Electrical Engineering
ICEENG 2018

Design and Simulation of a New Intelligent Authentication for Handover over 4G (LTE) Mobile Communication Network

Mahmoud El Omda[*], Mohamed Helmy Megahed** and Mohamed Hassan Abdel Azeem*

Abstract

LTE has become the dominant mobile communication network as it provides higher data rate, higher level of security and more applicable services. The handover is a critical process as it needs to be rapid and accurate process. In the handover over the Long Term Evolution (LTE) standard security protocol, the key management takes place between the source eNodeB and target eNodeB under the Mobility Management Entity (MME) via X2 interface. 3GPP has specified some security mechanisms to ensure the safety of handover key management, but still there exist some vulnerabilities compromising the security of the handover process, such as desynchronization attack. This paper proposed a new Lightweight Intelligent authentication protocol, which solves the desynchronization attack, solves Man in The Middle Attack, and achieves shorter setup time. This protocol solves the desynchronization attack and Man in The Middle Attack by adding a Certificate Authority (CA), which generates a certificate for each eNB of the LTE network. In addition, the proposed protocol achieves shorter setup time by applying a parallel key management and handover instead of sequential key management and handover with each eNB. The proposed protocol assumes a new method of authentication of the User Equipment (UE) by using a Key Management Unit (KMU).The proposed protocol is securely analyzed. In addition, measuring the performance analysis in terms of the communication overhead, computations overhead and setup time by using Eclipse Real Time Operating System program. Finally, the proposed protocol is compared with the Standard protocol and MRN related work.

Keywords

LTE Handover, Key Management, Desynchronization Attack, Man in the Middle Attack, KMU.

* Dept. of Comm, Arab Academy for Science and Technology and Maritime Transport University, Cairo, Egypt.

** Dept. of Comm, Canadian International College, Cairo, Egypt.

1. Introduction

LTE is the evolution of the 3G (UMTS) mobile communication network [1, 2], which provides higher performance for higher data rates, lower delay, and higher level of security. LTE is widely used in most regions of the world especially America and Europe and after few years, it will be the most widely used mobile communication network all over the world. The LTE has been designed to be all-IP architecture. The handover process is a critical process as it needs to take place accurately and rapidly. This process needs a Lightweight Intelligent Authentication during handover.

Evolved Packet System (EPS) is divided into two parts; the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC). The E-UTRAN is responsible for radio communications. The EPC is responsible for providing services, deriving key management, and containing subscribers' information.

LTE supports two kinds of Mobility Management Entity (MME) handovers, one is inter-MME and the other is intra-MME handover. The handover over the LTE was being achieved sequentially by achieving the authentication with the next hop only. This type of handover was suffering from higher setup time to create the session key between eNB and UE and it has some vulnerabilities such as Man in The Middle Attack and Desynchronization attack.

This paper presented a new concept of handover process, which achieves the handover process in parallel depends on defining the route of the UE (Established Known Route) before accessing to the mobile network, then deriving all session keys with all eNBs, which will provide the handover between all eNBs and the UE. This protocol enhanced the performance of the handover process as it achieved shorter setup time, higher security level and higher performance in terms of computation overhead, and storage overhead.

In this paper, the certificate authority will provide each entity such as eNB and secure UEs with a certificate. This certificate authority will change the certificate for each entity periodically according to certain policy. This paper introduced the usage of Key Management Unit (KMU) in the UE, which will support the UE to verify all certificates of eNBs and to solve desynchronization attack [3], in addition to derive all session keys with all used eNBS before performing the handover process. Also, this paper introduced the usage of CA, which generates all certificates for all eNBS to solve the Man In The Middle attack [4].

A. CONTRIBUTIONS:

1) Designing a New Intelligent Authentication protocol for handover process with shorter setup time by achieving authentication and handover in parallel process between UE and all eNBs in the route of UE.

2) Designing an authentication protocol, which solves Man in The Middle Attack and desynchronization attack by using the CA which distributes certificates to all eNBs and secure UEs.

