A secure and effective scheme providing comprehensive forward security to LTE/SAE X2 handover key management

Bangyi Sun, Jianfeng Chu, Liang Hu, Hongtu Li and Guangkun Shi
College of Computer Science and Technology, Jilin University, Changchun, Jilin
[e-mail: sunby15@mails.jlu.edu.cn,shigkjlu@163.com]
*Corresponding author: Guangkun Shi

Received November 2, 2016; revised March 12, 2017; accepted April 9, 2017; published September 30, 2017

Abstract

The commercialization of LTE/SAE technologies has begun a new era in which data can be transmitted at remarkably high rates. The security of the LTE/SAE network, however, remains problematic. The forward security in LTE/SAE X2 handover key management can be threatened by key compromise and de-synchronization attacks as base station in public spaces can be compromised. This study was conducted to address the lack of forward key security in X2 handover key management in scenarios in which an adversary controls a legal base station. We developed the proposed X2 handover key management by changing the parameter in the renewing step and adding a verification step. We compare the security and performance of our proposal with other similar schemes. Our enhancement scheme ensures forward separation security accompanied by favorable signal and computation load performance.

Keywords: X2 handover, forward security, LTE/SAE

This work is funded by: European Seventh Framework Program (FP7) under Grant No. GA-2011-295222, and by National Natural Science Foundation of China under Grant No. 61073009, and by National Sci-Tech Support Plan of China under Grant No. 2014BAH02F03.

https://doi.org/10.3837/tiis.2017.09.023 **ISSN : 1976-7277**

1. Introduction

The rapidly increasing demand for diverse data applications made Long Term Evolution (LTE)/System Architecture Evolution (SAE) one of the most common fourth-generation cellular networks worldwide [1][2]. LTE/SAE has effectually transformed the 3G, packet-switching network into an all-IP architecture system providing high performance as well as high data transmission rates. In LTE/SAE, the support of handover from the source base station to a target station in the access network provides seamless access to multiple services with negligible latency [3][4]. Notable security problems have emerged alongside the continuous improvements in these technologies. The 3GPP committee has specified security procedures on handover in EUTRAN to ensure a secure communication between user equipment (UE) and evolved NodeB (eNodeB) including a handover key management mechanism. Vulnerabilities yet exist in current handover procedures, as any external eNodeB may be compromised by physical, host, and network protocol vulnerabilities. Key compromise is one such threat, through which attackers can obtain keys and calculate session keys in subsequent handover processes after breaching the eNodeB. The other most common threat is de-synchronization attack, which is executed by manipulating the handover request message through the compromised eNodeB to disrupt updating of key refresh material and force session key derivation in a calculable direction. Attackers can also implement de-synchronization attack via a man-in-the-middle attack between the target eNodeB and core network; this is readily preventable by the application of IPsec, however [5]. Although LTE handover key management generally includes a key chaining architecture that refreshes the key materials in wireless encryption, attackers can obtain subsequent keys [6] and sabotage forward security [7].

Li [8] and Xiao [9] considered enhancing X2 handover key management in regards to lacking forward security. Li [8] rearranged the message flow of the X2 handover process to make the derivation of new keys between the UE and target eNodeB (K_{eNB}^*) occur in the target eNodeB directly. This eliminates risk when key compromise does happen, but does not protect forward security when de-synchronization happens. Xiao [9] attempted to make one of key parameters invisible to the source eNodeB by transferring it in cipher text; this approach prevents the source eNodeB from obtaining sufficient key material to renew K_{eNB}^* and secure the current key between the UE and target eNodeB in any case. The approach is impractical, however, as it necessitates two extra messages in the busy interface and excessive computation in the core network. Han [5] and Eman [10] discussed how network operators can determine an optimal interval for updates to protect the LTE network from de-synchronization attacks, but could not identify an ideal remedy for current problems in handover key management. Dan [11] showed that key separation is ensured in LTE X2 handover within the session key context. This scheme requires that the key hierarchy of LTE/SAE be reconstructed, however. Qachra[12] designed a general handover procedure for wireless networks and were able to verify the security when a source access point was compromised. In applying this scheme in LTE, the UE cannot begin a new handover process to another eNodeB if the current handover process is not complete (e.g., if there is a network delay or in a high-speed rail). In short: Complete forward security remains elusive, and there is much meaningful work to be done.

In this paper, we first introduce background knowledge in LTE/SAE architecture related to handover key management. We then describe key chaining architecture and message flow in the current X2 handover process as well as problems related to its capability. We then propose a new scheme designed to solve these problems. We analyze the security and performance of several similar schemes and discuss them in comparison to proposed scheme. Our proposed scheme is assessed on the basis of a formal framework called Proverif.

The remainder of this paper is organized as follows. Section 2 contains an introduction to the fundamentals of LTE/SAE architecture, including key hierarchy and the key chaining and message flow in the X2 handover process. In Section 3, we present our scheme for X2 handover key management enhancement. In Section 4 we analyze the security of our scheme and two other enhancement schemes, and give a formal verification of our our scheme; in Section 5, we analyze their respective performance. Section 6 provides a brief summary of the study and our conclusions.

