Synchronous Authentication Key Management Scheme for Inter-eNB Handover over LTE Networks

Shadi Nashwan
Computer Science and Information Department
Aljouf University
Aljouf, Saudi Arabia

***Abstract*—Handover process execution without active session termination is considered one of the most important attribute in the Long Term Evolution (LTE) networks. Unfortunately, this service always is suffered from the growing of security threats. In the Inter-eNB handover, an attacker may exploit these threats to violate the user privacy and desynchronize the handover entities. Therefore, the authentication is the main challenge in such issue. This paper proposes a synchronous authentication scheme to enhance the security level of key management during Inter-eNB handover process in LTE networks. The security analysis proves that the proposed scheme is secure against the current security drawbacks with perfect backward/forward secrecy. Furthermore, the performance analysis in terms of operations cost of authentication and bandwidth overhead demonstrates that the proposed scheme achieves high level of security with desirable efficiency.**

Keywords—LTE network; X2 handover; horizontal and vertical key derivations; desynchronizing attack

I. Introduction

In order to enhance the quality of service (QoS) with higher data rate in third generation (3G) networks, the Third generation partnership project (3GPP) has been developed the LTE network [1]. Therefore, the network architecture has been restructured to provide sufficient services by increasing bandwidth, enhancing performance, supporting heterogeneous connections with the other IP-technology and enhancing security level [4].

The main components of the LTE network architecture can be summarized as the following. The User Equipment (UE) connects to the Evolved Packet Core (EPC) through the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The latter component includes a set of Evolved NodeB (eNBs). The eNB is a base station that modulates and demodulates the signals to perform the radio communications between the UEs and EPC. The latter includes the Home Subscriber Serve (HSS), Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), Authentication Center (AuC) and Policy Charging Rules Function (PCRF) [7].

Data is transmitted between the eNBs and the P-GW through the S-GW. The P-GW connects the network with the outside IP networks. The PCRF recognizes the policies of QoS and the network resources. The HSS contains the AuC to fetch the user identifier and the pre-loaded shared key as well as to perform the key derivation functions during the authentication sessions. The MME interacts with HSS for user authentication and mobility management.

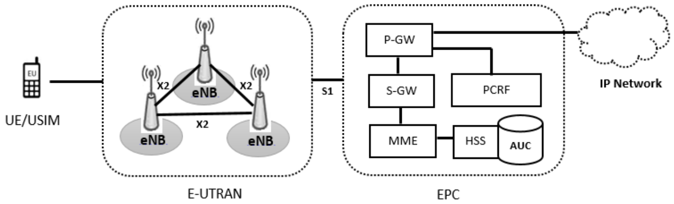

Fig. 1. LTE Network architecture.

The S1 interface connects the eNBs with the MME while the eNBs communicate with each other through X2 interface. Fig. 1 shows the LTE network architecture.

The improvement of mobility management is an essential process in LTE networks especially in the handover service which is requested by subscriber more frequently than other services in LTE networks. The security service is considered the main critical section in such improvement. This paper concentrates on the security drawbacks of the Inter-eNB handover and key management of LTE networks during the handover process.

When the UE moves away from the Serving eNB, the handover process should be performed to connect the UE with the Target eNB during the active session without service termination. In the LTE network, the air interface includes two different handover types, the X2 handover and S1 handover [5].

In the Inter-eNB handover (called X2 handover), both of the Serving eNB and the Target eNB are connected directly though the X2 interface. However, if the X2 interface does not exist between the Serving eNB and the Target eNB, or the Serving eNB initiates the handover process towards a particular Target eNB via the S1 interface, the S1 handover will be executed. In the S1 handover, both of the Serving eNB and the Target eNB are connected indirectly though the MME over the S1 interface.

Considering the Inter-handover, the Serving eNB sends the authentication parameters with session key to the Target eNB though the X2 interface directly, the mutual authentication does not exist between the Serving eNB and Target eNB which will be vulnerable to be attacked [16]. The UE exchanges the authentication parameters with the Serving eNB and Target eNB as clear text. Therefore, an adversary easily can catch these parameters. This is open the door for several drawbacks, an adversary can masquerade as a legitimate eNB to send an authentication messages by utilizing valid identities and authentication parameters, this is known as a rogue base station attack [2], [22]. Moreover, the MME provides the Serving eNB through S1 interface the recent parameters as clear text to generate a new session key to perform the handover process with the UE [3]. Subsequently, once the adversary acquires these parameters, the adversary using a rogue base station can disrupt and modify the refresh values of the authentication parameters, this is known as the desynchronizing attack [6], [10].

The handover process should be more secured against the current drawbacks in LTE networks. Therefore, the authentication is an important part in the handover process. Considering these security weaknesses, this paper proposes a synchronous authentication scheme to enhance the security level of key management during Inter-handover process in LTE networks.

The proposed scheme can overcome the existing drawbacks such as a rogue base station attacks, desynchronization attacks, replay attack and redirection attacks. Furthermore, the performance analysis in terms of operations cost of authentication and bandwidth overhead demonstrates that the proposed scheme achieves high level of security with desirable efficiency comparing with existing handover key management schemes.