3) Use Key Management Unit (KMU) to authenticate the UE with the Core Network and to verify the certificate for each entity.

B. OUTLINE THE PAPER:

Section 2 presents related work. Section 3 describes the network model. Section 4 describes the threat model. Section 5 describes proposed protocol. Section 6 describes the security analysis. Section 7 describes performance analysis and simulation results. Section 8 presents comparison with AKA-EPS and other works. Section 9 concludes the paper.

2. Related work

Recently, there were many researches to enhance the security level of the handover process over the LTE [5], these researches mentioned many ways to perform secure handover. The 3GPP standard protocol [6] achieved the authentication while handover between source and target eNB. The author in [7] achieved authentication based on key generation center to derive all session keys, but this method was being executed sequentially, which means higher delay and communication overhead. The author in [8] used public key infrastructure, but this method affected the UE batteries as it needs higher computations. The author in [9] used a hybrid authentication, but this method is not effective because of long setup time of public key infrastructure as it executed handover sequentially. Also, in [10] the concept of Mobile Relay network (MRN) is mentioned, but it still suffers from long setup time as it executed handover sequentially and it neglected the authentication of UE.

3. Network Model

The network model is called Evolved Packet System, which is consisted of two main parts as shown in Figure.1. The first part is Evolved Universal Terrestrial Radio Network (E-UTRAN), which is responsible for radio interfacing between UE and core network. This part is consisted of the User Equipment (UE), eNodeB (eNB) and Home eNodeB (HeNB). While the second part is the Evolved Packet Core (EPC), which is responsible for providing the UE with services. The EPC is consisted of the Services Gateway (S-GW), Packet Gateway (P-GW), Home Network and the Mobility Management Entity (MME). This paper is focusing on the MME function, which is in charge of controlling eNBS and its main propose is to control the Handover of UE between the eNBS. Also, this paper is focusing on Handover process.

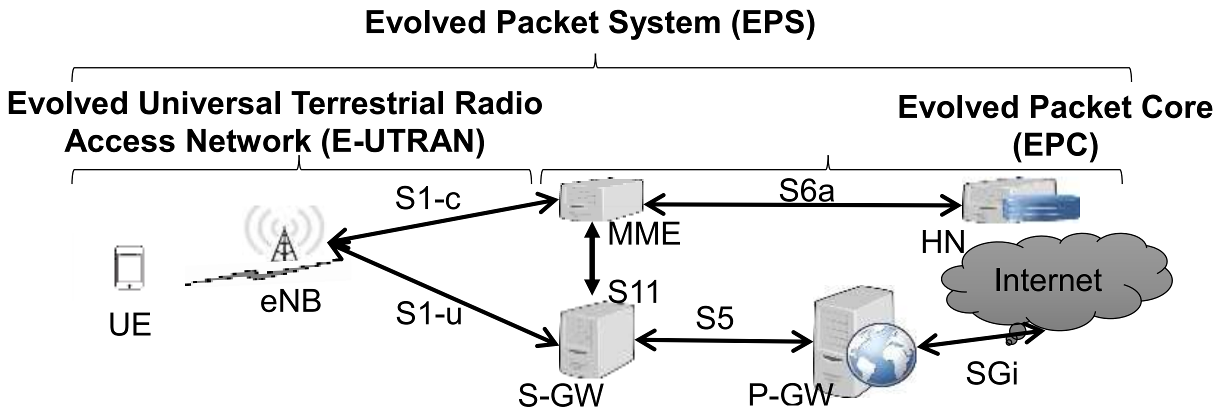
Evolved Packet System (EPS)
Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
Evolved Packet Core (EPC)
UE
eNB
S1-c
S1-u
MME
S11
S-GW
S6a
HN
S5
P-GW
Internet
SGi

Fig.1. LTE Network Model

There are two types of handover process, Inter and Intra-Handover. The Intra-Handover takes place between the source eNB and the target eNB under only one MME responsibility. While the Inter-Handover takes place between the source eNB and a target eNB unde different MMES. Figure.2 shows the types of the radio access network, which can be used to interface between the UE and core network. These radio access networks may be E-UTRAN, Trusted non 3GPP access or untrusted non 3GPP access. Each type of these radio access networks has its own handover authentication protocol.

