International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 4 Issue 10 ǁ October. 2016 ǁ PP. 19-28

Authenticated Key Management Scheme for Intra-Mme Handover Over LTE Networks

Khaled Mohamed Khairy[1], Ashraf Diaa Eldien[2], Ahmed A. Abdel-hafez[3], Essam Abd El-Wanis[4]
[1](PhD Student, Dept. of Communication/ Military Technical College/ Cairo, Egypt)
[2,3,4] (Dept. of Communication/ Military Technical College/ Cairo, Egypt)

Abstract : In the intra-MME handover over the Long-Term Evolution (LTE), the key management takes place in between the source eNodeB and target eNodeB under the same Mobility Management Entity (MME). 3GPP has specified some security mechanisms to insure the safety of intra-MME handover key management, but nevertheless there exists a few vulnerabilities compromising the protection of the LTE entities, one of the most harmful is the desynchronization attack.The major contribution of this paper is; to put forward a new authenticated key management scheme, to overcome the desynchronization attack, by keeping out the source eNodeB and use MME as a third trusted party for intra-MME handover. The proposed scheme is analyzed under three adversary models. A formal security analysis is performed as well using a specialized model checker, Scyther. Moreover, a performance evaluation of the proposed scheme is conducted. Finally, a comparison with the current intra-MME handover scheme is introduced.

Keywords : LTE, Handover, Desynchronization attack, Forward Security, Backward Security.

I. INTRODUCTION

LTE is the most used standard [1] developed by the 3G partnership project for next-generation mobile networks, designed for providing seamless coverage, high data rate, full interworking with heterogeneous radio access networks and service providers, and low latency [2]. LTE/System Architecture Evolution (LTE/SAE), is divided into two parts; the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC). Together are referred to as Evolved Packet System (EPS). The E-UTRAN comprises of Evolved NodeB (eNodeB), which provides the radio communications between the UE and the EPC. The control entity of E-UTRAN, Mobility Management Entity (MME) interacts with a central database known as Home Subscriber Server (HSS) to authenticate the UE and provides temporary identity for the user.The serving gateway manages the user plan mobility and maintains the data paths between the eNodeBs and the Packet Data Network (PDN) Gateways, which provides connectivity for the UE to external packet data networks. The HSS holds the MME identity to which the user is currently attached and it upholds information about the PDNs to which the user can connect. In addition, it includes the Authentication Center (AUC) to generate the Authentication Vectors (AV).

LTE supports two kinds of Mobility Management Entity (MME) handovers, one is the inter-MME and the other is the intra-MME handover. In the intra-MME handover, which can be called also inter eNodeB handover or X2 handover, the key management takes place in between the source eNodeB and target eNodeB under the same MME via X2 interface. Target eNodeB gets the session key from the source eNodeB, this session key is used further by target eNodeB. In this key derivation mechanism, target eNodeB knows the session key used by source eNodeB. To overcome this problem, the source eNodeB uses a one-way hash algorithm to compute the new session key to ensure backward key separation [3]. However, it still lacks security, as eNodeBs would know all the future session keys used in further handovers. Thus, two-hop forward key separation was introduced, in which designers introduced a new strategy of adding up fresh parameters i.e., Next Hop (NH) key and the NH Chaining Counter (NCC), from MME at the time of key derivation. This mechanism helps in protecting all the future session keys from eNodeB, except the session keys derived during the next two intra-MME handovers. Still, there exists a loophole in the handover key management, where an attacker can break the forward key separation using a rogue base station then apply the desynchronization attack. Therefore, all the future session keys between UE and eNodeB are compromised unless the local root key K_{ASME} is updated.

This paper proposes a new authenticated key management scheme to overcome the desynchronization attack during the intra-MME handovers, achieves the security requirements, and maintains the one-hop forward security and one-hop backward security.The remaining paper is organized as follows: Section 2 presents, the LTE security architecture, including the key hierarchy and intra-MME handover. Section 3, discusses the security flaws in the intra-MME handover key management. In section 4, the related work is listed and

discussed. Section 5, presents the proposed scheme, an analysis of its security and an evaluation of its performance. Finally, the conclusion and future work of this paper are presented in section 6.

II. LTE SECURITY ARCHITECTURE

This section is going to discuss mainly, the key hierarchy in LTE security architecture and transfer of messages in between UE, eNodeBs and MME during intra-MME handover key management.