2. Prerequisite knowledge

2.1 LTE/SAE architecture

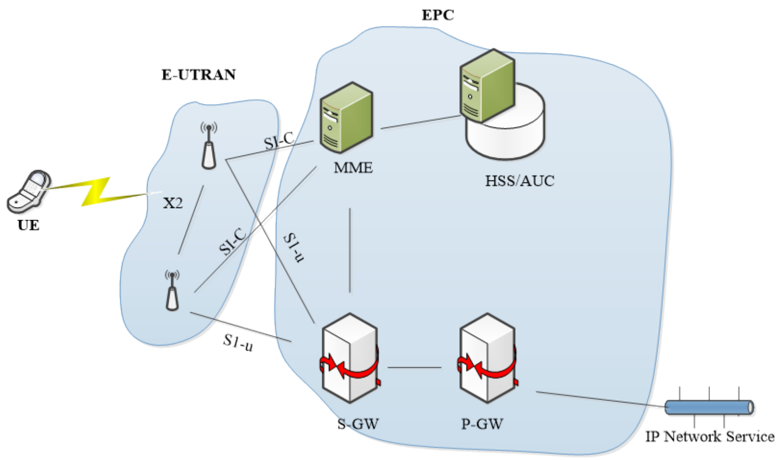


Fig. 1. LTE/SAE architecture

As shown in **Fig. 1** an LTE network is comprised of the access network and the core network, including the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC). E-UTRAN includes eNodeBs as base stations [13] to communicate with UEs [14] and EPC consists of a Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), and Home Subscriber Server (HSS);it is an all-IP and fully packet-switched backbone network in the LTE systems. Each eNodeB is connected to one or multiple MMEs and S-GWs in EPC passing through an S1 interface and connected to each other through an X2 interface. They communicate with UEs through a Uu interface. In LTE/SAE, the eNodeB located in a public place and connected to EPC over the IP layer. To guarantee the security of the core network, two layers of LTE security are designed to protect the passing traffic [15][16]. The layer responsible for ensuring security between the UE and eNodeB is called the Access Stratum (AS) layer; it is created when data in radio links need to be exchanged and protects the signaling and user data. The other layer, the Non-access Stratum (NAS) layer, is active whenever the UE is registered to the network and is tasked with securing signals in the region between the UE and MME.

2.2 Key hierarchy in LTE/SAE

The key hierarchy in the LTE/SAE network is shown in **Fig. 2**. When a UE registers to the LTE/SAE network, an Authentication and Key Agreement (AKA) [17] occurs between the UE and the MME on behalf of HSS and a local master key(K_{ASME}) is generated from the permanent master key(K) stored in UE and HSS. The first intermediate keys which are responsible for encryption and integrity verification in the NAS layer, denoted K_{NASenc} and K_{NASint}, are then derived and distributed to the MME. The second intermediate key, which is specific to the eNodeB and UE to protect the AS layer, denoted as K_{eNB}, is derived in the MME and distributed to the eNodeB [11]. The UEs can generate the above keys for the NAS and AS layer security from the permanent master key synchronously. The key K_{eNB} is our primary concern here: To provide key separation and reduce MME load, LTE/SAE network permits the K_{eNB} update to occur directly between eNodeBs, but this scheme has notable flaws as discussed below.

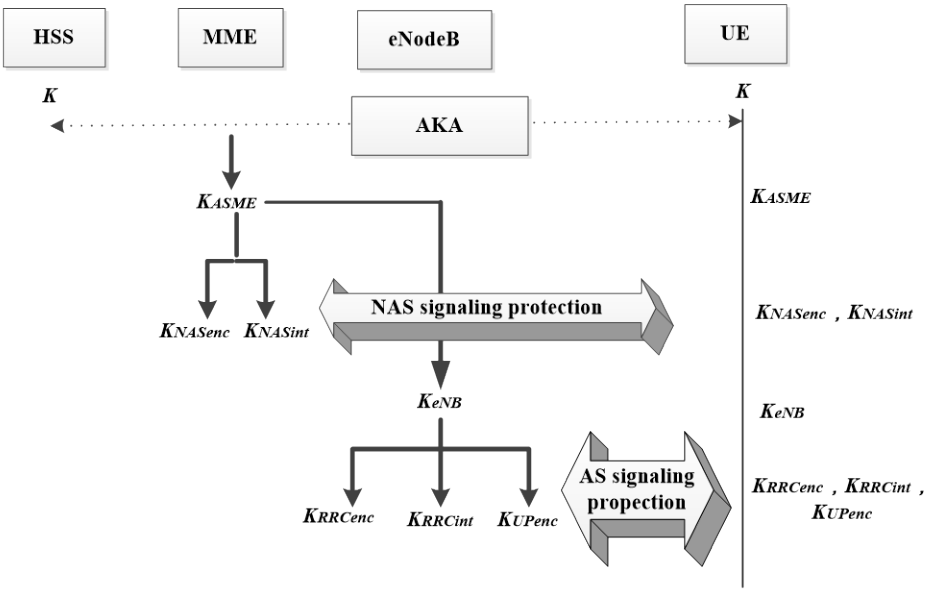


Fig. 2. Key hierarchy of LTE/SAE

In the LTE/SAE standard key distribution mechanism, the handover is implemented by the S1 interface or X2 interface. "S1 handover" denotes handover between different MMEs without direct signal among eNodeBs in the same MME; In this case, the UE and MME run a full AKA procedure to generate new parameters including keys for security, minimizing risk. Our concern in this study is X2 handover, generally called “intra-handover”, which occurs between eNodeBs in the same MME and represents generally weak key management.