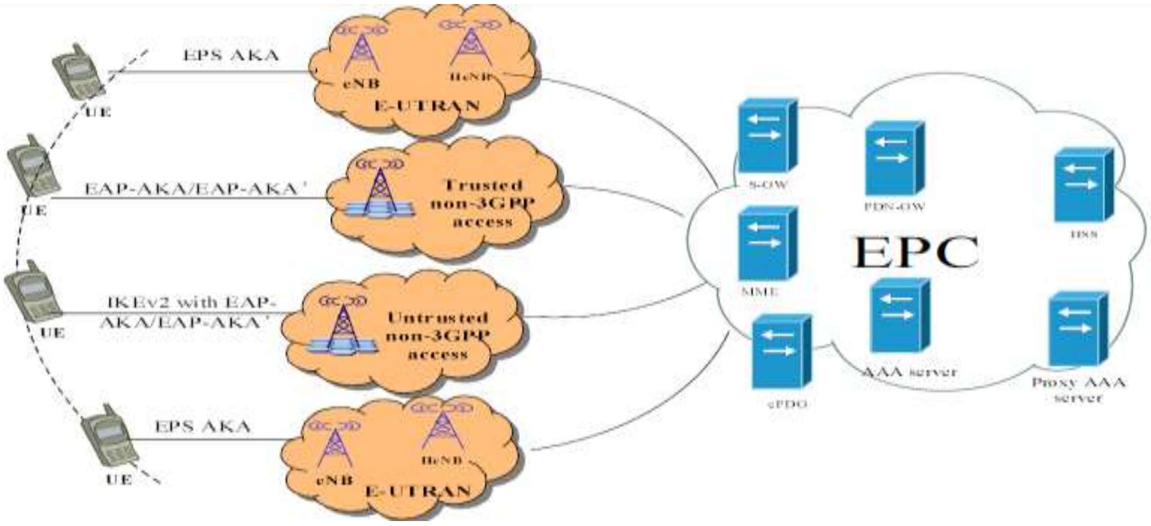

Fig.2. Radio Access Networks

The Handover authentication protocol for Intra-Handover is shown in Figure.3.

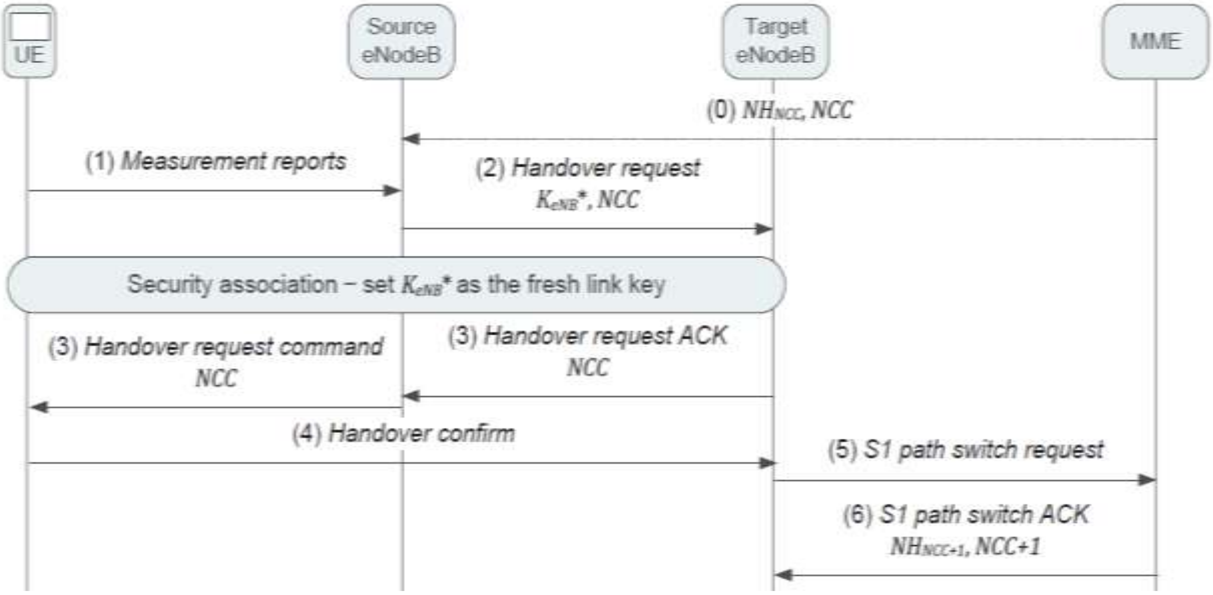
UE
Source eNodeB
Target eNodeB
MME
(0) NH_{NCC}, NCC
(1) Measurement reports
(2) Handover request K_{eNB}*, NCC
Security association – set K_{eNB}* as the fresh link key
(3) Handover request command NCC
(3) Handover request ACK NCC
(4) Handover confirm
(5) S1 path switch request
(6) S1 path switch ACK NH_{NCC+1}, NCC+1