This paper is organized as follows: Section 2 reviews the current handover authentication scheme. In Section 3, the related works is discussed. The proposed scheme is introduced in Section 4. The security and performance analysis of the proposed scheme are demonstrated in Sections 5 and 6, respectively. Finally, this paper will be concluded in Section 7.

II. LTE Handover Authentication Scheme

In this section, the Key hierarchy of LTE networks is illustrated, then the X2 handover process is reviewed. Finally, the security drawbacks of the X2 handover are discussed.

A. *Key Hierarchy in the LTE Network*

To minimize the security threats, the design consideration of the LTE networks not just separates between signaling and user data traffic but also separates the key management for encryption, integrity and handover protection [1], [8], [13].

TABLE I. Key Hierarchy of the AKA Protocol of LTE Network

Authentication entities	**Keys**
UE, HSS	root key K
UE, HSS	CK, IK
UE, MME, HSS	Local root key KASME
UE, eNB, MME	KeNB
UE, source eNB, target eNB	KeNB*

Table 1 illustrates the key hierarchy of the Extended Authentication and Key Agreement protocol (EPS-AKA) that is deployed in the LTE network [11], [18] and [19]. The root key (K) is used by the UE and the HSS to derive both of the Cipher key (CK) key and the Integrity key (IK) key. When the mutual authentication between the UE and the HSS is completed, both of the UE and the HSS derive the local root key (KASME) by binding the CK, IK with MME identity to the key derivation function (KDF) function, then HSS forwards the KASME to the MME. Furthermore, the (KeNB) key is derived key from KASME key by the UE and the MME, then the MME sends the KeNB to the eNB. The KeNB key is specified to encrypt the traffic between the UE and the eNB. Finally, based on the KDF function, the KeNB is used by the UE and the eNB to derive KeNB*, the source eNB forwards the KeNB* to the target eNB during the handover process.

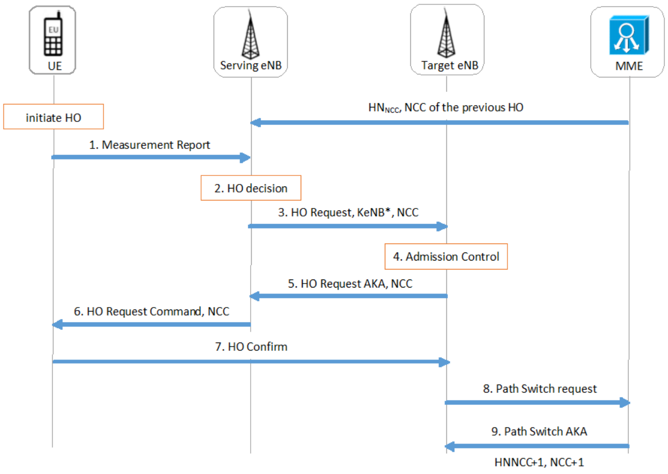

Fig. 2. X2 handover process.

B. *X2 handover process*

In LTE network, when a UE moves away from the Serving eNB, the handover process should be performed to connect the UE with the Target eNB without interrupting the active session. In the X2 handover, the Serving eNB sends the KeNB* to the Target eNB [2], [20], [21]. This process includes several steps that are shown in Fig. 2.

To initiate the handover process, the UE sends a measurement report to the Serving eNB which includes the information that is related to the neighboring eNBs to specify the Target eNB (Step 1). The Serving eNB analyses the measurement report to decide if the handover is necessary and to choose the best Target eNB. The Serving eNB derives the KeNB*, then transmits the handover request message with the KeNB* and Next Hop Chaining Counter (NCC) value to the Target eNB though X2 interface (Steps 2 and 3). In order to ensure if the resources is available to serve new UE, the Target eNB performs the admission control process, then sends the handover request acknowledgement to the Serving eNB, this message includes the NCC parameter to connect the UE with the target eNB (Steps 4 and 5).

$$\text{NH0} = \text{initial value of the KeNB}$$
$$\text{NH1} = \text{KDF (KASME, HH0)}$$
$$\text{NH2} = \text{KDF (KASME,NH1)}$$
then
$$\text{NHNCC} = \text{KDF}\left(\text{KASME,NHNCC-1}\right) \quad (1)$$

$$\text{KeNB*} = \text{KDF}\left(\text{NHNCC, PCI, EARFCN-DL}\right) \quad (2)$$

$$\text{KeNB*} = \text{KDF}\left(\text{KeNB, PCI, EARFCN-DL}\right) \quad (3)$$

The serving eNB sends the handover request command to the UE with the NCC that has been transmitted from the Target, after that the UE sends a confirmation message back to the Target eNB as a new serving eNB (Steps 6 and 7).