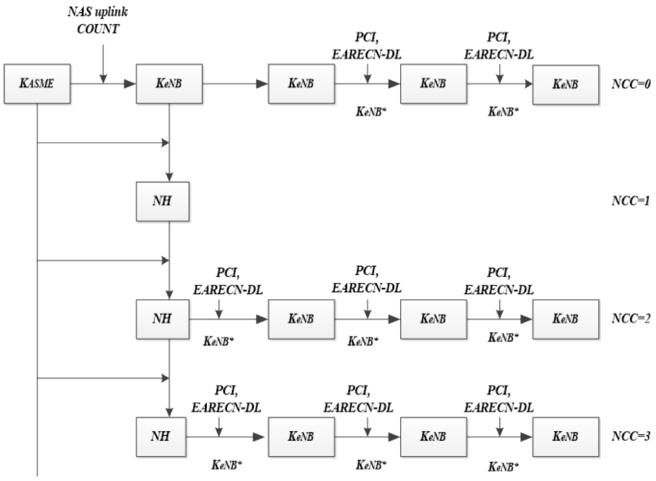


Fig. 3. Key chaining during handover [6]

As mentioned above, in a given handover process, K_{eNB} update occurs directly between eNodeBs to reduce the MME and signal traffic load. To maintain key separation, 3GPP adopts the key chaining architecture shown in Fig. 3.The source eNodeB uses horizontal or vertical key derivations [18] to derive a temporary, new K_{eNB} (K_{eNB}^{*}) which is used to derive new K_{eNB} between the target eNodeB and UE.

This key chain specifies two fresh keying materials: The Next Hop (*NH*) key and the *NH* Chaining Counter (*NCC*). The source eNodeB derives K_{eNB}^{*} from current K_{eNB} or *NH* using a one-way hash function KDF to ensure backward key separation [19]. To ensure forward key separation, the MME provides fresh key material to the target eNodeB after the X2 handover; this fresh material refreshes K_{eNB} in the subsequent handover. The two possible key derivation steps are described by equations (1) , (2), and (3) [18] below. The Target PCI is the Physical Cell Id (*PCI*) of target eNodeB and *EARFCN-DL* is its frequency. Thus, K_{eNB}^{*} is bound with K_{ASME} and the target eNodeB parameter.

$$K_{eNB}^{*} = KDF(K_{eNB}, Target\ PCI, EARFCN - DL) \tag{1}$$

$$K_{eNB}^{*} = KDF(NH_{NCC}, Target\ PCI, EARFCN - DL) \tag{2}$$

$$NH_{NCC} = KDF(K_{ASME}, NH_{NCC-1}) \tag{3}$$

Eq. (1) works in cases when source eNodeB does not have a *NH* key available. Eq. (2) represents a common case, in which the source eNodeB has an *NH* available and uses it to derive a fresh K_{eNB}^{*} for the target eNodeB.

2.3 X2 handover key management in LTE/SAE

The message flow in standard X2 handover is shown in Fig. 4. Detailed message and procedure descriptions are also provided below [19-21].

Source eNodeB has received the key material $\{NH_{NCC}, NCC\}$ from the MME in the Path Switch ACK of the last X2 handover.

1. UE sends a Measure Report to source eNodeB. Source eNodeB analyzes the measure report

and makes or refuses a handover decision. If a handover decision is made, source eNodeB uses Eq.(1) or (2) to derive $K_{eNB}{}^*$.

2. The source eNodeB forwards the Handover Request including pair $\{K_{eNB}{}^*, NCC\}$ to the target eNodeB. The target eNodeB renews the $K_{eNB}{}^*$ by hashing the received $K_{eNB}{}^*$ and the cell-level temporary identifier(*C-RNTI*), a temporary identity that denotes the UE, in the target eNodeB. The target eNodeB then uses the new K_{eNB} to derive keys for AS layer security.

3. The target eNodeB sends Handover Request Ack including *NCC* and *C-RNTI* to the source eNodeB in plaintext.

4. The source eNodeB forwards the Handover Command including *NCC* and *C-RNTI* to UE. The UE compares the received *NCC* with the *NCC* value associated with the current security association. If their values are the same, the UE uses Eq.(1) to derive $K_{eNB}{}^*$ from the currently active K_{eNB}. If the received *NCC* is greater than the current *NCC*, the UE uses Eq. (3) to compute the next *NH* key continuously until the two *NCC* values match and uses Eq.(2) to derive the $K_{eNB}{}^*$. The UE then renews $K_{eNB}{}^*$ using the received *C-RNTI* and $K_{eNB}{}^*$, and uses the new K_{eNB} to derive keys for AS layer security.

5. The UE sends a Handover Confirm to the target eNodeB and a direct connection between the target eNodeB and UE is built. Handover signal is over.

6. The target eNodeB sends the S1 Path Switch Request to the MME; The MME then uses Eq.(3) to calculate NH_{NCC+1}.

7. The MME forwards an S1 Path Switch Request ACK including fresh key material pair $\{NH_{NCC+1}, NCC+1\}$ for use in the subsequent handover to the target eNodeB.