Fig.3. LTE Handover Authentication

Table 1. Standard Protocol for Handover over LTE

Standard Handover Authentication over LTE protocol
The MME provides the Source eNB with the current and next hop network chain of commands before starting the handover process to be ready for communicating with the UE. The current chaining counter (NCC) is used to derive the current session key, while the next hop network chaining counter (NH_{NCC}) is used to derive the next session key to be used in the target eNB. **M1: UE ⟶ eNBS: (Measurement Report)** The UE sends m1 to the eNBS, which is measurement report to announce its location and its direction. **M2: eNBS ⟶ eNBT: (KeNB*, NCC)** The eNBS sends m2 to the eNBT, which is the network chaining counter and the derived session key. This derived session key is derived by the eNBS by using the network chaining counter, which is sent from the MME. **M3: eNBT ⟶ eNBS: (Handover Request ACK)** The eNBT sends m3 to the eNBS, which a handover request acknowledgment.

M4: eNBS → UE: (Handover Request Command, NCC)

The eNBS sends m4 to the UE, which is a handover request command and network chaining counter to derive the new session key.

M5: UE → eNBT: (Handover Confirm)

After deriving the session key and all cryptographic functions, the UE sends a handover confirmation message to the eNBT.

M6: eNBT → MME: (path switch Request)

The eNBT sends m6 to the MME to request a path switch and to request the current and next hop network chain of command.

M7: MME → eNBT: (NHNCC, NCC)

The MME sends m7 to the eNBT, which is the network chaining counter and next hop network chaining counter to use it to derive the next session key.

4. Threat Model

A. Man in The Middle Attack

A rogue base station (i.e., eNodeB) is a mobile base station that impersonate a legitimate base station. An adversary can control a rogue base station either by compromising a commercial eNodeB or by deploying a personal eNodeB through physical, host, and network protocol vulnerabilities. By physically penetrating an eNodeB, an adversary can access its stored cryptographic materials.

B. Desynchronization attack

The goal of this rogue base station is to disrupt updating of the NCC value, leaving the targeted eNBs desynchronized and future session keys vulnerable to compromise.

C. False UE

Any UE does not have a KMU, that is responsible of verifying certificates and generating session keys, will not access the secure network and is considered as non-secure UE.

5. Proposed Protocol

The proposed protocol proposed a new concept of handover authentication, which is used by defining the route of UE before starting the handover process. Handover Process is achieved in parallel with all eNBs, which achieves a Fast Intelligent Authentication for Handover over LTE network.