To achieve the forward key secrecy during the handover process, the Next Hop key (NH) value can be derived using the KDF function as defined in (1). The Serving eNB has fresh values of NHNCC key and NCC that have been sent from the MME during the previous handover session, the value of NHNCC means that the NH key is refreshed NCC times [1], [12]. Using the Physical Cell Identity (PCI) and E-UTRAN Absolute Radio Frequency Channel Number on the Download (EARFCN-DL), the UE and Serving eNB can derive the KeNB* from the NHNCC or from current KeNB as defined in (2) and (3), respectively.

Subsequently, the UE verifies the value of NCC that have been received from the Target eNB. In case, the received NCC is matched with the current NCC that is association with the previous handover session (i.e., NCC-1), then the UE derives the KeNB* using vertical key derivation as defined in (2), where a new value of NHNCC is derived from the previous value of NHNCC-1 and KASME key as defined in (1).

In case, the received NCC is greater than the current NCC that is association with the previous handover session, the UE using the current value of KeNB performs the horizontal key derivation to derive the KeNB* as defined in (3).

The new serving eNB (Target eNB) sends the S1 path switch request message to the MME through S1 interface (Step 8). Upon receiving the path switch request, the MME derives the fresh NH key and NCC values, then the MME sends S1 path switch request acknowledgement message back to the new Serving eNB, this message includes the NHNCC+1and NCC+1 next handover (Step 9).

C. Security Drawbacks of the X2 Handover

In despite of the key hierarchy system in LTE network performs more security level by supporting the backward/forward key separation features. The current X2 handover process is suffered from different drawbacks. The session keys and handover parameters are exchanged between handover entities as clear text without protection. The UE and the Serving eNB does not authenticate by the Target, and the user identity is exchanged between the handover entities without concealing.

In order to catch and modify the authentication messages that are exchanged between the handover entities, an adversary can use a rogue base station to masquerade as a legitimate eNB [21]. Subsequently, an adversary can forward modified NCC values between the handover entities by utilizing valid identities.

Therefore, an adversary can leave the Target eNB desynchronized and the session keys of the next handover processes vulnerable to compromise, then the adversary can decrypt all messages between the UE and eNB, this is known as the desynchronizing attack [10], [20].

When the NCC that sent from the MME is modified, an adversary forces the Target eNB to drive the KeNB* based on the current KeNB* using the horizontal key derivation. In the same manner, when the adversary changes the NCC value that sent to the Target eNB from the Serving eNB to be extremely larger than the original NNC value, the KeNB* will be derived using the horizontal key derivation. Consequently, forward key separation feature is disrupted and the future sessions keys of next hops will be compromised until the KASME key is recomputed during the next EPS-AKA execution.

III. Related work

There have been many researches on the authentication handover scheme of LTE networks.

In 2014, Han and Choi [10] propose a scheme to overcome the desynchronization attack of the handover process in the LTE network. An algorithm to derive the key based on specific minimal interval time has introduced. However, the scheme does not prevent the desynchronization attack and the communication overheads have increased.

Haddad et al. [9] introduce a secure and efficient handover scheme for the LTE-Advanced (LTE-A) network. The scheme classifies the eNB into two types, the eNB that is operated by the subscriber and the eNB that is operated by the network provider. The authors demonstrate different handover scenarios using uniform authentication scheme to thwart well-known attacks. The proposed scheme uses asymmetric key technique to perform the authentication between the communication entities rather than the symmetric key technique that is used in the current used scheme. However, it also cannot provide enough security.

In 2015, Lin et al. [15] pointed out that the X2 handover mechanism of LTE network has some security drawbacks. The first drawback is that the source eNB and UE are not authenticated by the target eNB. The second is that the attacker can modify the NCC and cause the desynchronizing attack. To overcome these vulnerabilities, Lin et al propose a scheme based on pre-loaded shared group key between all eNBs and MME. The scheme, however, does not resolve the current drawback issues in defeating desynchronization attack, repay attack and redirection attack.

In 2016, Khairy et al. [12] propose a new authenticated key management scheme for intra-MME handover. Hence, the MME is used as a third party and the source eNB is keeping out from the key management process to overcome the desynchronization attack. The scheme uses the pre-shared key for each eNB to protect the handover parameters between the eNBs and the MME. Hence, the mutual authentication between handover entities is partially achieved. Unfortunately, the proposed scheme increases the communication overheads of handover process.

Mathi and Dharuman [17] design a scheme to prevent the desynchronization attack due to rogue base station in handover key management of 4G LTE network. The proposed scheme generates a new key for future communication between the Target eNB and UE after the Target eNB is verified by the MME. However, similar to current handover key management scheme, the proposed scheme is not suitable to protect the handover process due to lack of the backward/forward keys separation and mutual authentication between handover entities.