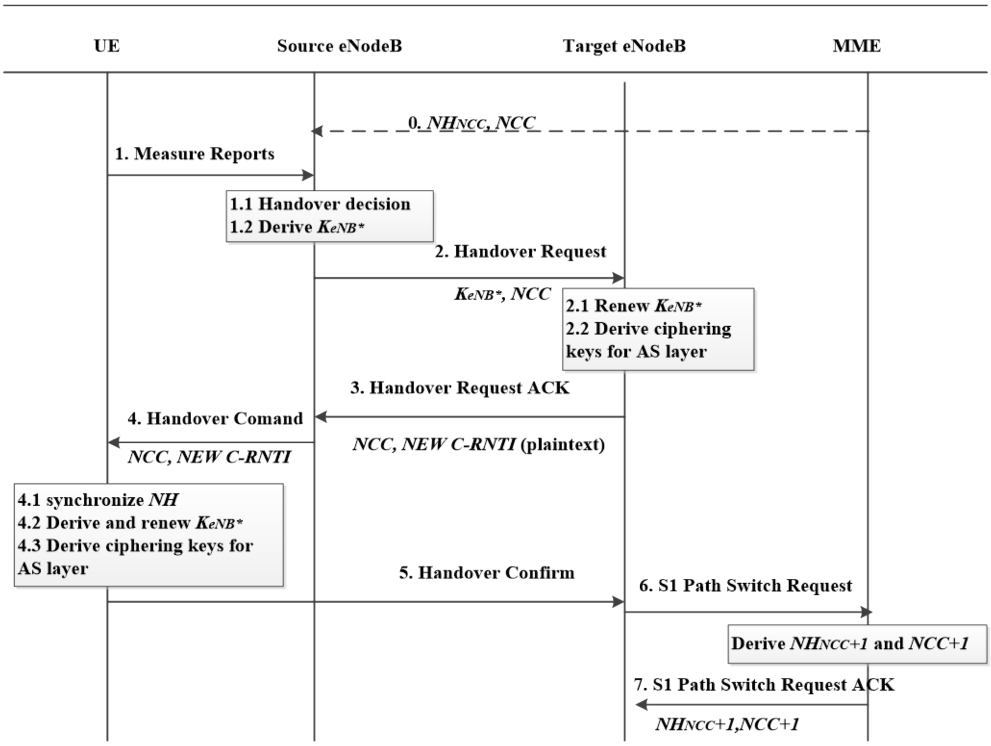


Fig. 4. Key management in X2 handover

3. Proposed method of x2 handover key management enhancement in LTE/SAE

The lack of one-hop forward security caused by key compromise originates in the derivation of $K_{eNB}{}^{*}$ by source eNodeB. Caching key refresh materials and parameters is the most effective approach to solving the security problem without reconstructing the current key hierarchy or signal procedures. We found that if we change the renewing function parameter after message 2 to a material that the source eNodeB cannot calculate, one-hop forward security in key compromise can be effectively ensured. Because the UE can calculate NH_{NCC+1} and the MME sends NH_{NCC+1} to the target eNodeB through a secure S1 interface in message 7, NH_{NCC+1} is a reasonable parameter selection; $K_{eNB}{}^{*}$ renewal is remitted to the moment that the target eNodeB receives the parameter. To resist de-synchronization attacks from the compromised eNodeB, we respectively hashed *NCC* in the UE and target eNodeB together with a calibration code as shown in **Fig. 5** The message flow is detailed below.

0. The source eNodeB has received the key material $\{NH_{NCC}, NCC\}$ from the MME in the Path Switch ACK of the previous X2 handover.

1.The UE sends a Measure Report to the source eNodeB, which analyses the report to make or refuse a handover decision. If a handover decision is made, the source eNodeB uses Eq.(1) or (2) to derive $K_{eNB}{}^{*}$.

2. The source eNodeB forwards the Handover Request including pair $\{K_{eNB}{}^{*}, NCC\}$ to the target eNodeB, which uses $K_{eNB}{}^{*}$ to derive temporary keys for AS layer security.

3. The target eNodeB sends a Handover Request ACK including *NCC* and *C-RNTI* to the source eNodeB in plaintext.

4. The source eNodeB forwards a Handover Command including *NCC* and *C-RNTI* to the UE. The UE compares the received *NCC* with the *NCC* value associated with the current security association, and if their values are the same, uses Eq.(1) to derive $K_{eNB}{}^{*}$ from the currently active K_{eNB}. If the received *NCC* is greater than the current *NCC*, the UE uses Eq.(3) to compute the next *NH* key continuously until the two *NCC* values match and uses Eq.(2) to derive $K_{eNB}{}^{*}$ and $K_{eNB}{}^{*}$ to derive temporary keys for AS layer security.

5. The UE sends a Handover Confirm to the target eNodeB. A temporary direct connection between the target eNodeB and UE is built.

6. The target eNodeB sends an S1 Path Switch Request to the MME. The MME then uses Eq.(3) to calculate NH_{NCC+1}.

7. The MME forwards an S1 Path Switch Request ACK including fresh key material pair $\{NH_{NCC+1}, NCC+1\}$ to the target eNodeB. To ensure a thorough analysis, we considered a case in which the recent handover process uses Eq.(1) to derive keys or one in which the handover process comes under a de-synchronization attack. In these particular cases, the target eNodeB does not receive pair $\{NH_{NCC+1}, NCC+1\}$ from the MME, but instead receives pair $\{NH_{NCC+N}, NCC+N\}$. We set a real-number parameter *N* to denote this. The target eNodeB compares the received *NCC* and current *NCC*: If the current *NCC* add 2 is greater than the received *NCC*, the value of *N* is 1; otherwise, the value of *N* is the received *NCC* minus the

current *NCC*. The current *NCC* is then hashed and NH_{NCC} is received as the calibration code, donated as α.

8. The target eNodeB send a Key Refresh Demand message which contains α and *N* to UE, then the target eNodeB renews K_{eNB}^{*} by hashing the received NH_{NCC+1} and K_{eNB}^{*} and uses the new K_{eNB} to derive keys for AS layer security. After receiving the message, the UE derives NH_{NCC+N} then hashes the current *NCC* and NH_{NCC+N} as a calibration code denoted β. The UE compares the received calibration code α with β. If they match, it renews K_{eNB}^{*} by hashing NH_{NCC+N} and K_{eNB}^{*}. It then uses the new K_{eNB} to derive keys for AS layer security. Otherwise, the UE requests a new AKA procedure. It only approves Key Refresh Demand once the handover process is underway.

