**I J C T A**, 8(5), 2015, pp. 1823-1830


# A Time-invariant Scheme for Handover Key Management Using Identity based Encryption in 4G LTE Networks

**Lavanya Dharuman* and Senthilkumar Mathi****

***Abstract:*** The 4G Long Term Evolution (LTE) is used to provide continuous communication for the mobility based users with high data rate in 4G network. However, the security issues are of paramount importance and have been a recent research area in LTE. The desynchronization attack is one of the major security threats in LTE during handover key management that occurs when source node acts as a rogue base station in order to hijack the future session key. The paper addresses the vulnerability of desynchronization attack in 4G LTE and elucidates how the attack jeopardizes the communication. Also, the paper proposes a secured and efficient handover scheme in key management using identity based encryption to authenticate the participating principals in LTE before the node tries to communicate with the target base station. The scheme is validated using a model checker – AVISPA. The analysis of security and performance evaluation shows that the proposed scheme provides an enhanced security and significant reduction in the communication cost for authentication and key generation in LTE.

***Keywords:*** Authentication, Desynchronization, Confidentiality, Long term evolution, Internet protocol, Wireless networks.

## 1. INTRODUCTION

In recent years, there has been a tremendous growth in communication technology which led to increase in data usage. The evolution of network technology from third generation (3G) to fourth generation (4G) using LTE exists because of the additional services offered by 4G [1]. The LTE supports only packet-switched services. It aims to provide Internet Protocol (IP) connectivity between user equipment (UE) and the packet data network (PDN). The Evolved Packet System (EPS) network is the evolution of 4G/LTE standard introduced by 3rd Generation Partnership Project (3GPP) and it increases radio access technologies of the mobile networks to provide higher data rate to the users [2,3].

As shown in Fig.1, the EPS architecture is divided into two parts; they are evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and evolved packet core (EPC). The E-UTRAN comprises of Evolved Node B (eNodeB) and it provides the radio communications between the mobile 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 UE and provides temporary identity for the user. The Serving Gateway manages the user plane mobility and also maintains the data paths between the eNodeBs and the PDN Gateways. That 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). The handover occurs when the user moves from one cell to another cell. Here, the source eNodeB provides the K*eNB to eNodeB for the use of key after the handover.

* Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, Amrita University, Tamilnadu, India, *Emails: *dharmanlavanya@gmail.com*, **m_senthil@cb.amrita.edu

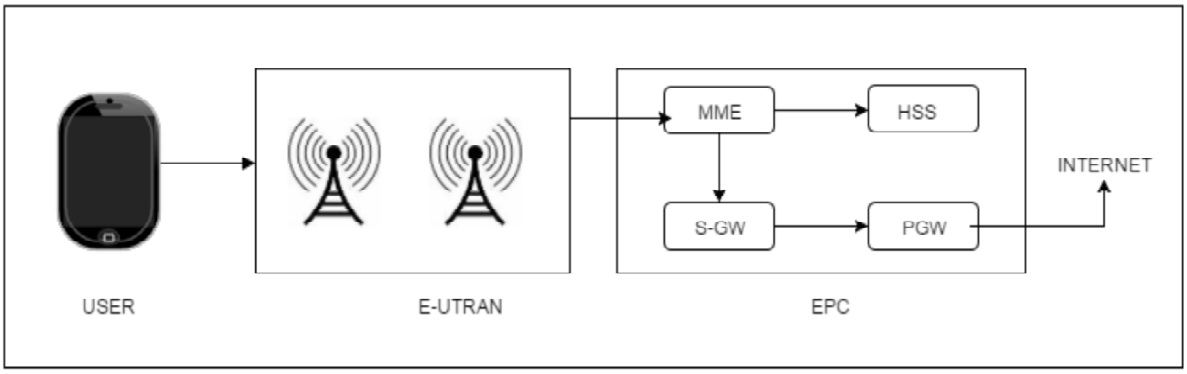


**Figure 1: EPS Architecture**

Considering the intra-MME handover, the source node provides key ($K^*_{eNB}$) to the target in the EPS architecture [4]. The source eNodeB forwards the NCC and *K*eNB* to the target assuming that it involves the vertical key derivation. Here occurs desynchronization attack which leads to the derivation of future session keys. To address these issues, the paper proposes a handover key management scheme in LTE using identity based encryption (IBE).

