A proxy signature-based handover authentication scheme for LTE wireless networks

Qiu, Yue; Ma, Maode; Wang, Xilei

2017

Qiu, Y., Ma, M., & Wang, X. (2017). A proxy signature-based handover authentication scheme for LTE wireless networks. *Journal of Network and Computer Applications*, 83, 63-71.

<https://hdl.handle.net/10356/83489>

<https://doi.org/10.1016/j.jnca.2017.01.023>

© 2017 Elsevier. This is the author created version of a work that has been peer reviewed and accepted for publication by *Journal of Network and Computer Applications*, Elsevier. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1016/j.jnca.2017.01.023>].

Downloaded on 26 Apr 2023 12:20:28 SGT

A Proxy Signature-based Handover Authentication Scheme for LTE Wireless Networks

Yue Qiu, Maode Ma and Xilei Wang

School of Electrical and Electronic Engineering,
Nanyang Technological University, Singapore

Abstract

A seamless and secure handover is always one of the important design goals of the cellular networks. The handover scheme of 4G Long Term Evolution (LTE) wireless networks is complex due to the presence of two possible different types of base stations. In LTE communication systems, a normal base station is referred to as an eNodeB (eNB). What increases the level of complexity of the system is the fact that the other kind of base stations, namely, Home eNodeB (HeNB), cannot directly communicate with eNB. In the LTE networks, the handover scenarios involving a HeNB could result in a complicated handover procedure. Besides, since key chains have been used in the handover processes, it is found to be lack of backward security. Therefore, in order to handle the handover involving a HeNB efficiently with security provisioning, in this paper, a proxy signature-based handover scheme is proposed. The proposed scheme works based on the Elliptic Curve Cryptography (ECC) algorithm, which makes the computational cost of the handover process smaller compared to other handover schemes.

Keyword: Handover, Authentication, Security, Long Term Evolution

1. Introduction

With rapid development of wireless technology, more and more people have now been able to be contacted in any place and at any time by wireless communication networks. A lot of applications demanding a high data transmission rate over mobile wireless networks have become true to be realized. In order to support the high data transmission rate, a 4G cellular network named Long Term Evolution (LTE) has specified by the third Generation Partnership Project (3GPP) committee. As one of the new progression of the 3GPP Global System for Mobile communications (GSM) and Universal Mobile Telecommunications System (UMTS) families, LTE systems can provide a higher capacity to support a broadband mobile wireless communication compared to the first two generations of the wireless technologies [1].

The LTE network consists of two subsystems. One is the Evolved Packet Core (EPC) and the other is the Evolved Universal Terrestrial Radio Access Networks (E-UTRANs). Responsible for the overall control as the backbone network, the EPC comprises of several main logic elements, namely, the Packet Data Network (PDN) Gateway (PDN-GW), the Serving Gateway (S-GW), the Mobility Management Entity (MME), Evolved Serving Mobile Location Centre (E-SMLC), the Home Subscriber Server (HSS), the Policy Control and Charging Rules Function (PCRF) and the Gateway Mobile Location Centre (GMLC). The E-UTRAN, on the other hand, is the access network consisting of base stations which are responsible to communicate with User Equipments (UEs). In the LTE system, normal base stations are named as eNodeBs (eNBs) [1]. In addition, in order to achieve better indoor network performance, a new kind of base stations named as Home eNodeB (HeNB) has been introduced.

With more applications developed over the 4G LTE wireless networks, the issue of the performance and security of the 4G LTE cellular system becomes a major concern and a hot research topic. The handover process is also one of the important aspects to impact the performance and security. The tradeoff between performance such as power consumption and security such as the authentication needs to be considered carefully. The fact that the two different kinds of base stations are not able to directly communicate with each other makes the LTE handover authentication procedure to be a rather complex [2]. It is pointed out that the LTE handover process is vulnerable against several types of security attacks like eavesdropping, man-in-the-middle attack and masquerading [3]. [4] describes three types of vulnerabilities in the LTE handover process. It discloses that the LTE handover process is vulnerable to the replay attacks, de-synchronization attacks, and is lack of backward security. A number of handover authentication schemes have been proposed to achieve the backward security. However, some of the proposals often require the involvement of the current base station, which may not be feasible in some environments [5, 6]. On the other hand, some of the proposals require the participation of an Authentication, Authorizing, and Accounting (AAA) server [7-9], which can provide strong security functionality. But they require the establishment of a trust relationship between the base stations and the AAA server, which could lead to much authentication traffic. In addition, the AAA servers are usually located far from the base stations, the establishment of the connection between them could take much time and the information exchange may suffer a high delay.