2.1 Key Hierarchy

Generating the keys, for ciphering and integrity protection in LTE/SAE adopts a deriving method. All the keys in LTE are derived from the subscriber specific master key or the root key (K). This key is a random 128-bit string permanently stored in the USIM and the AUC [4]. Each time a UE registers itself to the LTE network, EPS-AKA takes place between a UE and MME on behalf of the HSS. The root key derives {CK, IK}, which derive the local root key (K_{ASME}). Next, MME derives three keys from K_{ASME}. The first two transient keys, {K_{NASenc}, K_{NASint}}. The third key (K_{eNB}), on which this paper focus, specific for encrypting the traffic between the eNodeB and the UE. During the handover, the KeNB is further transformed to a new K_{eNB}* with a Key Derivation Function (KDF). Therefore, keeping K_{eNB} away from attackers, especially during the period of a handover, is a very important and meaningful work

2.2 Intra-MME Handover

For efficiency, source eNodeB provides the next K_{eNB} to the target network for use after the handover. Before the next EPS-AKA, a set of session keys is linked to each other in what is known as handover key chaining [5]. To achieve backward key separation, source eNodeB derives the next K_{eNB}* from the current one K_{eNB} by applying a one-way hash function. To ensure forward key separation, the source eNodeB must capitalize on fresh keying material from the MME, which can provide fresh keying material to the target eNodeB only after the intra-MME handover. This fresh material is to be used in the next handover. The result is two-hop forward key separation, in which the source eNodeB does not know the target eNodeB key only after two intra-MME handovers. Handover key chaining includes two extra parameters as fresh keying material; the Next Hop (NH) key and the NH Chaining Counter (NCC). MME recursively generates a new NH key derived from K_{ASME} for each handover. The source eNodeB derives the new K_{eNB}* value from either; the currently active K_{eNB} (horizontal key derivations), or from the NH key received from an MME on the previous handover (vertical key derivations).

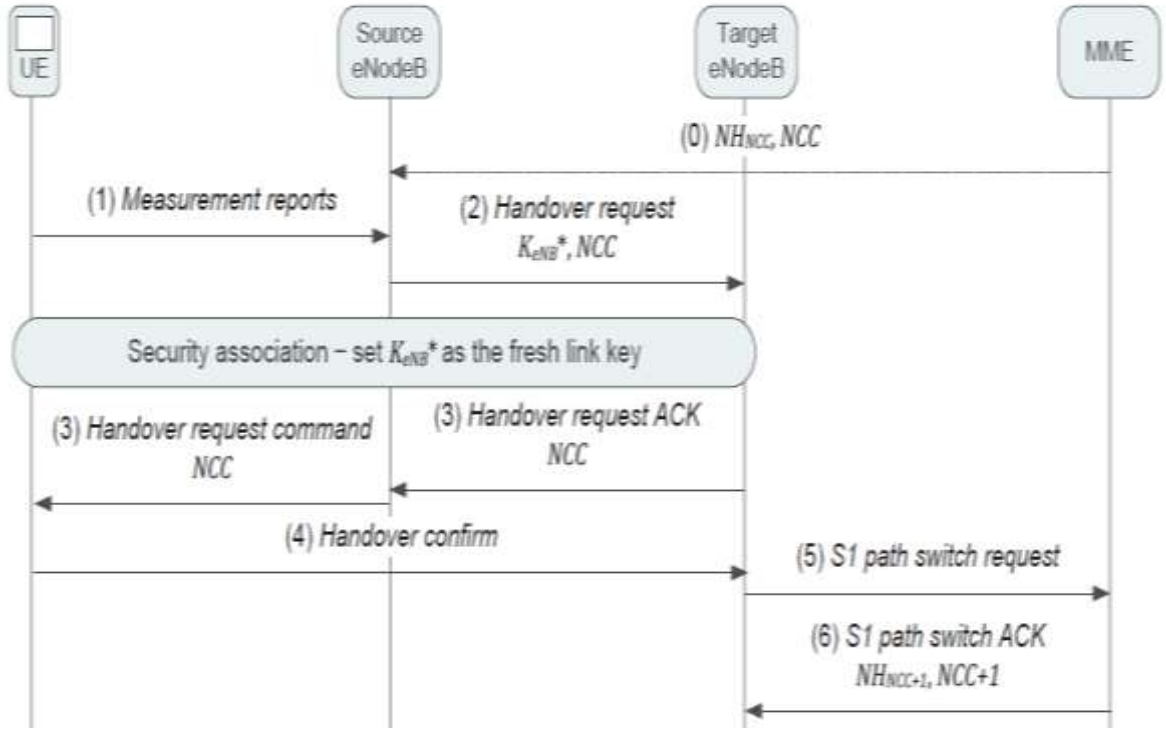

Figure1: Message Flow of the intra-MME Handover in the EPS.

K_{eNB}*= KDF (NH_{NCC}, α). (1)
K_{eNB}*= KDF ($K_{eNB,}$α). (2)
Where NH_{NCC} = KDF (K_{ASME}, NH_{NCC-1}). (3)
NH_0 = KDF (K_{ASME}, K_{eNB})
(α) Target Physical Cell Identity (PCI) and Frequency.