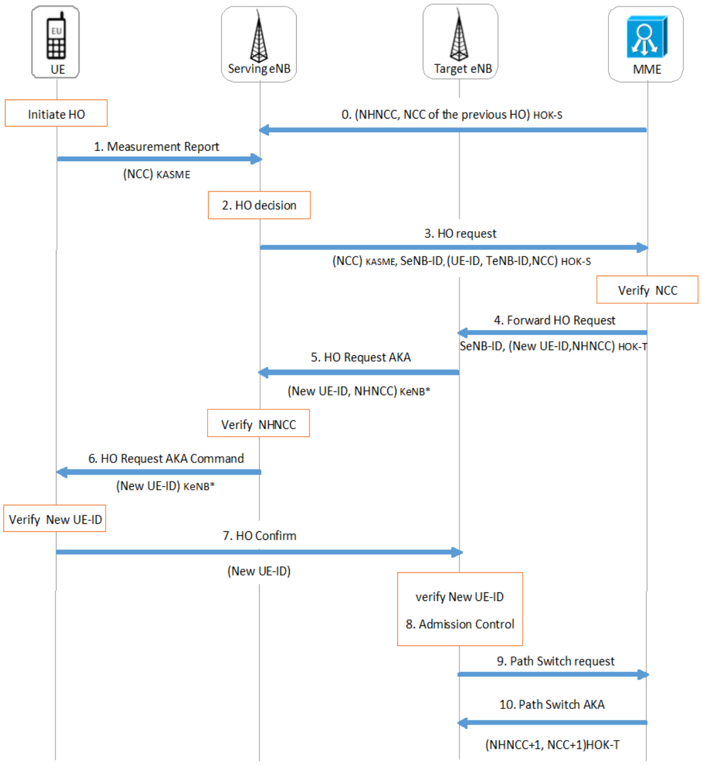

Fig. 3. Proposed X2 handover process.

IV. Proposed Scheme

This section introduces a synchronous authentication key management scheme for Inter-handover over LTE networks. In the current handover key management scheme, an attacker can catch the KeNB key that is sent from the MME to the Serving eNB, then an attacker forces the handover entities to derive the new session key KeNB* using the horizontal key derivation based on the current session key (KeNB). Therefore, the forward Keys separation feature is disrupted.

One of the main goals of the proposed scheme is to keep the forward Key separation feature by continuous the synchronization between all the handover entities. Therefore, just the vertical key derivation will be used with a fresh NHNCC key value to derive KeNB*. The pre-loaded shared key for each eNB with MME (HOK) is used in the proposed scheme to protect the handover parameters that are exchanged between MME and eNBs. Fig. 3 illustrates the proposed scheme according to the following.

The UE initiates the handover process by sending the measurement report to the Serving eNB, this message contains the encrypted NCC value using KASME key (Step 1). Through measurement report, the Serving eNB decides that the handover is necessary or not. The Serving eNB chooses the best Target eNB according to the measurement report (Step 2).

The Serving eNB sends the handover request message to the MME through S1 interface for performing the handover process. The message contains the encrypted NCC that has been sent by the UE along with the identity number of the Serving eNB (SeNB-ID). The message also contains a set of encrypted authentication parameters using the pre-loaded key of Serving eNB (HOK-S). The encrypted authentication parameters includes the identity number of the UE (UE-ID), identity number of the Target eNB (TeNB-ID) and the NCC value that has been received by the Serving eNB from the MME during last handover session (Step 3).

Upon receiving the handover request message, the MME decrypts the UE-ID, TeNB-ID and NCC that have been added by the Serving eNB, then fetches the KASME key of the UE to decrypt NCC value that has been sent from the UE through the serving eNB. In case, both NCC values are not equal, the handover request will be rejected by the MME. Otherwise, MME fetches the NHNCC that is associated with the NCC value, then calculates the new UE-ID. According the TeNB-ID, the MME fetches the pre-loaded key of the Target (HOK-T) to encrypt the NHNCC and the new UE-ID. After that, MME forwards the handover request message along with the encrypted values of NHNCC and the new UE-ID over S1 interface to Target eNB (Step 4).

Upon receiving the handover request message, the Target eNB checks that it has a resource for the handover process. The Target eNB decrypts the NHNCC and new UE-ID, then derives the new KeNB* from the received NHNCC as defined in (2). The Target eNB sends the Handover request acknowledgement to the Serving eNB over X2 interface. This acknowledgement includes the encrypted value of the NHNCC and the new UE-ID using the new session key KeNB* (Step 5).

The Serving eNB decrypts the NHNCC using the KeNB*, then authenticates the acknowledgement message by comparing the NHNCC value that has been received from the MME with the NHNCC value that has been received from the Target eNB. In case, both values are not equal, then the Serving rejects the handover process. Otherwise, the Serving eNB sends the handover request acknowledgement command message to the UE along with the encrypted value of a new UE-ID (Step 6).

The UE derives the new session key KeNB* as defined in (2) to decrypt the new UE-ID that has been received from the Target eNB. In order to verify the new UE-ID, the UE calculates the new UE-ID in the same way in the MME. The UE compares between both values, if are not equal, then UE rejects the handover process, else sends handover confirmation message along with the new UE-ID over X2 interface to the Target eNB. This message announces that the handover process has been successful (Step 7).