A. Proposed protocol assumptions:

1) A Certificate Authority (CA) is added to the HSS to generate and verify certificates for each entity.
2) A Key Management Unit (KMU) is added to the UE to be in charge of verifying certificates and generating the session keys.

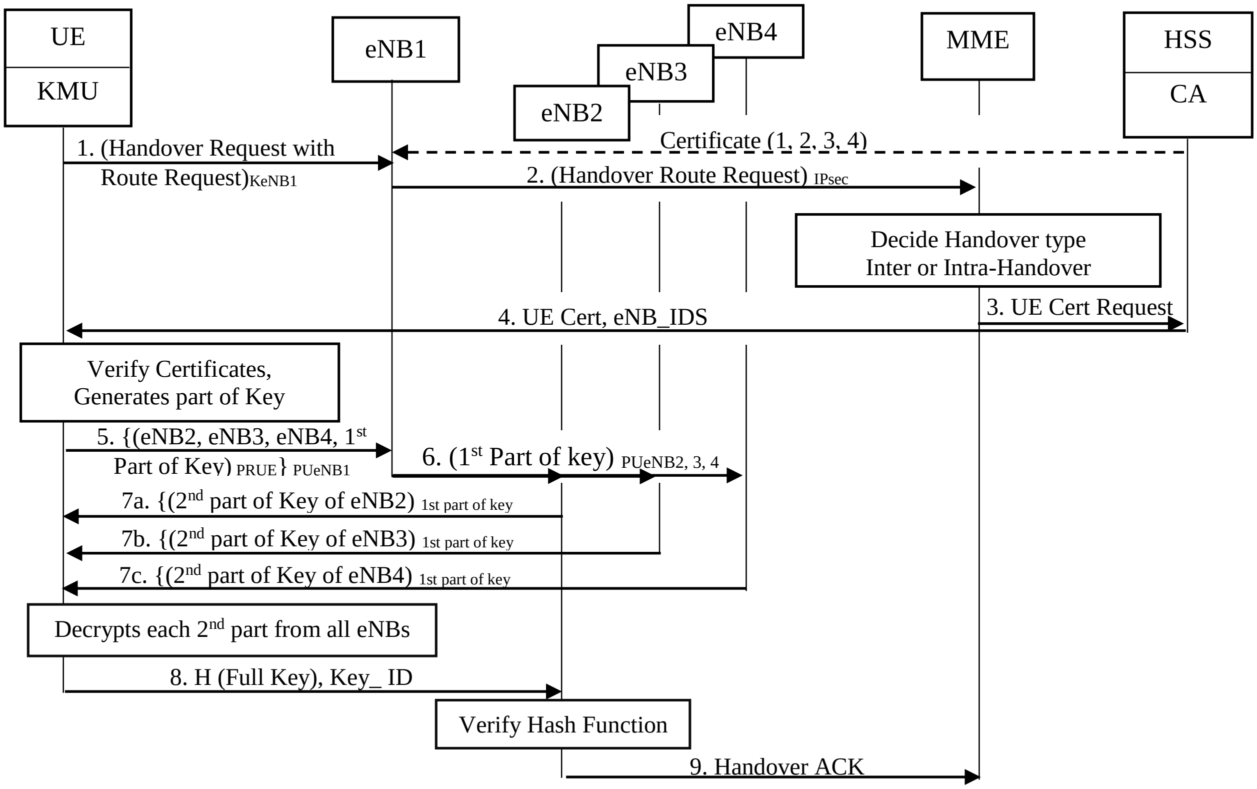
UE
KMU
eNB1
eNB4
eNB3
eNB2
MME
HSS
CA
Certificate (1, 2, 3, 4)
1. (Handover Request with Route Request)KeNB1
2. (Handover Route Request) IPsec
Decide Handover type Inter or Intra-Handover
3. UE Cert Request
4. UE Cert, eNB_IDS
Verify Certificates, Generates part of Key
5. {(eNB2, eNB3, eNB4, 1st Part of Key) PRUE} PUeNB1
6. (1st Part of key) PUeNB2, 3, 4
7a. {(2nd part of Key of eNB2) 1st part of key
7b. {(2nd part of Key of eNB3) 1st part of key
7c. {(2nd part of Key of eNB4) 1st part of key
Decrypts each 2nd part from all eNBs
8. H (Full Key), Key_ ID
Verify Hash Function
9. Handover ACK