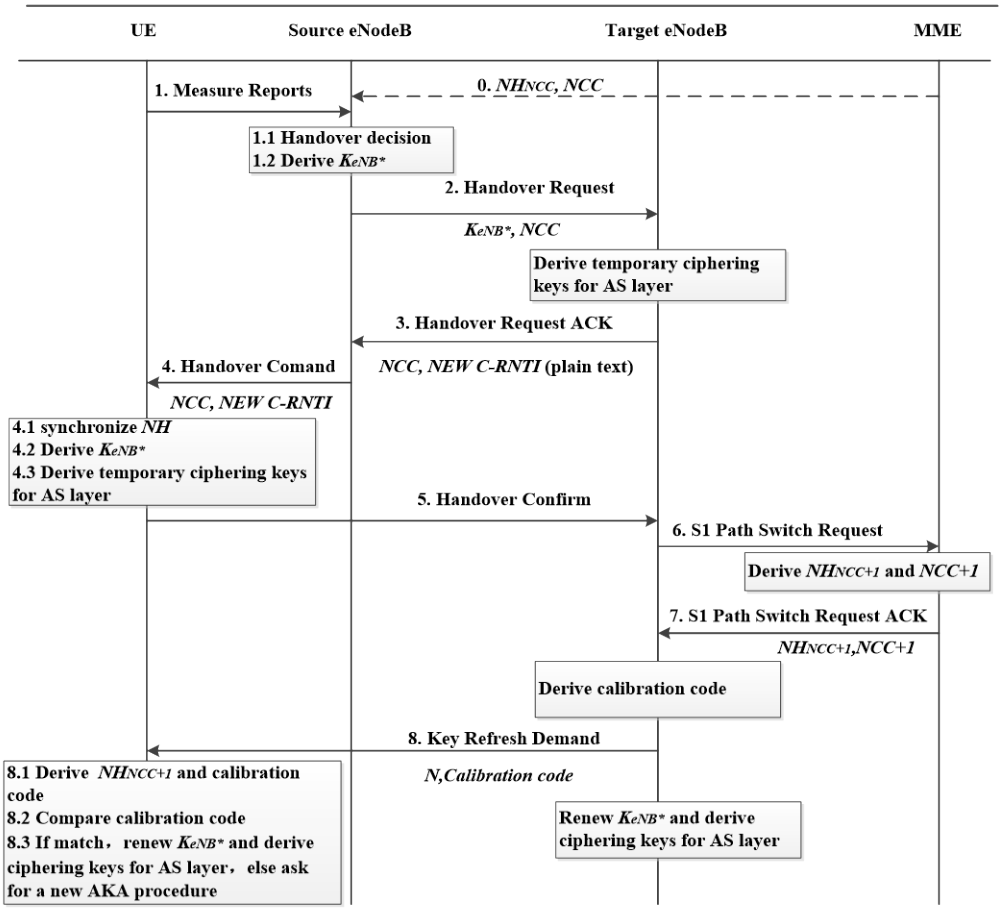

UE
Source eNodeB
Target eNodeB
MME
0. NHNCC, NCC
1. Measure Reports
1.1 Handover decision
1.2 Derive KeNB*
2. Handover Request
KeNB*, NCC
Derive temporary ciphering keys for AS layer
3. Handover Request ACK
4. Handover Comand
NCC, NEW C-RNTI (plain text)
NCC, NEW C-RNTI
4.1 synchronize NH
4.2 Derive KeNB*
4.3 Derive temporary ciphering keys for AS layer
5. Handover Confirm
6. S1 Path Switch Request
Derive NHNCC+1 and NCC+1
7. S1 Path Switch Request ACK
NHNCC+1,NCC+1
Derive calibration code
8. Key Refresh Demand
N,Calibration code
8.1 Derive NHNCC+1 and calibration code
8.2 Compare calibration code
8.3 If match, renew KeNB* and derive ciphering keys for AS layer, else ask for a new AKA procedure
Renew KeNB* and derive ciphering keys for AS layer

Fig. 5. Proposed method of enhancing X2 handover key management

4. Security analysis

As described in Section 2, X2 handover key management includes a chaining architecture and K_{eNB}^{*} is bound with target eNodeB parameters. This ensures key separation among the eNodeBs [22]. KDF and renewing functions, both hash functions, ensure backward separation.

4.1 Security analysis of the current scheme

We first analyzed the security of the current scheme. We used two attack models for this purpose: Key compromise and de-synchronization attack. As discussed in the Introduction, these are the attacks most likely to be used by adversaries.

A. *Adversaries can capture signal information in radio channels and have access to stored keys in the source eNodeB.*

In this case, all keys and key derivation materials stored in source eNodeB are visible to the adversary. The adversary has the current active K_{eNB} to decipher messages during signal capture. The adversary can attain target cell parameters *C-RNTI* (assigned to the UE by the target eNodeB), NH_{NCC} ,and *NCC*. The current handover uses either Eq.(1) or (2) to derive $K_{eNB}{}^{*}$, while the adversary already holds all materials necessary to calculate $K_{eNB}{}^{*}$ and renew $K_{eNB}{}^{*}$ to secure the K_{eNB} used between the target eNodeB and UE. K_{ASME} is held only by the UE and MME, however, so the adversary cannot derive NH_{NCC+1} using Eq.(3) for the subsequent handover. In this scenario, the current X2 handover lacks one-hop forward security.