Upon receiving the handover confirmation message, the Target eNB compares the new UE-ID that has been received from UE with the decrypted UE-ID value that has been received from MME, if the both values are not equal, then the Target rejects the handover process, else the Target eNB is becoming the new Serving eNB (Step 8). Through this step, the Target eNB authenticates the UE and indirectly authenticates the Serving eNB and the MME. After admission control process, the Target eNB sends the S1 Path Switch Request to the MME over S1 interface to the MME. Through this message, the new Serving eNB notifies the MME to change the

UE location and requests the switch path towards the new Serving eNB (Step 9).

Upon receiving the path switch request, the MME calculates the fresh values NHNC and NCC, then the MME sends S1 path switch request acknowledgement message back to the new Serving eNB, this message includes the encrypted fresh values of the (NHNCC+1) that is computed as defined in (1) and NCC+1 by the HOK-T of next handover (Step 10).

V. Security Analysis

In this part, the security analysis is conducted to demonstrate that the proposed scheme has attractive security features during the Inter-handover process. In addition to, explain how the enhancements of the proposed scheme can resist the current drawbacks.

The same security architecture of the current handover key management scheme is used in the proposed scheme. Moreover, the proposed scheme uses the same authentication parameters and functions to enhance the security level of the handover process to be more secure against the current drawbacks as the follows:

A. Mutual Authentication

The mutual authentication feature can be performed between all handover entities in the proposed scheme during the Inter-handover process. More precisely, the MME authenticates the UE and the Serving eNB by verifying the NCC values that have been sent from the UE and the Serving eNB.

Indirectly, the Target eNB authenticates the MME, Serving eNB and UE by verifying the new UE-ID values that has been sent through the serving eNB and has been computed by the MME and UE. The Serving eNB can authenticate both of the MME and Target eNB by comparing the NHNCC value that has been sent from the MME in previous handover session with the NHNCC value that has been sent from the Target eNB. In the same manner, the UE authenticates the MME, Serving eNB and Target eNB by comparing the computed new UE-ID with the new UE-ID that has been encrypted by the Target eNB.

Therefore, the mutual authentication is achieved between all handover entities while in current handover scheme the Target does not authenticates the Serving eNB and UE.

B. Key Backward/Forward Security

The proposed scheme depends on the secrecy of the pre-loaded shared key of the eNB (HOK) with the MME that is used to encrypt the NCC and NHNCC values that are exchanged between the eNBs and the MME. The new session key KeNB* is never sent between the handover entities as in the current scheme. Instead, the KeNB* is derived locally using the vertical key derivation function by the Target eNB and UE.

In the proposed scheme, an adversary cannot reversely deduce the previous session key from the current session key due to using the same vertical key derivation function of the current handover scheme. Consequently, the proposed scheme satisfies one-hop key separation for Backward/Forward security. In contrast, the current scheme can achieve only two-hop forward security.

C. Anonymity

The proposed scheme changes the identity number of the UE (UE-ID) periodically. In each handover session, a new UE-ID will be computed by the UE and the MME. Subsequently, the user identity will be concealed in all next handover session between the user and network. Thus, through using fresh values of the NCC and UE-ID in all next handover sessions, the anonymity feature is hold in proposed scheme. In contrast, the same UE identity is used for all handover sessions in the current scheme.

D. Resistance to Attacks

In addition to, the attractive security features that are mentioned in previous sections, the proposed scheme can resist different attacks. Supposed an adversary can catch the handover messages between the handover entities, and can use a rogue base station to impersonate and control either the Serving eNB or the Target eNB. In the proposed scheme, an adversary cannot deduce the new session key parameters that are exchanged between the handover entities where all parameters are sent as encrypted messages. The NCC is sent to the Serving eNB as encrypted message from the UE using the KASME key. The NCC value that is sent to the MME from the Serving eNB also is encrypted by HOK-S. In same manner, the NHNCC is sent as encrypted message either through the S1 interface or X2 interface using the HOK-T and KeNB*, respectively. Therefore, the refreshing of the current NCC and NHNCC values cannot be disrupted by manipulating the message between handover entities, any change in the NCC or NHNCC, the handover process will be rejected by receipted entity.

In proposed scheme, handover process is performed through the MME, the Serving eNB sends the identity of the Target eNB as encrypted message to MME, the latter sends the Serving eNB identity to the Target eNB also as encrypted message. In addition to, the User identity is changed in each time the handover process is held. Therefore, if an adversary redirects or replays the handover messages to another eNB then handover process will be rejected. Consequently, the adversary cannot deduce the new session key or disrupt the refreshment of authentication parameters, also cannot reply or redirect the communication messages between the handover entities. Therefore, the drawbacks of the current scheme are eliminated, the proposed scheme can prevent the desynchronization attack, replay attack and redirection attack.

E. Comparisons

Table 2 shows that the proposed scheme achieves the highest security level among the other handover Key management schemes. In contrast, the current scheme achieves the lowest security level. As mentioned in previous sections, the proposed scheme provides several security features such as the mutual authentication between all handover entities, anonymity of the user, perfect Backward/Forward secrecy. Furthermore, the proposed scheme is secure against the desynchronization attack, replay attack and redirection attack.