Fig.4. Proposed Protocol

Table 2. Proposed Protocol

Intelligent Authentication for Handover
M1: UE ⟶ eNBS : (Handover Request)$_{\mathbf{KeNBS}}$ The UE sends a handover request to the source eNB and it defines its route (source-destination locations). This is message M1 and it is encrypted by using the session key between UE and eNB, which is derived from EPS-AKA between the UE and eNB. **M2: eNBS ⟶ MME: (Handover Route Request)$_{\mathbf{IPsec}}$** After the eNBS receives M1, the eNBS sends m2 to the MME. This message is a handover route request to decide the type of handover (Inter or Intra Handover).

M3: MME → HSS: (UE Certificate Request)

After the MME receives m2, it decides the type of handover. Then it sends m3 to the HSS. The HSS will add Certificate Authority (CA) to generate and verify all entities' certificates. M3 is a UE certificate request.

M4: HSS → UE: (UE Certificate, eNB-IDs)

The HSS sends M4 to the UE. This message contains the user equipment certificate, which is the public and private key of the UE, the identities of all eNBs that UE will perform handover with and the validity time of this certificate.

M5: UE → eNBS: {(eNB2, 3, 4_IDs, 1st Part of Key)$_{PRUE}$}$_{PUeNB1}$

After verifying the certificate by the KMU, The UE sends M5 message to the eNB 1. This message contains the 1st part of the session key, which will be used with the all target eNBs. This message is double encrypted message as it is encrypted by the private key of the UE and it is encrypted again by the public key of each eNB in the route.

M6: eNB1 → eNB2, 3, 4: (1st part of key)$_{PU2,\,3,\,4}$

After decrypting the m5, each eNB again sends M6 to the eNB2, 3, 4, which is encrypted by using the public key of each eNB.

M7: eNB2, 3, 4 → UE: (2nd Part of Key)$_{1st\ part\ of\ key}$

After decrypting m6, The eNB2, 3, 4 send m7 to the UE, which is the 2nd part of the session. This messages is encrypted by using the 1st part of the session key using AES-256 algorithm.

M8: UE → eNBT: (H(Full Key, Key_ID))

After decrypting the 2nd part of the key, the UE sends m8 to the eNB2, 3, 4, which is the hash function of the full key and the key_ID.

M9: eNBT → MME: (Handover ACK)

After verifying the hash function of m8, which is handover confirm. The MME sends m9 to the MME, which is handover acknowledgment message.

6. Security Analysis

The proposed protocol has enhanced the performance level and security level as it solved three main problems of the standard protocol, which are Desynchronization attack, Man In The Middle attack and long setup time.

A. Standard Protocol

The standard protocol suffers from Man In The Middle Attack, Desynchronization and sequential long setup time.

B. MRN Protocol

The MRN concept neglected the authentication between the UEs and MRN, which may suffer from Man in the Middle Attack, Desynchronization Attack as it focused only on the authentication between the MRN and eNBs.

C. Proposed Protocol

1) The proposed protocol solved Man In the Middle attack by using certificate concept to authenticate the UE and eNBs and by using KMU.

2) The proposed protocol solved desynchronization attack by using certificate concept for authenticating eNBs and deriving the session key between the eNBs and UEs before starting handover process.

3) The proposed protocol achieved a Fast Intelligent Authentication, which achieved the authentication in parallel manner not sequential. The session key is divide into two parts, the 1st part is derived by UE, while the second part is derived by eNBs.

7. Performance Analysis Simulation Results

A. Communication Overhead

1) The standard Protocol achieved the Intra-Handover in 5 messages.