In [10], an authentication scheme using a proxy signature has been proposed. By the proxy signature approach, the HSS, AAA server or current base station can issue its proxy delegation to the UEs for the authentication, which can effectively lower the level of complexity of the entire

network. However, it only has a one-directional authentication performed, which means that an access point (AP) can authenticate the mobile nodes but the mobile nodes cannot verify the authenticity of the AP. This leads to the system to be vulnerable when one AP is compromised because a dishonest AP can build connections with other malicious APs and establish a forgery session key with the legitimate mobile nodes using the handover information sent from the original AP. The scheme proposed in [11] enables the eNB and UE to mutually authenticate each other by the proxy signature approach to achieve a good forward/backward security for the network. Nevertheless, it requires the UE to perform five times of RSA verification, which will increase the unnecessary computational cost to the power-limited UEs. In order to make the authentication process to be more efficient with the same level of the security, a proxy signature-based authentication scheme working based on the Elliptic Curve Cryptography (ECC) has been proposed in [12], which is able to reduce the computational cost of the authentication process because the primary benefit of the ECC over the RSA algorithm is due to its much smaller key size [13]. But similar to the scheme in [10], the Mesh AP (MAP) cannot be authenticated by the Mesh Host (MH) by the scheme.

In order to improve the performance of the handover authentication, symmetric cryptography is employed as an alternative. A handover scheme has been proposed in [14] to enable a secure handover between eNBs with the assistance of relay nodes. This scheme works based on a symmetric key mechanism without a specification on the secure transmission of the confidential keys. A re-authentication protocol, which has also adopted the symmetric encryption, has been proposed in [15] to enable secure roaming from the LTE to the WLAN. However, a Hybrid Interconnection Unit (HIU) is required to serve as a relay, which may increase the system costs. It is obvious that although the symmetric cryptography is lightweight and faster, the asymmetric approach is much more secure and flexible.

In this paper, as our major contribution, a proxy signature-based authentication scheme for the handover in LTE wireless networks, named as ECC-based Proxy Signature for Handover (EPH), is designed to achieve a mutual authentication with a computational cost reduction at the same time. The beauty of the proposed scheme is that it is suitable for different handover scenarios with the involvement of the eNB and the HeNB, which has not been considered by the state-of-the-art solutions. By the proposed scheme, the overall system complexity is able to be reduced. We have conducted the logic prove by Burrows, Abadi, and Needham (BAN) Logic and formal verification by SPIN to present the logic correctness of the proposed solution.

The rest of this paper is organized as follows. In Section 2, the preliminaries information is

introduced. In Section 3, EPH scheme is presented in detail. This scheme is logically proved by BAN Logic and formally verified by SPIN in Section 4. The security analysis and the performance analysis of the proposed scheme are presented in Section 5. Finally, the conclusion of the paper is presented in Section 6.

2. Preliminary

2.1 eNB and HeNB

The eNBs are the major components in the access network of LTE, E-UTRAN, which connect backbone network, EPC, with the UEs for the Internet connections. They have the interfaces to the EPC, UEs and different eNBs. All the wireless communication functions of the E-UTRAN are operating at the eNBs following the communication protocols in the LTE E-UTRAN.

The HeNB is a novel type of eNB that controls a femtocell in the LTE networks. Femtocells are designed to cover small indoor areas such as a house. Most of them are the Closed Subscriber Group (CSG) cells which can only be accessed by a limited group of users. There are three access modes of the HeNBs, which are defined as follows.

1. Closed access mode: HeNBs are usually operated by a certain CSG and only those UEs that are listed in the CSG subscription list can access them.
2. Hybrid access mode: This mode is similar to the closed access mode. Nevertheless, all the legitimate UEs are allowed to access the HeNBs. But those HeNBs in the subscription list have higher priority.
3. Open access mode: A HeNB have the functions same as a normal eNB [1].

The access mode of a HeNB often impacts the handover process in the LTE networks. Different from the eNBs, the involvement of the HeNBs will increase the complexity of the overall system. In this paper, the proposed scheme will handle the handover processes for both eNBs and HeNB in a comprehensive way to reduce the complexity of the handover processes over the entire system.

2.2 Proxy Signature

In some circumstances, it is desirable for a signer to delegate his/her capability to another party so that the party could sign on behalf of the original signer. The proxy signature is the signature scheme that enables the signers to delegate his/her capability to other parties. The concept of proxy signature has first been introduced in [16] with some basic characteristics summarized as follows.

Firstly, the proxy signature is unforgeable. Only those who have been delegated the signing capability could create a proxy signature. Any other parties, including the original signer, are not able to do so. Secondly, the presence of the proxy signature represents the agreement of the signer on a message. Thirdly, the proxy signature shows the identity of its creator. Last, the proxy signer cannot repudiate its signing behavior.

A new proxy signature has been proposed in [17] based on the algorithm presented in [18]. This proxy signature is useful to provide security in the handover process and it has been utilized in [11] for the design of handover schemes.