B. *Adversaries can capture signal information in radio channels and control the source eNodeB entirely.*

In this case, the adversary can control the source eNodeB to send manipulated messages to the UE and target eNodeB. The adversary sends a Handover Request message that contains an extremely high- value *NCC* to the target eNodeB, while sending the original *NCC* value to the UE. The *NCC* value from the S1 Path Switch Request ACK message is considerably smaller than that received from the compromised eNodeB, which causes the target eNodeB and the UE to generate the subsequent session key using Eq.(1) based on the current K_{eNB}. Once the UE moves to a new target eNodeB, the adversary sends a manipulated message containing the original *NCC* value unless a new AKA procedure is executed. In this scenario, the adversary can calculate the subsequent K_{eNB} before a new AKA occurs; forward security is broken.

4.2 Security analysis of the proposed scheme

Forward security is threatened via the scenarios described above in current X2 handover key management schemes. We used the same two attack models to analyze the security of the proposed scheme.

A. *Adversaries can capture signal information in radio channels and have the access to stored keys in the source eNodeB.*

As mentioned above, in this case, the adversary holds current active K_{eNB}, target cell's parameters, new *C-RNTI* and *NCC*. The adversary can derive $K_{eNB}{}^{*}$ using Eq.(1) or (2). In our scheme, renewing material is transferred through the S1 interface but not the air interface; the adversary cannot capture NH_{NCC+1} or calculate NH_{NCC+1} to renew $K_{eNB}{}^{*}$, and forward security is thus ensured. By design, the UE only approves a Key Refresh Demand once the handover process has begun. This minimizes the likelihood of replay attack or false Key Refresh Demand messages from the source eNodeB controller.

B. *Adversaries can capture signal information in radio channels and control the source eNodeB entirely.*

As discussed in Section 4.2, in this case, the adversary sends different *NCC* values to execute a de-synchronization attack. In our scheme, we adopt a pair of calibration codes to verify whether the *NCC* that the source eNodeB has sent to the target eNodeB equals that sent to the UE. The *NCC* in the target eNodeB is hashed with the NH_{NCC} that target eNodeB received from the MME, and the *NCC* in the UE is hashed with the NH_{NCC} derived by the UE. If the calibration codes are not equal, a de-synchronization attack is considered to have been executed and the UE requests a new AKA procedure. If the adversary tries to perform a de-synchronization attack in the role of target eNodeB, the only message he can manipulate is the Key Refresh Command. If the adversary manipulates *N*, the UE will refresh the session key using NH_{NCC+N} which is derived by the manipulated *N*, but the controlled target eNodeB cannot calculate NH_{NCC+N} to refresh K_{eNB}^{*} as the *NH* key can only be derived in UE and MME. At this point, the connection is aborted and the UE asks for a new AKA. Manipulating the calibration is not necessary, as the UE will ask for a new AKA if the calibration does not match.

4.3 Formal verification of the proposed scheme with ProVerif

ProVerif [12] is a tool automates the verification of security protocols. It utilizes theorem-proving techniques where the protocol actors and attacker are modeled according to the symbolic approach defined by Dolev and Yao [23]. Noomene [24] modeled security procedures in LTE using ProVerif; we modified their novel X2 handover model to suit our scheme.

To model a compromised eNodeB, the messages in our model were transferred in a public channel (except the messages between the target eNodeB and the MME). ProVerif provided a query and phase instructionfor checking secrecy. Secrecy (including forward security)was verified in the model as follows:

```
query attacker(secret) phase 1.
……
let UE(uecaps:caps, kenb:key)=
……
phase 1;
out(pubch,senc(secret,kenbdstar));
0.
……
```

The result of the verification was successful, indicating that our proposed scheme is secure for an unbounded number of handovers. Though ProVerify is not able to resolve a query in which the attacker manipulates messages in the channels, we effectively assessed the situation in which the adversary manuscripts the message from a compromised eNodeB in Section 4.2. Our proposed scheme was successful in providing forward security in the X2 handover procedure. The complete handover model is available at the URL https://gist.github.com/cszdxs1/d92479570fc4df943592945862911441.

4.4 Security comparison among similar schemes

Our enhanced scheme can be utilized to ensure forward security in X2 handover key management. A comparison among ours and other schemes in regards to security provided below in **Table 1**. In one of the schemes used for comparison [8], the message flow of the X2 handover process is rearranged so that K_{eNB}^{*} derivation occurs in the target eNodeB directly.

In this scheme, the source eNodeB sends *NCC*+1 to the UE; the UE derives NH_{NCC+1} and refreshes $K_{eNB}{}^{*}$ from it, then informs the target eNodeB with NCC+1. The target eNodeB queries MME for NH_{NCC+1}. When the target eNodeB receives NH_{NCC+1}, it can derive $K_{eNB}{}^{*}$ as a new K_{eNB}. During a de-synchronization attack, however, a compromised eNodeB can send the MME a manipulated *NCC* value to obtain NH_{NCC+1} values. In short, this scheme cannot fully ensure forward security. In the other scheme used here as a reference [9], one of the key parameters is made invisible to the source eNodeB by transferring it in cipher text. Before the target eNodeB sends key material *NCC* and *C-RNTI* to the source eNodeB, it sends *C-RNTI* to the MME. The MME then encrypts C-RNTI using the K_{ASME} that is also stored in the UE and sends it back to the target eNodeB. After receiving the ACK message, the target eNodeB sends a message with the cipher text to the source eNodeB. The cipher text is ultimately decrypted by the UE using K_{ASME}, then the *C-RNTI* is used to renew the $K_{eNB}{}^{*}$. In this approach, the source eNodeB does not have sufficient key material to renew $K_{eNB}{}^{*}$ or to obtain the K_{eNB} used between the UE and target eNodeB.