Fig. 1 illustrates the message flow of the intra-MME handover. The source eNodeB has fresh keying material, {NH_{NCC}, NCC}, from the previous handover (see message (0) in Fig.1). NH_{NCC} denotes that the NH key is updated NCC times. The source eNodeB forwards the {K_{eNB}*, NCC} pair to the target eNodeB (see message (2) in Fig.1). The subsequent session keys between a UE and the target eNodeB are derived directly from the new K_{eNB}*. The target eNodeB sends the NCC to a UE (see message (3) in Fig.1).

UE compares the received NCC with the NCC value, associated with the current security association (i.e., NCC-**1).** If the same; UE uses the vertical key derivation. In this case, the new session key K_{eNB}*will be derived by KDF from the fresh NH key (NH_{NCC}) as denoted in equation (2). Where, the NH_{NCC} is derived from the previous NH value (NH_{NCC-1}) and K_{ASME}, see equation (3). Otherwise, UE uses the horizontal key derivation), as denoted in equation (1). If the received NCC is greater than the current NCC, UE will first synchronize these two NCC values by computing the NH key and the NCC value iteratively until the two NCC values match, then derives the K_{eNB}* from the currently active K_{eNB} using equation (2).

When the target eNodeB complete the handover signaling with UE, it sends the *S1 path switch request* message (message (5) in Fig.1) to the MME. The MME increments the NCC value by one, then computes a new NH (i.e., NH_{NCC+1}) from the K_{ASME} and current NH key. Then, the MME forwards the fresh {NH_{NCC+1}, NCC+1} pair to the target eNodeB for use in the next handover.

III. SECURITY ANALYSIS OF INTRA-MME HANDOVER

Although the 3GPP AKA has been accepted as reliable and has been employed for a while, but still exist some weaknesses in 3GPP AKA [6]. The weaknesses include; redirecting user traffic using rouge base station and mobile terminals and the desynchronization attack consequently. This section examines the security vulnerabilities of the intra-MME handover by modeling a rogue base station attack.

1.1. Rogue Base Station Attack

A rogue base station is a mobile device that impersonates 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 [7]. By physically penetrating an eNodeB, an adversary can access its stored cryptographic materials. Because eNodeBs are Internet endpoints, an adversary also can gain access to the operating systems of eNodeBs by disseminating viruses and worms and commandeers eNodeB as members of a botnet. Furthermore, a commercial eNodeB can be compromised by vulnerabilities because of the IP stack such as identity forgery, eavesdropping, packet injection, packet modification, denial-of-service (DoS) attacks, and so on. An attacker can masquerade as legitimate eNodeB by stealing identities and utilizing them to transmit messages.

1.2. Desynchronization Attacks

The goal of the rogue base station attack is to disrupt updating of the NCC value, leaving the targeted eNodeB desynchronized, and the future sessions keys vulnerable to compromise. In turn, the rogue eNodeB attack allows an adversary to force the targeted eNodeBs to perform horizontal key derivation. The refreshing of the NCC value can be disrupted by manipulating the message between eNodeBs. The rogue eNodeB purposely sets an extremely high value for the NCC value denoted as α, and sends it to the targeted eNodeB in the handover request in message (2) of Fig.1. This extremely high α value ranges near the highest value permitted for the 8 bits NCC counter. An adversary sends the original NCC value denoted as β to the UE. By synchronizing the false NCC value (i.e., α), orders it not to perform vertical key derivation. The NCC value from the *S1 path switch ACK* message (6) of Fig.1, is considerably smaller than that received from the rogue eNodeB (i.e., β+1 << α). In turn, this size difference makes the targeted eNodeB and the UE to derive the next session key based on the current K_{eNB} instead of on the new $NH_{\beta+1}$ Key. An opponent can also desynchronize the NCC value by manipulating the S1 path switch ACK message. An eNodeB compromised by the IP vulnerabilities [8] would be capable to launch IP spoofing and man-in-the-middle attacks onto the S1 interface to modify the NCC update message from an MME to the targeted eNodeB. A forged message that includes a lower NCC value than a current NCC value would cause the targeted eNodeB not to acknowledge the fresh NCC value.

Once the desynchronization attacks break the security of forward key separation, an attacker with a rogue eNodeB can decipher messages between the genuine eNodeB and a UE, including RRC signaling and U-plan data. In turn, a compromised K_{eNB} would then be utilized for further active attacks.

The effect of compromising a key by a desynchronization attack lasts until K_{ASME} is revoked, through the EPS-AKA procedure required between an MME and a UE. In this process, the new session key K_{eNB}*and subsequent security contexts are created from scratch.Therefore, to fit with the security requirements of the next generation mobile communication system; an enhancement of the current intra-MME handover key management is needed to prevent the desynchronization attack and to maintain the one-hop forward and one-hop backward security.