2) The MRN Concept achieved mutual authentication between MRN and core network in 5 messages, but it neglects the authentication messages between the UEs and MRN.

3) The Proposed Protocol achieved the authentication for handover process in 9 messages for both types of handover (Intra or Inter-Handover).

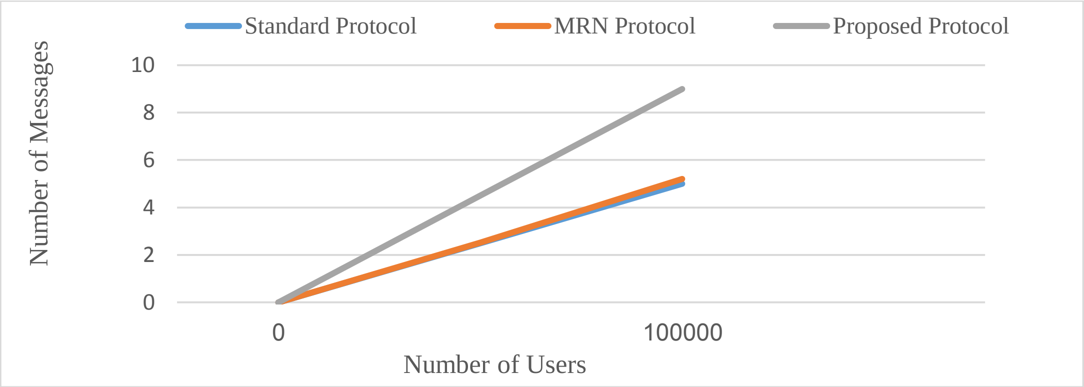

Fig.5 Communication Overhead

B. Computations Overhead

1) The standard protocol used the basic cryptographic functions, which are used in EPS-AKA. It needs to perform all these cryptographic function each handover process.

2) The MRN concept added a new entity, which is MRN itself. This MRN is authenticated with UEs along the established Known route, but the MRN uses 3 Key Distributions Functions (KDFs) and one AES encryption Function. Also, it needs to perform all these operations each handover process.

3) The proposed protocol used the hybrid key management to perform the handover. This hybrid key management is consisted of asymmetric key and symmetric key management. The number of these operations is based on the number of eNBs along the established Known Route, but these operations are performed only once and in offline mode.

C. Setup Time

Implementation of the standard protocol, MRN protocol and proposed Protocol are performed using Eclipse environment and C programming language, the simulations have taken place on a Laptop using a 64-bit windows 10 operating system. The Laptop is running with speed of 2.49 GHz, to calculate the time taken for the followings:

1) Standard protocol, which is (0.453 Sec). This time will be taken every handover process.
2) MRN protocol, which is (0.560 Sec). This time will be taken every handover process.
3) Proposed Protocol, which is (0.760 Sec) assuming three target eNBs, which means three hybrid authentication and key agreement. This time will be taken only once before starting handover process.