The IBE sends only partial private key to the node and in turn node has a partial value to calculate the private key. The private key is used to decrypt the nonce sent by HSS to authenticate the source node. The rogue source cannot predict the private key of the genuine source since it uses two partial key to generate the private key. Hence, the authentication of the source node using IBE cannot be compromised. The main contributions of this paper are: 1) to ensure authentication of eNodeB using IBE. 2) To prevent rogue base station this in turn avoids desynchronization attack. 3) The proposed scheme is verified using AVISPA – a model checker. 4) significant reduction in communication cost.

The paper is organized as follows: The related works are discussed in Section 2. Section 3 explains the proposed scheme and section 4 includes formal and informal security analysis. Section 5 discusses the performance evaluation based on the communication cost between the entities and provides conclusion in Section 6.

## 2. RELATED WORK

When the NCC value is set high by the rogue base station, it is desynchronized between the entities. As a result, it causes the desynchronization attack in the presence of rogue node. To overcome this, Chan-Kyu et al suggested a scheme for secure handover key management that introduces an optimal time to update the root key value [4]. Since, it depends on key interval time; there is a possibility for the attacker to perform the attack before the root key updation due to synchronization.

Furthermore, the handover key management using device certification by Sridevi et al suggested a technique that enhances security between the correspondent entities in LTE architecture. Here, it involves a new device called, certificate authority wherein all the entities of LTE have to be verified with their identity through the certificate chain [5] to ensure the genuineness of the communicants. 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 bottleneck to occur due to the centralized feature.

Subsequently, the handover key management based on ciphering key parameter by Xiao et al investigated a scheme [6] that includes an additional parameter known as cell radio network temporary identifier (C-RNTI) in the EPS architecture. Here, the UE sends handover request to source in turn the request message is forwarded with the key (K*eNB) and NCC to target. The target generates C-RNTI and sends it to MME. The enciphered C-RNTI by MME is sent to the target. On using the master key which is pre-

shared between UE and MME, they encrypt C-RNTI and the *K*eNB*. Nevertheless, the scheme uses too many communications between the entities; assume if target is the rogue then C-RNTI uses a false value, where communication between the source and the target can jeopardize.

The investigations [4, 5, 6, 7, 8, 9, 10, 11, 12, 13] have emphasized that, the prevention of security threats due to the rogue base station is lacking to provide authentication and mitigate the desynchronization attack between the communicants of the EPS architecture during handover key management. On illustrating and escalating from the earlier investigations, the present paper put forwards a scheme using the IBE to overcome rogue base station attack which paves the way for desynchronization attack in LTE handover key management. The next section discusses the proposed scheme.

## 3. PROPOSED SCHEME

The proposed scheme uses IBE to authenticate the source and target nodes. The IBE is a mechanism which distributes the partial private key to the entities without the intervention of the certificate authority [14]. It uses the private key generator (PKG) to distribute the partial private key and also it does not need a database to retrieve the keys. Consequently, it establishes a secured environment and ensures the authentication of the source and target nodes.

The intricacies of the proposed scheme are depicted in Fig 2. The proposed scheme incorporates IBE to prevent rogue base station during handover key management in LTE networks. During key management, the session key between the source and target are compromised by increasing the NCC value to its highest value, because of the failure in forward handover. The failure occurs when source enodeB becomes rouge base station; this in turn derives all possible session key which can be used for communication between source and target. But in the proposed scheme, the nonce is included to provide authentication to indicate that source is genuine. The nonce value is encrypted using the public key of the node and. The IBE includes PKG to distribute partial private key to the legitimate principals.