IV. RELATED WORK

To overcome the desynchronization attack, *Chan-Kyu et al* suggested a scheme for secure handover key management, which introduces an optimal time to update the local root key value [5]. Since, it depends on key interval time; there is a possibility for the attacker to perform the attack before the local root key updating. Furthermore, the handover key management using device certification by *Sridevi et al* suggested a technique that enhances security between the corresponding entities in LTE architecture [9]. Here, it involves a new device called, certificate authority; it uses the public key cryptography for deriving certificate and session keys. Wherein, all the entities of LTE should be verified with their identity through the certificate chain. However, the scheme is not scalable and contains time and bandwidth constraints. Also, all entities demand its certificate from a single authority, there is a possibility for the bottleneck to occur due to the centralized feature.

The authors in [10] introduced the concept and operational mechanism of Session Key Context (SKC), which is a way to distribute the keys to the base stations. They showed how the intra-MME handovers can be made always one-hop key separated by using the SKC concept, by providing multiple {NH, NCC} pairs from the MME to target eNodeB, in SKC structure. In this case, target eNodeB takes the row that has its identity in it, decrypts and verifies it, and uses the {NH, NCC} pair in it. In this method, the source eNodeB can't get the NH used by target eNodeB for deriving the new K_{eNB} because the NH value is encrypted by the identity of target eNodeB. Thus, the source eNodeB can't derive the new key used by target eNodeB. Therefore, one-hop forward security can be satisfied. But for applying this new scheme, the key hierarchy and signaling procedures of the current intra-MME handover need to be reconstructed.

The authors in [11] tried to make some key parameters invisible to the source eNodeB, by investigating a scheme that includes an additional parameter known as, Cell Radio Network Temporary Identifier (C-RNTI), in the EPS architecture. Herein, UE sends handover request to the source eNodeB, in turn the request message is forwarded with the key (K_{eNB}*) and NCC to the target eNodeB, which generates the C-RNTI assigned to the UE, and sends it to MME. The ciphered C-RNTI by MME using the master key (K_{ASME}) is sent to the target eNodeB. On using the master key (K_{ASME}) which is pre-shared between UE and MME, they encrypt C-RNTI and the K_{eNB}*, so that the source eNodeB can't get C-RNTI during the handover, and it can't directly derive the new K_{eNB} used by target eNodeB. Nevertheless, the scheme uses too many communications between the entities, assume if the target eNodeB is a rogue, then C-RNTI uses a false value, where communication between the source and the target can jeopardize.

The authors in [12] introduce a mitigation scheme to minimize the effect of desynchronization attack. A new key derivation function has been added to the existing framework to force the attacker to send the real NCC value to both UE and eNodeB and thus annihilate any chances of modification to NCC. In this scheme; eNodeB perform a key derivation with the inputs K_{eNB}* and NCC value. The target eNodeB sends the NCC value to UE via source eNodeB. As soon as UE receives the NCC value from the source eNodeB, it must check whether current NCC is greater than the previous NCC value. If so, then UE uses vertical key derivation, else uses horizontal key derivation.

In case of vertical key derivation, firstly UE derives NH key corresponding to the NCC value. Then it derives K_{eNB}* using NH key and then derives K_{eNB}** using KDF, i.e. K_{eNB}**=KDF (K_{eNB}*, NCC). This scheme can reduce the impact of desynchronization attack, yet not totally in view of two-hop forward key separation in X-2 handovers, also it can avoid the data exposure except during forward key separation. Finally, the data exchanged after the desynchronization attack is exposed to attacker unless S1 handover (inter-MME handover) takes place.

V. PROPOSED SCHEME

In this section; assumptions of the network model and the adversary model are introduced. Then the proposed scheme is explained. Finally, the security analysis of the proposed scheme and an evaluation of its performance are conducted.

1.3. Network Model

1.3.1. LTE Mobile Network Model

LTE entities: the UE, the eNodeBs, the MME and the HSS will be involved in the proposed scheme, considering both voice and data modes while the handover process takes place.

1.3.2. Backhaul Link Protection

IKEv2/IPsec with integrity and confidentiality protection is mandatory for all traffic (control/user/management plan) for S1 and X2 user plan interfaces, or physically protected.

1.4. Adversary Model

Three adversary models are constructed for the better carrying out the security analysis of the proposed scheme:

(1) Attackers can steal and decipher the messages in radio channels.
(2) Attackers can steal and decipher the messages in radio channels, and totally control the source eNodeB.
(3) Attackers can steal and decipher the messages in radio channels, and totally control the target eNodeB.