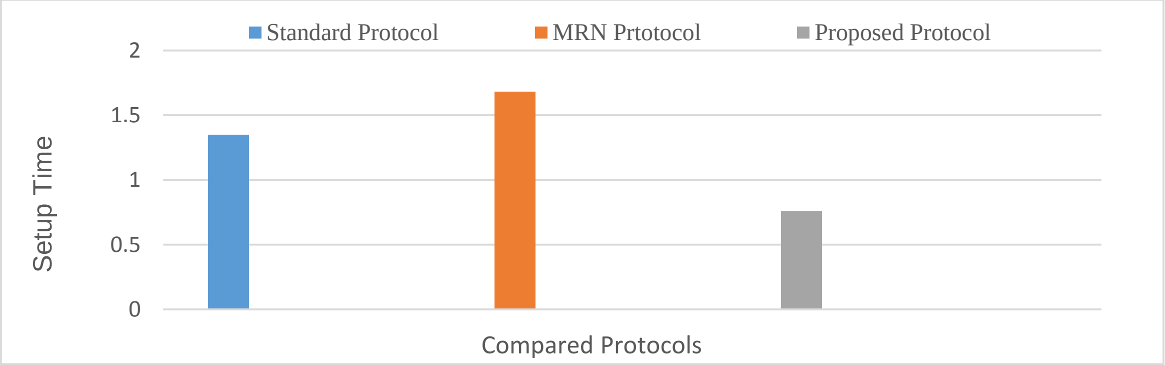

Fig.6. Setup Time for 3 eNBs

Comment: The proposed protocol enhanced the setup time as it is executed only once in the beginning of the call and in offline mode.

8. Comparison with Related Work

This section is comparing the proposed protocol with the standard protocol and the concept of MRN. Table.3 shows this comparison.

Table 3. Comparison with Related Work

Comparison	Standard Protocol	MRN Protocol	Proposed Protocol
Communication Overhead	5 messages for each Intra-Handover	5 messages for each handover weather inter or intra handover	9 messages Only once for any type of handover
Computations Overhead	Lower	Higher	Lower
Setup Time for three eNBs	1.35 Sec	1.68 Sec	0.760 Sec
Man in The Middle Attack	Exist	Exist	Not Exist
Desynchronization Attack	Exist	Exist	Not Exist
Security Level	Low	Low	Higher
KMU	Not used	Not used	Used
Authenticate UE	Not achieved	Not achieved	Achieved
Certificate for every eNB	Not achieved	Not achieved	Achieved

9. Conclusion and future work

The proposed protocol solved Man in the Middle attack by adding a CA, which distribute the certificates for each eNB. In addition, the proposed protocol used a KMU for each UE to verify the certificates of each eNB and to achieve the key management. Also, the proposed protocol solved Desynchronization attack by achieving the authentication and key agreement with all eNBs in offline mode in parallel and before starting the handover process to lower setup time. The proposed protocol achieved a Fast Intelligent Authentication Handover over LTE network based on driving a part of session key by the UE, while the second part is derived by each eNB. For the future work, we are going to complete the full security architecture by implementing END- to- END authentication.

References

[1] Dahlman, and J. Skold, “4G: LTE/LTE-Advanced for Mobile Broadband”, 2013, Academic press, pp 431.

[2] E. Dahlman, S. Parkvall, J. Skold, and P. Beming, “3G Evolution: HSPA and LTE for mobile broadband”, 2010, Academic press, pp 431.

[3] Senthilkumar Mathi and Lavanya Dharuman, “Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication scheme” in Twelfth International Multi-Conference on Information Processing (IMCIP), in 2016.

[4] Zaher Haddad , Mohamed Mahmoud , Imane Aly Saroit and Sanaa Taha, “Secure and Efficient Uniform Handover Scheme for LTE-A Networks” in Wireless Communication and Networking Conference (WCNC), in 2016.

[5] Md Mehedi Masud, “Survey of security features in LTE Handover Technology”, in Scientific Research Journal, in 2015, vol III.

[6] 3GPP, “Technical Specification Group Services and System Aspects”; 3G security; Handover interface for Lawful Interception (LI) (Release 14) 3GPP TS 33.108 V14.2.0 (2017-09)

[7] N. Sivaranjani, R2. Kohila and M2. Nithya, “Cryptography Key Initiator for 4G LTE Networks Using Session Keys”, in Middle East journal of scientific Research, in 2016.

[8] Qi Jing, Yuqing Zhang and Animu Fu “A Privacy Preserving Handover Authentication Scheme for EAP-Based Wireless Networks” in GLOBCOM, in 2011.

[9] Qinglei Kong, Rongxing Lu and Shuo Chen, “Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks”, in IEEE Internet of things, in 2017.

[10] Jin Cao, Maode Ma and Hui Li, “G2RHA: Group-to-Route Handover Authentication Scheme for 4G LTE-A High Speed Rail Networks”. In IEEE Transaction on Vehicular Technology, in 2017.