Initially, the HSS checks the NCC and nonce. Here, the nonce is equal but NCC is not equal due to the rogue base station. To check whether source is genuine, the HSS sends a new encrypted nonce (*E*

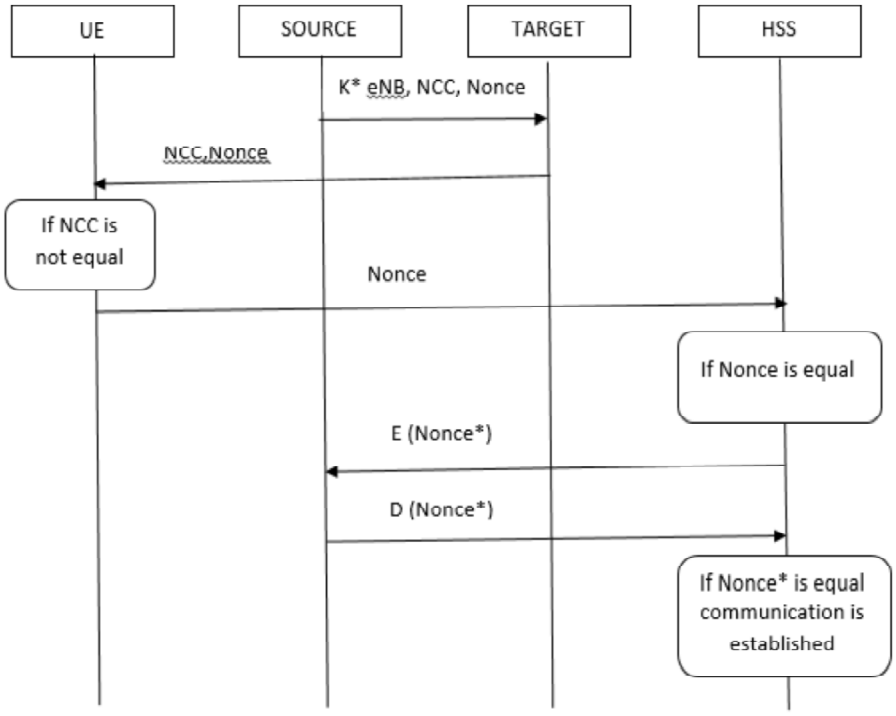


**Figure 2: Proposed scheme for handover key management in LTE**

*(Nonce*)*) using source public key. If the source is rogue, it cannot decrypt since it does not have the private key of the source. Thus, a rogue source can easily be prevented using IBE. As shown in Fig.2, the authentication is achieved to check whether source is rogue or genuine and desynchronization attack can also be prevented.

## 4. SECURITY ANALYSIS

This section includes the informal and formal discussion of the security issues of the proposed scheme.

### 4.1. Authentication

Authentication is the process of identifying the genuine user in the network. The proposed scheme involves nonce value to provide authentication to the source. It uses IBE to provide authentication to the source. Here, the IBE generates the partial private key from master key and distributes to the source node. Consecutively, the nonce from HSS is encrypted using source nodes public key. To authenticate, the source node necessitates the generation of the private key to decrypt the nonce (*Nonce**). Consequently, it requires the partial private key from the PKG in order to derive its complete private key. It is impossible for the rogue node to generate the private key using IBE mechanism. Hence, the proposed scheme provides authentication between all communicants without the intervention of attacker. Table 1 summarizes the comparative analysis of authentication.

**Table 1**
**Comparative analysis of authentication**

| *Scheme* | *Authentication* | | |
|---|---|---|---|
| | *UE-Source* | *Source-UE* | *Source-HSS* |
| Chan-Kyu et al 2014 | Yes | Yes | No |
| Sridevi et al 2015 | Yes | Yes | No |
| Xiao et al 2014 | Yes | Yes | No |
| Proposed | Yes | Yes | Yes |

### 4.2. Confidentiality

Confidentiality is the process of ensuring the reach of sensitive data only to the disclosed users. The proposed scheme uses IBE mechanism to authenticate the source node; in further process authenticated source generates the session key and sends to the target for the next handover. This key is used to encrypt the future communication between the target node and the user. The session keys are derived using the master key. Since all the communication between the user and base station is encrypted, our scheme provides confidentiality to the data. The comparative analysis of confidentiality is depicted in Table 2.