1.5. The Proposed Scheme

The main idea of the proposed scheme is; keeping out the source eNodeB, and involving the MME as a Third Trusted Party (TTP) during the handover key management. MME prepares the challenges needed for the mutual authentication between the UE and the target eNodeB. In addition, MME generates the fresh materials needed to drive the new session key K_{eNB}*, and sends these materials for both the UE protected by the local root key K_{ASME}, and to the target eNodeB which is physically protected or encrypted with the pre-shard IPsec association keys K_{IP} between the core network and the eNodeB. The proposed scheme as shown in Fig.2, can be illustrated by the following steps:

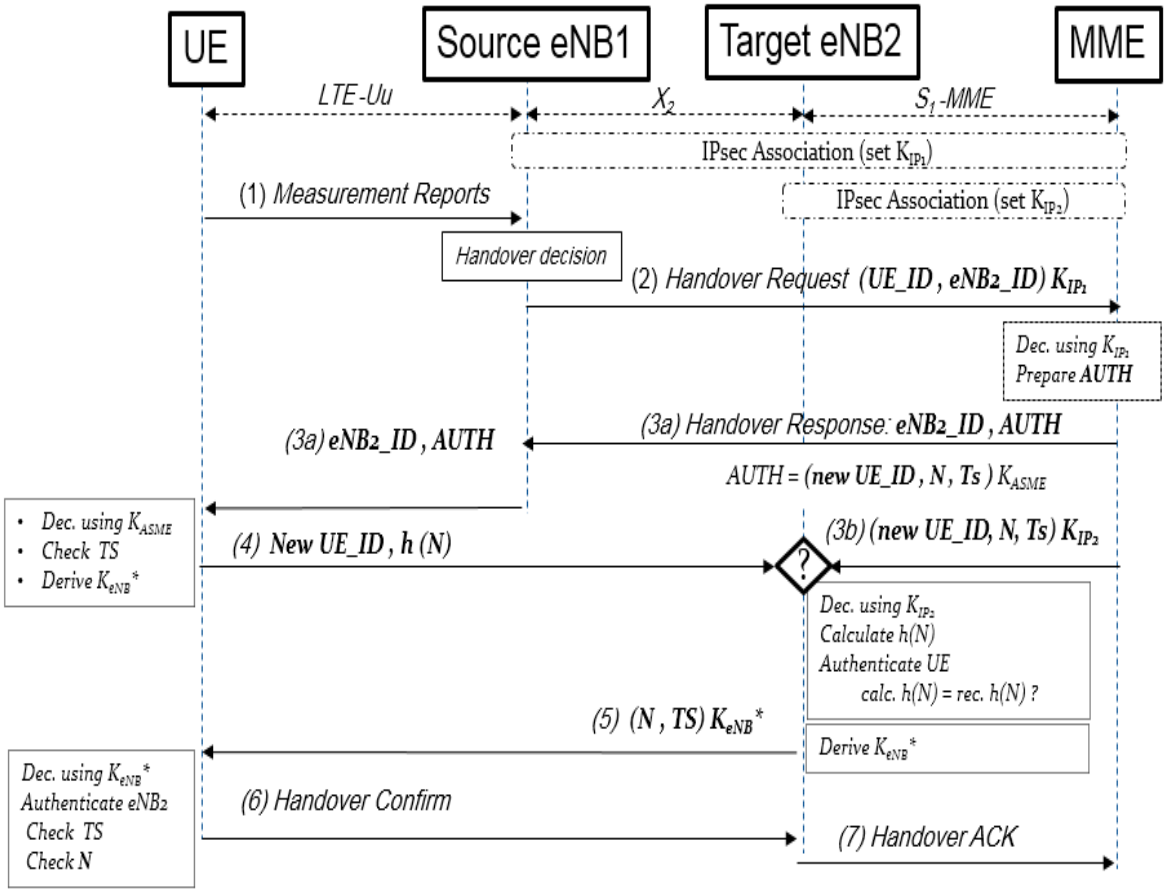

Figure 2: The Proposed Scheme

1) UE sends the measurement report to the source eNodeB, as the message (1).
2) Source eNodeB takes the handover decision, then sends the handover request to the MME, as the message (2).
3) MME sends back an authenticator vector (AUTH) to the UE, as the message (3a), and sends its contents to the target eNodeB, encrypted by K_{IP2}, as message (3b).
4) UE checks the freshness of the message (3a), and use the nonce to derive the new session key K_{eNB}* as denoted in equation 4, then sends the hash of the received nonce as a challenge to the target eNodeB, asthe message (4).

$$K_{eNB}^{*} = KDF(N, \alpha) \qquad (4)$$

5) Target eNodeB authenticates the UE by comparing the received hash from the UE with the calculated one from the message (3b). If the same; it derives the new session key K_{eNB}* using equation (4), and sends the message (5), to the UE to prove its identity.
6) UE authenticates the target eNodeB by checking the freshness of message (5) and the Nonce, if the same; UE sends back handover confirmation, message (6).
7) Target eNodeB acknowledges the MME, message (7), that the handover process has finished successfully.