TABLE II. SECURITY PROPERTIES AMONG THE HANDOVER SCHEMES

	Current HO	Lin et al. [15]	Khairy et al. [12]
Mutual Authentication	NO	NO	partially
Anonymity	NO	NO	Hold
Key Backward separation	One-hop	One-hop	One-hop
Key Forward separation	Tow-hop	One-hop	One-hop
Desynchronization attack	NO	Hold	Hold
Replay attack	NO	NO	partially
Redirection attack	NO	NO	partially
	Proposed HO	**Mathi and Dharuman [17]**	
Mutual Authentication	Hold	partially	
Anonymity	Hold	NO	
Key Backward separation	One-hop	One-hop	
Key Forward separation	One-hop	Tow-hop	
Desynchronization attack	Hold	No	
Replay attack	Hold	NO	
Redirection attack	Hold	NO	

VI. PERFORMANCE ANALYSIS

In this part, the performance analysis is discussed to observe the effect of security level enhancement in the proposed scheme during the X2 handover process.

The numerical results in terms of operations cost of authentication and bandwidth overhead are discussed by comparing the proposed scheme with different handover Key management schemes.

TABLE III. ASSUMPTIONS OF THE LTE NETWORK

Assumptions	Assumptions values
Mean density of UE/USIM ρ.	300/km2
Total number of UE/USIM.	2 × 49 × 300 = 29400
Size of MME Area.	49 km2
Average rate of originating service request.	1/hr/user
Average rate of terminating service request.	1/hr/user
Average speed of UE/USIM $\mathcal{V}$.	5 km/hr
Number of MME.	2 MMEs.
Number of TA.	128 TAs.
Number of the eNB in each TA	2, 3, 5 eNBs.
Border covered length ℓ.	30 km.

For bandwidth overhead consumption, the handover key management schemes have been simulated in MATLAB running on a 2.10 GHz processor with 4GB memory computing machine. Table 3 illustrates the assumptions of the LTE network.

A. Operations Cost of Authentication

TABLE IV. NOTATIONS OF THE OPERATIONS COST

Notations	Description
Cc	Encryption/ decryption cost
Kc	Key derivation cost
Vc	Verification cost
Gc	Generate new identifier cost
Rc	Refreshment parameter cost

Table 4 illustrates the notations of the operations cost in the authentication process. In this context, assume that the cost of all operations per hop are equal to 1 unit and the operations vector (O_V) in each entity of handover process can be determined as $[C_c, K_c, V_c, G_c, R_c]$, the O_V represents how many times the operations are executed in the handover entity.

$$V_{sum} = \sum O_v \ [C_c, K_c, V_c, G_c, R_c] \qquad (4)$$

The sum of operations vectors (Vsum) for all handover entities represents the operations cost of authentication in handover Key management scheme. Here, the (Vsum) is a vector defined as in (4).

TABLE V. OPERATIONS COST IN EACH HANDOVER ENTITIES

	UE	Serving eNB	Target eNB
Mathi and Dharuman [17]	[0, 1, 1, 0, 1]	[0, 1, 0, 0, 1]	[0, 1, 0, 1, 2]
Lin et al. [15]	[0, 1, 0, 0, 1]	[2, 1, 0, 0, 1]	[1, 0, 0, 0, 2]
Khairy et al. [12]	[4, 1, 3, 2, 0]	[2, 0, 0, 0, 0]	[5, 1, 2, 1, 0]
Current	[0, 1, 0 ,0, 0]	[0, 1, 0 ,0, 1]	[0, 0, 0 ,0, 2]
Proposed	[2, 1, 1, 1, 1]	[3, 0, 1, 0, 1]	[6. 1, 1, 0, 2]
	MME	**Vsum**	**Total of Vsum**
Mathi and Dharuman [17]	[0, 0, 1, 1, 2]	[0, 3, 2, 2, 6]	13 unit
Lin et al. [15]	[1, 0, 0, 0, 2]	[4, 2, 0, 0, 6]	12 units
Khairy et al. [12]	[8, 0, 0, 3, 0]	[21, 2, 5, 5, 0]	33 units
Current	[0, 0, 0 ,0, 2]	[0, 2, 0, 0, 6]	8 units
Proposed	[7, 0, 1, 1, 2]	[18, 2, 4, 2, 5]	31 units

The results in Table 5 show that the operations cost of authentication in the handover key management schemes increase with the increases of the security level. Therefore, if the security level has increased, then the number of operations will be increased, especially the encryption/decryption and verification operations. Compared with other handover key management schemes, the proposed scheme can achieve the highest security level with desirable authentication cost.