**Table 2**
**Comparative analysis of confidentiality**

| *Scheme* | *Confidentiality* | |
|---|---|---|
| | *UE-Source* | *Source-UE* |
| Chan-Kyu et al 2014 | Yes | No |
| Sridevi et al 2015 | Yes | No |
| Xiao et al 2014 | Yes | Yes |
| Proposed | Yes | Yes |

### 4.3. Integrity

Data Integrity refers to accuracy and consistency of the data during data transfer. In proposed scheme, the nonce value is encrypted using source public key and decryption is possible only with source node's private key. Thus the use of asymmetric key encryption ensures data integrity. Table 3 shows the comparative analysis of data integrity.

**Table 3**
**Comparative analysis of data integrity**

| *Scheme* | *Integrity* | | |
|---|---|---|---|
| | *UE-Source* | *Source-UE* | *Source-HSS* |
| Chan-Kyu et al 2014 | No | No | No |
| Sridevi et al 2015 | Yes | Yes | No |
| Xiao et al 2014 | Yes | Yes | No |
| Proposed | Yes | Yes | Yes |

### 4.4. Desynchronization Attack Prevention

In the existing system, the *NCC* values of the source is being changed when the source is rogue and thus results in desynchronization attack. During the authentication process, the source is being verified using IBE mechanism. This identifies the rogue node in the LTE network and reports to the HSS to exit the further communication with the rogue base station.

### 4.5. Replay Attack Prevention

The use of nonce value in the scheme keeps changing periodically. It is easy to identify the attacker who performs replay attack, since the nonce keeps changing periodically. Thus replay attack is avoided in our proposed method.

### 4.6. Formal Analysis Using Avispa

The Automated Validation of Internet Security Protocols and Applications (AVISPA) provide the platform for verifying security of the protocol. Here, the protocol specification is written in High Level Protocol Specification Language (HLPSL) [15]. Then, the HLPSL is translated using a translator called HLPSLIF into a low-level format, known as Intermediate Format (IF). The IF is given to the following back-ends of AVISPA for attack trace,

(1) OFMC – On the fly model – AVISPA uses four different backgrounds for the security check, one of them is OFMC and this combines two methods for analyzing security protocol.

(2) CL-ATSE – The Constraint Logic based Attack Searcher – This applies constraint solving, it is built in a modular way, which can handle algebraic functions in cryptography.The proposed scheme consists of four different roles for source node, target node, user and server. The HLPSL code is depicted in Fig 3. The validation of HLPSL of the proposed scheme for OFMC and CL-ATSE back end results are summarized in Fig 4. No revealed attacks were found from the results.

## 5. PERFORMANCE EVALUATION

This section discusses the performance evaluation of the proposed scheme with that of the existing scheme. The communication cost for the proposed scheme in terms of authentication and key generation is computed as follows, Communication cost for authentication in bytes = Source-Target + Target-UE + UE-HSS + HSS-Source + Source-HSS = 305 bytes. Fig 5 shows the comparison results of four schemes in terms of

```
role se(UE,SE,TA,HSS: agent,
        SEPUK,TAPUK,HSSPUK: public_key,
        SK: symmetric_key,
         HASH: hash_func,
               SND,RCV: channel(dy))
        played_by SE def=
        local KENB,NCC,SENN,SEPUB: text , State: nat
        init State :=0
        transition
        0.State = 0 /\ RCV(start)
          =|>State' := 3 /\ KENB' :=new() /\ NCC' :=new() /\ SND(KENB'.NCC')
        3.State = 3 /\ RCV(HASH(SENN').{SENN'}_SEPUK)
        =|>State' :=  7 /\ SND(HASH(SENN').{SENN'}_SEPUK) /\ secret(SENN',senn,{SE,HSS})


end role

role ta(UE,SE,TA,HSS:agent,
        SEPUK,TAPUK,HSSPUK: public_key,
        SK: symmetric_key,
         HASH: hash_func,
                SND,RCV: channel(dy))
        played_by TA def=
        local KENB,NCC,SENN,SEPUB: text, State: nat
        init State := 1
        transition
        1.State = 1 /\ RCV(KENB'.NCC')
            =|>State' := 5 /\ SND(NCC')


end role
```