Table 1. Security among various schemes

	Key compromise	De-synchronization attack
Current scheme	×	×
Proposed scheme	√	√
Reference scheme [8]	√	×
Reference scheme [9]	√	√

5. Performance analysis

Transmission load and computation load are the two aspects of concern in this section. Communication overhead(i.e., signal cost) is an important factor affecting transmission performance. A comparison of the communication overhead related to various schemes in X2 handover key management is shown in **Table 2**. An extra message through the Uu interface is added in our scheme, as described above. The message quantity with the rearranged message flow in the first reference scheme [8] is the same as the original without extra signal cost. Two extra messages through the S1 interface are added in the second reference scheme [9]. Another important factor affecting transmission performance is the usage rate of each interface. As one MME serves multiple eNodeBs, the S1 interface bears much greater load than the Uu interface; the extra messages sent to the MME in the first reference scheme [8] make this particularly costly.

Table 2. Communication overhead among similar schemes

	Signal costs (messages)		
	Uu	X2	S1
Current scheme	3	2	2
Proposed scheme	4	2	2
Reference scheme [8]	3	2	4
Reference scheme [9]	3	2	2

The schemes described here all enhance handover security while introducing additional computation cost. Said cost is not the only factor that affects computation performance, however the devices that bear the additional cost should also be considered. The additional computation costs of the reference schemes and proposed scheme are described in **Table 3**. In our scheme, the extra cost of the additional derivation of the AS layer key and calibration code can be considered negligible because it is disseminated across the UE and eNodeBs. Conversely, the extra MME creates a computationally intensive load when encrypting *C-RNTI* that may render the second reference scheme [9] entirely impractical.

Table 3. Computation costs among similar schemes

	UE	Source eBodeB	Target eNodeB	MME
Proposed scheme	Derivation of AS layer key and calibration code	None	Derivation of AS layer key and calibration code	None
Reference scheme [8]	None	None	None	No addition
Reference scheme [9]	Decryption	None	None	Encryption

Compared to the enhancement in the first reference scheme [8], our proposed scheme is not vulnerable to de-synchronization attacks. The proposed scheme also contains only one extra message (as opposed to the two extra messages in the second reference scheme [9]) through the S1 interface as a measure of preventing transfer through the air interface in key management. The centralized signal load to the MME is disseminated to the Uu interface, which has much more bandwidth between eNodeBs and UEs, while the centralized computation load to the MME is replaced with an additional key derivation for the AS layer disseminated to UEs and eNodeBs. In our scheme, handover latency is the same as that in the current scheme by virtue of the temporary direct connection between the UE and target eNodeB built into message 5. Transition to our enhancement scheme is also easily realized by improving upon existing software, i.e., it does not necessitate reconstructing the current architecture.

6. Conclusion

As discussed at length in the Introduction, there are notable forward security problems in the standard X2 handover key management process which leave the network subject to attack. In the scheme we propose here to solve the forward security problem, NH_{NCC+1} serves as the renewing parameter and the renewal of $K_{eNB}{}^{*}$ is remitted. When the target eNodeB receives NH_{NCC+1}, it notifies the UE to renew the temporary keys; we add a verification procedure at this stage to eliminate any vulnerability to de-synchronization attacks.

Based on security analysis of the proposed scheme and other similar schemes, we found that forward security is ensured in our scheme and one of two similar reference schemes [9]. Forward security is sabotaged in the other reference scheme we examined [8] when a de-synchronization attack occurs. Our scheme also has the same latency as the current scheme, despite the one additional message and extra computation. These extra loads, as opposed to those in the second reference scheme [9], are disseminated so that the core network is spared any excessive load. In short, the proposed scheme is feasible as well as effective in ensuring forward security. We are currently in the process of researching the feasibility and effectiveness of applying the scheme proposed here to next-generation wireless networks.

Reference

[1] Liu Qi, Shi Yameng ,Li Fuchang and Fan Bin，"Research on Services Modeling in LTE Networks," *China Communications*, vol. 13, no. 2, pp. 109-120, February 2016. Article (CrossRef Link)

[2] Cao Jin, Ma Maode and Li Hui, "Unified handover authentication between heterogeneous access systems in LTE networks," in *Proc. of the IEEE Global Communications Conference*, pp.5308-5313, December 3-7, 2012. Article (CrossRef Link)

[3] Yaseein Soubhi Hussein, Borhanuddin M Ali, Mohd Fadlee A. Rasid and Aduwati Sali, "Handover in LTE networks with proactive multiple preparation approach and adaptive parameters using fuzzy logic control," *KSII transactions on internet and information systems*, vol. 9, no. 7, pp. 2389-2413, July, 2015. Article (CrossRef Link)

[4] Amitava Ghost, Rapeepat Ratasuk and Bishwarup Mondal, "MONDAL B, et al. LTE-advanced: Next-generation wireless broadband technology," *IEEE wireless communications*, vol. 17, no. 3, pp. 10-22, June 2010. Article (CrossRef Link)

[5] Chan-kyu Han and Hyoung-Kee Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 2, pp. 457-468, February, 2014. Article (CrossRef Link)

[6] Cao Jin, Ma Maode, Li Hui, Zhang Yueyu and Luo Zhengxing, "A survey on security aspects for LTE and LTE-A networks," *IEEE communications surveys& tutorials*, vol. 16, no. 1, pp. 283-302, First quarter, 2014. Article (CrossRef Link)