B. Bandwidth Overhead

Liang and Wang [14] classify the intra-domain handoff authentication request events. The numerical analysis is taken into account just the event that when the UE starts the request within current MME domain and this request ends before the UE moves to another MME domain.

$$\lambda_1=\lambda_u P_r(\lceil \overline{N}_a \rceil \text{-}1) \qquad (5)$$

Therefore, the arrival rate of handoff authentication requests (λ_1) can be calculated as in (5) [8], [14]. Where (λ_u) is the service request arrival rate, $\overline{N}_a$ is the average numbers of eNBs passed by the UE in the same MME domain and (P_r) is the probability that X2 handover happens.

$$T_{AP}=\sum_{i=1}^{6} Auth_i \qquad (6)$$

Let the authentication parameters size between (UE-Serving eNB), (UE-Target eNB), (UE-MME), (Serving eNB-Target eNB), (MME-Serving eNB), and (Target eNB–MME) be Auen1, Auth2, Auth3, Auen4, Auth5 and Auth6, respectively.

Therefore, the total size of authentication parameters (T_{AP}) that are exchanged between the handover entities is calculated as indicated in (6).

TABLE VI. TOTAL SIZE OF AUTHENTICATION PARAMETERS IN THE HANDOVER KEY MANAGEMENT SCHEMES

Handover schemes	**(T_{AP})**
Mathi and Dharuman scheme	2432 bits
Lin et al. scheme	2176 bits
Khairy et al. scheme	4224 bits
Current scheme	2176 bits
Proposed scheme	3456 bits

The total size of authentication parameters of the handover key management schemes, as depicted in Table 6, the proposed scheme , Khairy et al. [12] scheme and Mathi and Dharuman [17] scheme, consume during the handover key management (3456), (4224) and (2432) bits, respectively while, Lin et al. [15] scheme and the current scheme consume 2176 bits.

Therefore, the total size of authentication parameters of proposed scheme ranges in the middle. However, the proposed scheme is secure against various attacks and provides more security features than the other schemes.

$$T_{Bw}= 128 \times \left|(\lambda_1 \times T_{Ap})\right| \qquad (7)$$

Subsequently, the total bandwidth of the handover process (T_{BW}) for each handover Key management schemes is defined as in (7).

The effect of security level enhancement is shown in Fig. 4 and 5. These figures depict that the relationships between the bandwidth overhead during the handover process with authentication handover key management scheme when the $\overline{N}_a$ = 1 and $\overline{N}_a$ = 2, respectively.

Therefore, the total bandwidth overhead consumption increases with the increase of the security level. Compared with other handover key management schemes, the proposed scheme provides several security features with desirable bandwidth overhead consumption.

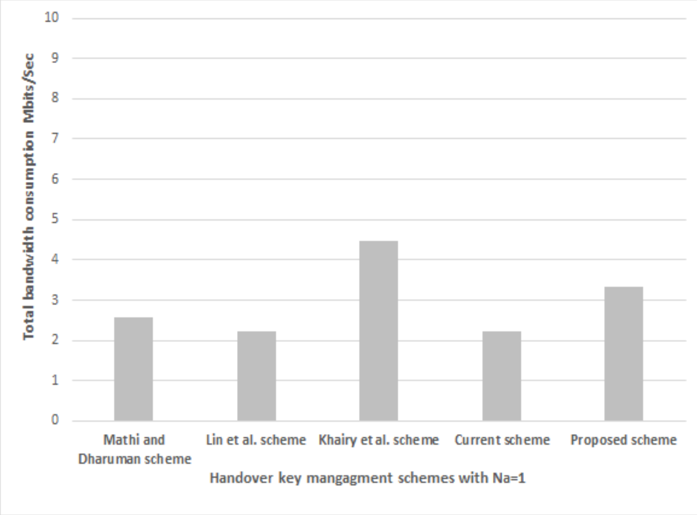

Fig. 4. Total bandwidth when ($\overline{N}_a$ = 1).

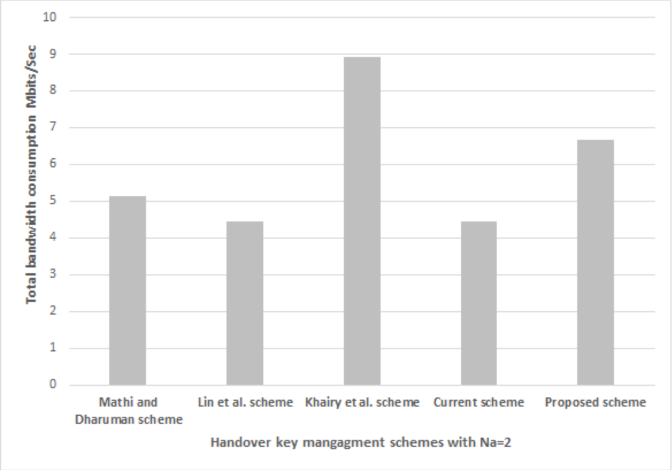

Fig. 5. Total bandwidth when ($\overline{N}_a$ = 2).

VII. CONCLUSION

This paper proposes a synchronous handover authentication scheme to prevent the drawbacks of the current handover key management scheme during Inter-eNB handover over LTE networks. Compared with other authentication handover key management schemes, the proposed scheme not only provides strong security features including perfect Backward/Forward secrecy and user anonymity but also the mutual authentication between all handover entities.