**Figure 3: Role definitions for source and target node in HLPSL**

| % SPAN 1.6 - Protocol Verification : paper.hlpsl | % SPAN 1.6 - Protocol Verification : paper.hlpsl |
|---|---|
| File | File |
| SUMMARY<br>SAFE<br><br>DETAILS<br>BOUNDED_NUMBER_OF_SESSIONS<br>TYPED_MODEL<br><br>PROTOCOL<br>C:\progra~1\SPAN\testsuite\results\paper.if<br><br>GOAL<br>As Specified<br><br>BACKEND<br>CL-AtSe<br><br>STATISTICS<br><br>Analysed : 0 states<br>Reachable : 0 states<br>Translation: 0.03 seconds | % OFMC<br>% Version of 2006/02/13<br>SUMMARY<br>SAFE<br>DETAILS<br>BOUNDED_NUMBER_OF_SESSIONS<br>PROTOCOL<br>C:\progra~1\SPAN\testsuite\results\paper.if<br>GOAL<br>as_specified<br>BACKEND<br>OFMC<br>COMMENTS<br>STATISTICS<br>parseTime: 0.00s<br>searchTime: 0.09s<br>visitedNodes: 45 nodes<br>depth: 6 plies |

**Figure 4: Protocol verification – OFMC and CL-ATSE backend results**

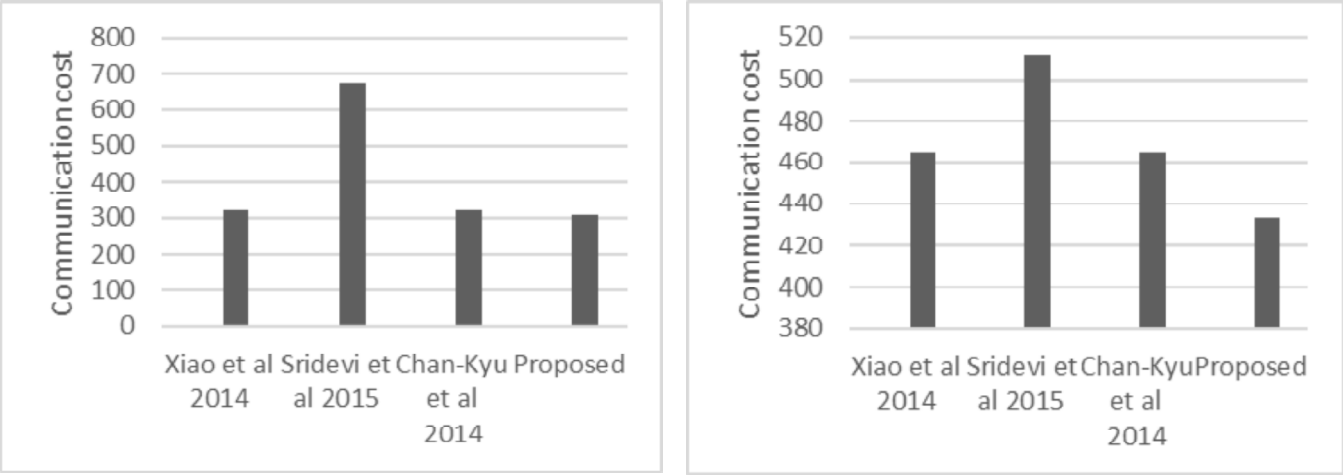


**Figure 5: Communication cost for authentication and key generation**

communication cost. The proposed schemes communication cost is lower than the Chan-kyu's et al scheme. Sridevi et al suggested digital certificate which costs higher than the other schemes. Hence, it is noted that the communication cost of the proposed scheme for authenticating the communicants of the LTE is comparatively less than other schemes.