[7] Cao Jin, Li Hui, Ma Maode, Zhang Yueyu and Lai Chengzhe, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Computer Networks*, vol. 56, no. 8, pp. 2119-2131, May, 2012. Article (CrossRef Link)

[8] Li Taicheng, He Li and Wu Bin, "Key refresh during cell handover in LTE featuring one-Hop forward security," *Computer Systems & Applications*, vol. 20, no. 8, pp. 67-71, August, 2011. Article (CrossRef Link)

[9] Xiao Qinshu, Zhou Wenan, Cui Baojiang and Li Lingrong, "An Enhancement for key management in LTE/SAE X2 handover based on ciphering key parameters," in *Proc. of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp.256-261, November 8-10, 2014. Article (CrossRef Link)

[10] Eman F. ElGaml, Hussein ElAttar and Hesham M. ElBadawy, "Evaluation of Intrusion Prevention Technique in LTE Based Network," *International Journal of Scientific & Engineering Research*, vol. 5, issue.12, pp.1395-1400, December 2014. Article (CrossRef Link)

[11] Dan Forsberg, "LTE key management analysis with session keys context," *Computer Communications*, vol. 33, no. 16, pp. 1907-1915, July 2010. Article (CrossRef Link)

[12] Naïm Qachri, Olivier Markowitch and Jean-Michel 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, July,2013. Article (CrossRef Link)

[13] 3GPP, Evolved universal terrestrial radio access network(EUTRAN), architecture description, 3GPP TS 36.401 v9.2.0, 2010. Article (CrossRef Link)

[14] Chang Junren, Li Yajuan, Feng Shulan, Wang Haiguang, Sun Chengzhen and Zhang Philipp, "A fractional soft handover scheme for 3GPP LTE-Advanced System," in *Proc. of the 2009 IEEE International Conference*, pp.1-5, June 14-18, 2009. Article (CrossRef Link)

[15] NIEMI V, NYBERG K. UMTS security. John Wiley & Sons ,UK,2003. Article (CrossRef Link)

[16] 3GPP. Security objectives and principles. 3GPP TS33.120, 2001. Article (CrossRef Link)

[17] 3G Security, Security Architecture (Release 11), 3GPP TS 33.102, Version 11.1.0, 2011. Article (CrossRef Link)

[18] 3GPP System Architecture Evolution (SAE), Security Architecture(Release 11), 3GPP TS 33.401, v11.2.0, 2011. Article (CrossRef Link)

[19] Hyun-Seo Park, Yong-Seouk Choi, Byung-Chul Kim, and Jae-Yong Lee, "LTE mobility enhancements for evolution into 5G," *ETRI Journal*, vol. 37, no. 6, pp. 1065-1076, December, 2015. Article (CrossRef Link)

[20] Chen Jengyueng, Yang Chunchuan and Mai Yiting, "A Novel Smart Forwarding Scheme in LTE-Advanced Networks," *China Communications*, vol. 12, no. 3, pp. 120-131, March 2015. Article (CrossRef Link)

[21] Mohmad Anas, Francesco D. Calabrese, Preben E. Mogensen, Claudio Rosa and Klaus I. Pedersen, "Performance evaluation of received signal strength based hard handover for UTRAN LTE," in *Proc. of the IEEE 65th Vehicular Technology Conference*, pp.1046-1050, April 22-25, 2007. Article (CrossRef Link)

[22] Dan Forsberg, Huang Leping, Kashima Tsuyoshi and Seppo Alanara, "Enhancing security and privacy in 3GPP EUTRAN radio interface," in *Proc. of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp.1-5, September 3-7, 2007. Article (CrossRef Link)

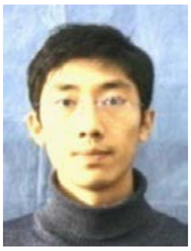
[23] Danny Dolev and Andrew ChiChih Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, October, 1983. Article (CrossRef Link)

[24] Noomene Ben, Henda and Karl Norrman, "Formal Analysis of Security Procedures in LTE - A Feasibility Study," *Lecture Notes in Computer Science Springer International Publishing*, vol. 8688, pp. 341–361, 2014. Article (CrossRef Link)

Bangyi Sun is studying for his combined Master's and Phd's degree in the College of Computer Science and Technology, Jilin University, Changchun. His research interests include Wireless network, Data security and privacy.

Jianfen Chu received the M.S. and Ph.D. Degrees both from the College of Computer Science and Technology, Jilin University, Changchun. He is currently a sub-professor in the College of Computer Science and Technology, Jilin University. His research interests include Network Penetration, Data security and privacy.

Liang Hu has his BS degree on Computer Systems Harbin Institute of Technology in 1993 and his Ph.D. on Computer Software and Theory in 1999. Currently, he is the professor and Ph.D. supervisor of College of Computer Science and Technology, Jilin University, China. His main research interests include distributed systems, computer networks, communications technology and information security system, etc. As a person in charge or a principal participant, Dr Liang Hu has finished more than 20 national, provincial and ministerial level research projects of China.



Hongtu Li received the M.S. and Ph.D. Degrees both from the College of Computer Science and Technology, Jilin University, Changchun. He is currently working in grid and network security laboratory as an assistant reseacher at Jilin University. His research interests include information security and cryptology.

Guangkun Shi received his B.S. and M.S. degrees from Jilin University, China in 2004 and 2007, respectively, both in electronics engineering. At present, He is engaged in Ph.D. degree study at Jilin University. His research interests are in the areas of communication networks including cloud computing, data centre and next generation Internet technologies.