The security analysis has shown that the proposed scheme is secure against various attacks such the desynchronization attack, replay attack and redirection attack. The accurate performance analysis in terms of operations cost of authentication and bandwidth overhead has been discussed, which demonstrate that the authentication cost and bandwidth overhead consumption of the whole handover process are desirable among the other handover Key management schemes.

REFERENCES

[1] 3gpp-ts 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (2015-12), Release 11 Technical Specification.

[2] M. Abdeljebba, R. El Kouch, "Fast Authentication during Handover in 4G LTE/SAE Networks", Open Access IERI Procedia, Vol 10, pp. 11-18, 2014.

[3] P. Agarwal, D. Thomas, and Kumar. A, "Security Analysis of LTE/SAE Networks under De-synchronization Attack for Hyper-Erlang Distributed Residence Time", IEEE Communications Letters, Vol 21, No 5, pp.1055-1058, 2017.

[4] W. Ahmed, S. Anwar. and M. Arshad, "Security Architecture of 3GPP LTE and LTE-A Network: A Review", INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, Vol 7, No 1, 2016.

[5] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol 16, No 1, pp.283-302, 2014.

[6] E. El-Gaml, H. ElAttar, H. El-Badawy, "Evaluation of Intrusion Prevention Technique in LTE Based Network", International Journal of Scientific & Engineering Research, Vol 5, No 12, pp.1395- 1400, 2014.

[7] D. Forsberg, G. Horn, W. Moeller and Niemi. V, "LTE SECURITY", John Wiley and Sons, United Kingdom, 2013.

[8] F. Degefa, D. Lee, J. Kim, Y. Choi and D. Won, “Performance and security enhanced authentication and key agreement protocol for SAE/LTE network”, Computer Networks, Vol 94, pp. 145-163, 2016.

[9] Z. Haddad, M. Mahmoud, S. Taha, and I. Saroit, “Secure and Efficient Uniform Handover Scheme for LTE-A Networks”, In Wireless Communications and Networking Conference (WCNC), pp. 1-6 IEEE 2016.

[10] C. Han, H. Choi, “Security Analysis of Handover Key Management in 4G LTE/SAE Networks”’, IEEE Transactions on Mobile Computing, vol. 13, no. 2, pp. 457-468, 2014.

[11] T. Karpagam, S. Sivakumar, “Efficient and Secure Authentication Handover using Network functions virtualization”, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Vol 17, No 1, pp.36-40, 2015.

[12] K. Khairy, A. Diaa Eldien, A. Abdel-hafez and E. Abd El-Wanis, “Authenticated Key Management Scheme for Intra-Mme Handover Over LTE Networks”, International Journal of Research in Engineering and Science (IJRES), Vol, No 10, pp. 19-28, 2016.

[13] C. Lai, H. Li, R. Lu and X. Shen,”SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks”, Computer Networks, Vol 57, pp.3482-3510, 2013.

[14] W. Liang, W. Wang, “On performance analysis of challenge/response based authentication in wireless networks”, The International Journal of Computer and Telecommunications Networking, Vol 48, No 2, pp. 267-288, 2005.

[15] Y. Lin, W. Longhuang and C. Yang, “Enhanced 4G LTE Authentication and Handover Mechanism“, International Journal of Electrical, Electronics and Data Communication, Vol 3, No 9, pp.45-47, 2015.

[16] M. Masud, “Survey of security features in LTE Handover Technology”, Scientific Research Journal (SCIRJ), Vol, No 8, pp.27-31, 2015.

[17] S. Mathi, L. Dharuman, “Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme”, Open Access Procedia Computer Science, Vol 89, pp.170- 179, 2016.

[18] S. Nashwan, B. Alshammari, “Formal Analysis of MCAP Protocol Against Replay Attack”, British Journal of Mathematics & Computer Science, Vol 22, No 1, pp. 1-14, 2017.

[19] S. Nashwan, B. Alshammari, Mutual Chain authentication protocol for SPAN Transactions in Saudi Arabian Banking, International Journal of computer and communication engineering, Vol 3, No 5, pp. 326- 333, 2014.

[20] N. Qachri, O. Markowitch and J. Dricot, “A Formally Verified Protocol for Secure Vertical Handovers in 4G Heterogeneous Networks”, International Journal of Security and Its Applications, Vol 7, No 6, pp.309-326, 2013.

[21] B. Sridevi, D. Mohan, “Security analysis of Handover Key Management among 4G LTE entities Using Device Certification”, International Journal of Electrical, Computing Engineering and Communication, Vol. 1, No 2, pp. 1-7, 2015.

[22] P. Tayade, P. Vijaykumar, “A Comprehensive Contemplate on Security Aspects of LTE and LTE Advanced in Wireless Communication Network”, International Journal of Control Theory and Applications, Vol 10, No 31, pp.197-217, 2017.