The communication costs for key generation between entities are depicted in Fig 5. The communication cost for proposed work is calculated as follows, Communication cost for key generation in bytes = Source-Target + Target-UE + UE-HSS + HSS-Source + Source-HSS = 433 bytes. The proposed scheme shows low communication cost for key generation (see Fig 6) since there is no certificate authority and new entity C-RNTI.

## 6. CONCLUSION

In this paper, the proposed scheme uses IBE to prevent desynchronization attack and replay attack in handover key management of LTE. The security analysis of the proposed scheme using AVISPA shows that no revealed attacks were found from the results. From the numerical analysis, it is noted that the proposed scheme outperforms the existing in terms of communication cost for authentication and key generation.

## *References*

[1] Mohapatra S.K., Swain B.R. and Das P., "Comprehensive survey of possible security issues on 4g networks." *International journal of network security & its applications*, 7(2), 61, 2015.

[2] Wang J., Zhang Z., Ren YLiB and Kim JU., "Issues toward Networks Architecture Security for LTE and LTE-A Networks." *International Journal of Security and Its Applications*, 8(4), 17-24, 2014.

[3] Barth U., "3GPP Long-Term Evolution/System Architecture Evolution Overview." Alcatel White Paper, 2006.

[4] Han C.K. and Choi H.K., "Security analysis of handover key management in 4G LTE/SAE networks." *Mobile Computing, IEEE Transactions on*, 13(2), 457-468, 2014.

[5] Xiao Q., Cui B and Li L., "An Enhancement for Key Management in LTE/SAE X2 Handover Based on Ciphering Key Parameters." *In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on pp*. 256-261. IEEE, 2014.

[6] Sridevi B. and Mohan D., "Security analysis of Handover Key Management among 4G LTE entities Using Device Certification", 2015.

[7] El-Gaml E.F., ElAttar H. and El-Badawy H.M.,"Evaluation of Intrusion Prevention Technique in LTE Based Network."

[8] Choudhary A. and Bhandari R.,"Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network."

[9] Mathi S. and Anbarasi P.N.,"A Secure and Efficient Location Update Scheme for Next Generation Proxy Mobile IP in Distributed Environment." *Procedia Computer Science*, 57, 942-951, 2015.

[10] Mathi S., Lavanya M. and Priyanka R., "Integrating Dynamic Architecture with Distributed Mobility Management to Optimize Route in Next Generation Internet Protocol Mobility." *Indian Journal of Science and Technology*, 8(10), 963-974, 2015.

[11] https://en.wikipedia.org/wiki/System_Architecture_Evolution. [Accessed on Nov 2015].

[12] Vidya K and Mathi S., "Security Enhancement of Handover Key Management Based on Media Access Control Address in 4G LTE Networks". *In Proceedings of IEEE International Conference on Computational Intelligence and Computing Research* pp. 868-872, 2015.

[13] Anbarasi P.N. and Mathi S.,"A Tokenized Binding Update Scheme for Next Generation Proxy IP Mobility." *In Artificial Intelligence and Evolutionary Computations in Engineering Systems*, S.S. Dash et al, Ed., India, Springer, Volume. 394, 2015.

[14] Chatterjee S. and Sarkar P., "Identity-based encryption. Springer Science & Business Media", 2011.

[15] Armando A., Basin D., Boichut Y., Chevalier Y., Compagna L., Cuéllar and Mödersheim S., "The AVISPA tool for the automated validation of internet security protocols and applications". *In Computer Aided Verification* (pp. 281-285). Springer Berlin Heidelberg, 2005.