1.6. Security Analysis of the Proposed Scheme

The security analysis of the proposed scheme, under the three adversary models, comparing with the current scheme, shows that:

1) Attackers can steal the messages in radio channels

- In this situation, the attacker can't obtain the new session key parameters sent on air to the UE, encrypted using K_{ASME}. The attacker also can't obtain the current active session key K_{eNB}. Thus, he can't derive the new key K_{eNB}*.
- Therefore, the proposed scheme can achieve one hope forward key separation.The current scheme also satisfies one-hop forward security in this adversary model.

2) Attackers can steal the messages in radio channels, and totally control the Source eNodeB

- In this situation, the attacker can obtain K_{eNB} and the encrypted AUTH, but can't get the fresh parameters of the new session key K_{eNB}*. Therefore, the proposed scheme can achieve one hope forward key separation.
- The current scheme satisfies two-hops forward key separation, because the attacker can get K_{eNB} and {NH, NCC} values stored in the source eNodeB. Thus, he can derive K_{eNB}*. But at the next handover, he can't get NH_{NCC} derived by MME using K_{ASME}, used in the next handover.

3) Attackers can steal the messages in radio channels, and totally control the Target eNodeB;

- In this situation, the attacker can get the fresh parameters and derives K_{eNB}* using equation (4), and compromise the messages between the UE and the target eNodeB, the exposure time of these messages will not exceed the time of the next handover. At the next handover, the attacker will not be able to get the new K_{eNB}*.
- Therefore, the proposed scheme can always achieve one hope forward key separation.

As in the current scheme, a one-way key derivation function is used to derive the new session key K_{eNB}*, an attacker can't reversely deduce the previous key K_{eNB}, achieving one hope backward key separation in the three models.

As a summary, the comparison results of security requirements are presented in Table 1. The proposed scheme authenticates both the UE and the target eNodeB before the handover takes place. Also, it doesn't send the new session key parameters on the air to the UE as a plain message, as the current scheme used to. Instead, it sends these parameters encrypted to the UE and the target eNodeB, achieving the confidentiality and the integrity of the new session key's parameters, and achieves the non-repudiation. The proposed scheme achieves, one hope key separation forward and backward under the three adversary models, meanwhile, the current scheme can satisfy only one-hop backward security.

Table 1. Comparison Results of Security Requirements

Security Requirements	Current Scheme	Proposed Scheme
Confidentiality	No	Yes
Data Integrity	No	Yes
Authenticity	No	Yes
Non-Repudiation	No	Yes
Prevent Desynchronization Attack	No	Yes
Forward Key Separation	Two-hops	One-hop
Backward Key Separation	One-hop	One-hop

1.7. Formal Verification

In this section, a formal security analysis of the proposed scheme is conducted, using a specialized model checker Scyther [13].

1.7.1. A Model Description

The proposed scheme consists of four communicating agents, UE, source eNodeB, target eNodeB, and MME. Each agent performs one or more roles, as well as certain security claims. An intruder may try to oppose such security goals. This description identifies the following components of the security protocol model.

1) Protocol specification, describes the behavior of each of the roles in the protocol.
2) Threat model, based on Dolev and Yao's network threat model [14], where the intruder has complete control over the communication network.
3) Cryptographic primitives such as encryption, using the black box approach.

1.7.2. Properties Specifications

Session key parameter's secrecy, aliveness, agreement, and authentication, are the security properties that will be analyzed and verified. Scyther will verify the protocol description, if it passed; Scyther will start verifying the roles' claims, considering the threat model. If the claims verification failed, a design review then needed.

1.7.3. Verification Results

The proposed scheme description has been verified and analyzed by Scyther tool. The formal verification results are shown in Fig.3; the session key parameter's secrecy and the aliveness, agreement, and authentication claims have been verified for the four communicating agents.

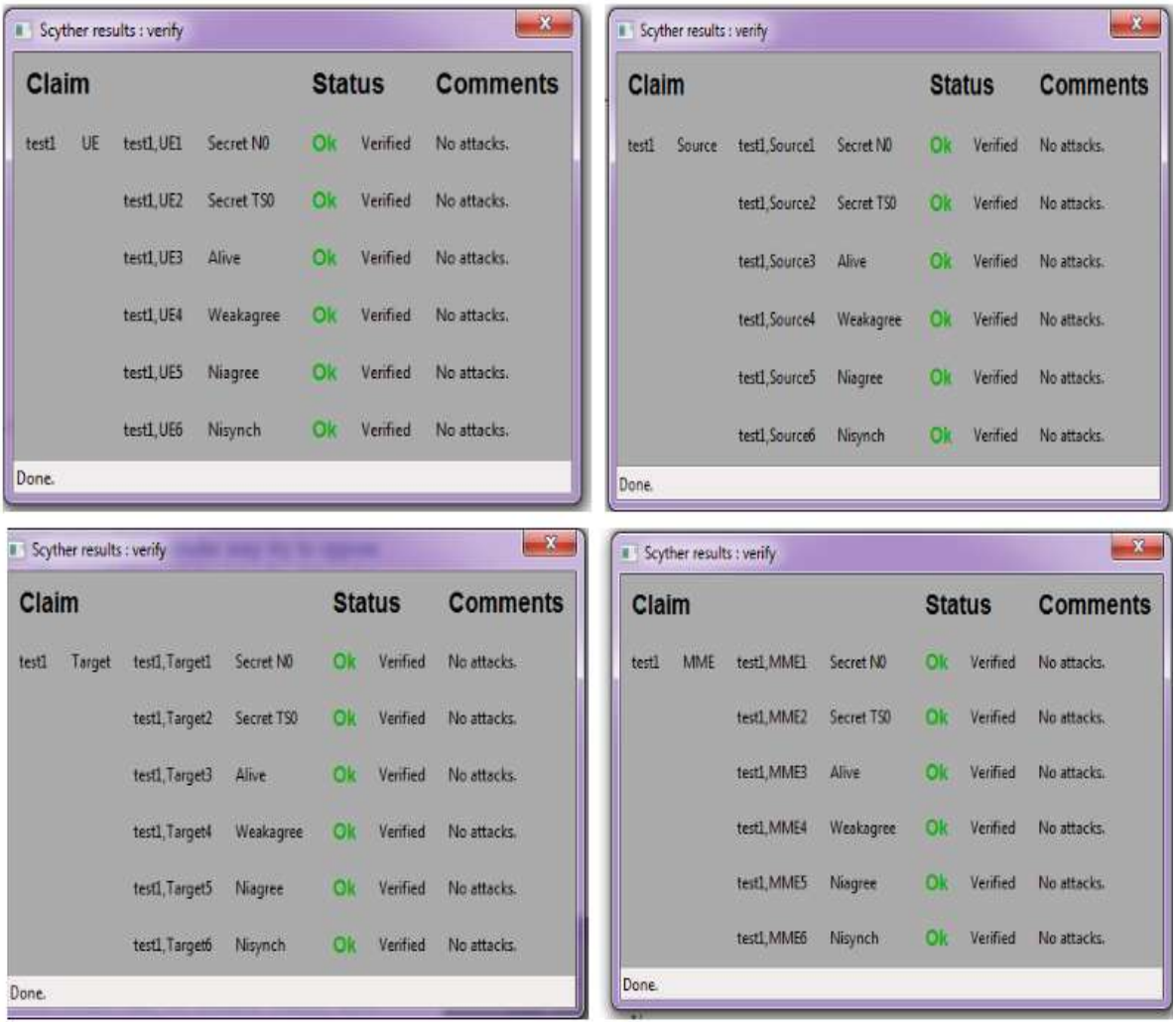

Figure 3. Formal Verification Results

1.8. Evaluation of the Proposed Scheme

As a comparison with the related work, the proposed scheme doesn't use the public key cryptography to establish a certificate chain for the entities of LTE to verify their identities; instead, it uses the symmetric pre-shared keys and the hash function which are lightweight functions. Also, the MME doesn't have to provide multiple {NH, NCC} values, to the source eNodeB, which increase the storage cost of the source eNodeB. In addition, the proposed scheme doesn't add additional parameters, and doesn't use too many communications between the entities to enhance the security of the current scheme.In this section, a comparison between the proposed scheme and the current scheme will be introduced, per the performance, including; the computation overheads, the communication overheads, and the storage overheads.

1.9. Computation Overheads

As shown in Table 2 and Table 3; The proposed scheme performs (12) operations as the current scheme used to do, as a total number of computations, if no attack exists. Meanwhile, if the desynchronization attack has happened; current scheme will perform more computations to synchronize the two NCC values by the UE, before deriving the new session key K_{eNB}*, as described Table 4.

Table 2. Computational Complexity of the proposed scheme

	UE	Source eNodeB	Target eNodeB	MME	Total
Encryption	2	1	1	2	6
Hashing	1	-	1	-	2
Comparison	1	-	1	-	2
KDF	1	-	1	-	2
Incrementing NCC	-	-	-	-	-

Table 3. Computational Complexity of Current Scheme without attack

	UE	Source eNodeB	Target eNodeB	MME	Total
Encryption	-	1	2	3	6
Hashing	-	-	-	-	-
Comparison	1	-	-	-	1
KDF	2	1	-	1	4
Incrementing NCC	-	-	-	1	1

Table 4. Computational Complexity of Current Scheme with attack

	UE	Source eNodeB	Target eNodeB	MME
Encryption	-	1	2	3
Hashing	-	-	-	-
Comparison	Up to 255	-	-	-
KDF	1 (K_{eNB}*) &Up to 255(NH)	1 (K_{eNB}*)	-	1 (NH)
Incrementing NCC	Up to 255	-	-	1

1.9.1. Communication Overheads

As shown in Table 5. The current scheme needs 8 messages for the handover to take place. On the other side, the proposed scheme added only one message as a communication overhead more than the current scheme for achieving all the security requirements.

Table5. Comparison Results of Communication Overheads

	UE		Source eNodeB		Target eNodeB		MME		total
	TX	RX	TX	RX	TX	RX	TX	RX	
Current Scheme	2	1	2	3	2	3	2	1	8
Proposed Scheme	3	2	2	2	2	3	2	2	9

1.9.2. Storage Overheads

In the current scheme, the UE needs to store the NCC value associated with the current security association. MME also need to update and store the pair {NH_{NCC+1}, NCC+1} to be sent to the target eNodeB as acknowledgement to the s1 path switch request. On the other side, the proposed scheme doesn't need to store these values. Instead, it uses a fresh pseudo random nonce, generated by the core network, changing periodically each handover, to derive the new session key.

VI. CONCLUSION AND FUTURE WORK

In this paper, a new authenticated key management scheme for intra-MME handover is proposed, based on; keeping out the source eNodeB from the key management process, and using the MME as a third trusted party. In the proposed scheme; MME sends the fresh materials needed to drive the new session key K_{eNB}* for both the UE and the target eNodeB, away from the source eNodeB, protected by the pre-shared local root key K_{ASME} and the pre-shared IPsec association key $K_{IP2,}$ respectively.

Therefore, the key separation is maintained and the desynchronization attack is prevented. Moreover, the proposed scheme increases the essential root key update interval, because the proposed scheme breaks the handover key chaining by keeping out the source eNodeB from the handover key management. Thus, the exposure time of the handled packets by the rouge base station, if exit, will not exceed the time of the next handover. Comparing with the current scheme, the effect of a desynchronization attack can last until the next update of the local root key K_{ASME}.

A design verification of the proposed scheme was conducted, using a specialized model checker *Scyther*, showing that; the session key parameter's secrecy and the aliveness, agreement, and authentication claims have been verified for the communicating agents.

The performance evaluation of the proposed scheme is conducted, showing that; the proposed scheme achieves its goals with a slight increase in the communication overheads, only one message more than the current scheme. Also, the proposed scheme didn't increase the computational overheads, when no attack is presented. Moreover, the current scheme needs more computations than the proposed scheme to overcome the desynchronization attacks, if exists. Finally, the proposed scheme doesn't need to store the session key's parameters as the current scheme used to do, but a fresh parameter is used to derive the new session key. As a future work; the inter-MME handover will be analyzed per security aspects and performance, for proposing a provable secure lightweight authentication protocol, to overcome the EPS-AKA vulnerabilities and makes the inter-MME handover more efficient.

REFERENCES

[1]. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, "Formal analysis of the 3G authentication protocol, version 3.1.0," 3GPP, TR 33.902, 1999.

[2]. E. Dahlman, S. Parkvall, and J. Skold, 4G: LTE/LTE-advanced for mobile broadband: Academic press, 2013.

[3]. 3GPP, "3GPP System Architecture Evolution (SAE); Security architecture," 3rd Generation Partnership Project (3GPP), Version 11.2.0, TS 33.401, 2011.

[4]. 3GPP, " Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 11) 3GPP TS 33.401 V11.6.0 (2013-03).

[5]. Chan-Kyu Han, Hyoung-Kee Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks," in Mobile Computing, IEEE Transactions, Vol.13, pp.457-468, Feb. 2014

[6]. Muxiang Zhang Yuguang Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communications, vol. 4 Issue 2, 2005.

[7]. Chan-Kyu Han, Hyoung-Kee Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks," in Mobile Computing, IEEE Transactions, Vol.13, pp.457-468, Feb. 2014

[8]. Park, Yongsuk, and Taejoon Park. "A survey of security threats on 4G networks." 2007 IEEE Globecom Workshops. IEEE, 2007.

[9]. Sridevi, B., Divya Mohan, and R. Neelaveni. "Secured Handover Key Management among LTE Entities Using Device Certification." Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference on. IEEE, 2014.

[10]. Forsberg D, "LTE key management analysis with session keys context," in Computer Communications, 33: pp.1907-1905, 2010.

[11]. Xiao, Qinshu, Baojiang Cui, and Lingrong Li. "An Enhancement for Key Management in LTE/SAE X2 Handover Based on Ciphering Key Parameters." P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on. IEEE, 2014.

[12]. Chandavarkar, B. R. "Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE." Contemporary Computing (IC3), 2015 Eighth International Conference on. IEEE, 2015.
[13]. Cas Cremers, "Scyther - Semantics and Verification of Security Protocols", Ph.D. THESIS, Eindhoven University of Technology, 2006.
[14]. Wenbo Mao, "A Structured Operational Modeling of the Dolev-Yao Threat Model", Hewlett-Packard Laboratories, United Kingdom, August 2002.