2.3 Elliptic Curve Cryptography (ECC)

The Elliptic Curve Cryptography (ECC) has been first proposed in [19] and [20]. As a public-key cryptography scheme, it utilizes the algebraic structure of elliptic curves. With a generator or base point G , the public key and its corresponding private key will have a relationship as follows.

$$Puk = Prk * G \quad (1)$$

where Puk and Prk are the public key and private key respectively. Both of them belong to the same elliptic curve. The ECC works are based on the fact that in a finite field, it is hard to find Prk with Puk and G , but the reverse procedure is not difficult.

The beauty of the ECC is that it requires a smaller storage size and less information exchange than other kinds of cryptography mechanism. Typically, in term of key size, ECC is more efficient than the famous RSA algorithm [13]. With a key size of 160 bits, an ECC algorithm system could provide a similar security level that can be offered by a RSA algorithm system with a key size of 1024 bits. In order to reduce the computational cost of a handover scheme, a proxy signature based on ECC has been proposed in [12]. In this paper, we design the proposed scheme based on the ECC scheme to achieve the mutual authentication with a lower computational cost. Although symmetric cryptography is lightweight and faster, asymmetric cryptography is much more secure and flexible. For example, by the symmetric cryptography, keys are generated based on initial keys or shared secret, while by the asymmetric cryptography, session keys can be generated without prior knowledge, which is much more flexible than that of the symmetric cryptography. Since ECC has a smaller key size and faster computation than RSA, it is feasible to be applied in common network environments.

3. The Proposed Scheme - EPH Scheme

3.1 Overall Description

Our proposed EPH scheme has adopted the proxy signature scheme introduced in [12]. By the EPH scheme, a cyclic group, denoted as C , is selected for the ECC by a generator in the network. This C is assumed to be public and known to all parties in the networks. C is selected such that its order is a prime number p where $|p| = 160$ bits. A base point of C is denoted as G . In the network, each entity has its own public key and private key selected from C . The public key of an entity i is denoted as Y_i and the private key of it is denoted as X_i . Based on Equation 1, $Y_i = X_i G$. The private key of any entity is selected so that it belongs to Z_p^* . Three hashing functions are used in the system. They are denoted as $h_1(): \{\}^* \rightarrow \{\}^n$, $h_2(): C \rightarrow \{\}^n$ and $h_3(): \{\}^* \rightarrow Z_p^*$.

The entire scheme consists of two phases: attach phase and handover phase. The attach phase describes the process of authentication and proxy delegation generation which occurs when a UE or a base station first enters the network. The handover phase, on the other hand, presents the handover process as the UE moves from one cell to another. There is a slight difference in the process of authentication among the following three scenarios. First, the target base station is associated with the same MME as the current base station. Second, the target base station is a HeNB whose access mode is not an open access mode. Third, the target base station is connected to a new MME.

3.2 Attach Phase

In the attach phase, the public key of HSS and MME Y_{HSS} and Y_{MME} are assumed to be public. Since the eNBs/HeNBs, the MMEs and the HSS are connected through wired links, there are many mature and proven protocols applied in wired links such as Internet Protocol Security (IPsec) and Internet Key Exchange version 2 (IKEv2) can be used for protecting the traffic and establishing shared secret keys among them. It is assumed that the MME and HSS have a secret key K_{MH} for the communication based on these protocols. Figure 1 shows the steps of the execution of the attach phase.

1. As the Evolved Packet System Authentication and Key Agreement (EPS-AKA) scheme [21], the attach phase is initiated by an UE. The UE first sends an attach request containing its International Mobile Subscriber Identity (IMSI) number to the MME which is encrypted with the public key of MME.
2. Received the attach request sent by the UE, the MME forwards the IMSI of the UE to the HSS by sending the attachment data request to it. This message is encrypted with K_{MH} . The first two steps are the same as that in the EPS-AKA.

3. After the attachment data request is received, a proxy warrant w_{UE} for the UE, which defines the expiration time of the proxy delegation, is chosen by the HSS for the validation of the effectiveness of the proxy delegation. If the warrant is expired, a message should be sent to the HSS to request a valid warrant. A random number r ($r \in Z_p^*$) is also generated in order to compute the proxy delegations. The proxy delegation pair (m_{UE}, n_{UE}) of the UE is generated as follows.

$$m_{UE} = rG \quad (2)$$

$$n_{UE} = X_{HSS} h_3(w_{UE}, h_2(m_{UE})) + r \quad (3)$$

Finally, a data response message with (m_{UE}, n_{UE}, w_{UE}) and authentication vectors (AVs) are sent to the MME. The AVs defined in [21] contains the authentication information such as authentication token (AUTN) and K_{ASME} . These parameters are encrypted with K_{MH} .

Figure 1. The Attach Phase

4. The MME decrypts the received message with K_{MH} . Then it authenticates the UE as at the step 4 and 5 in EPS-AKA. An AV is selected by the MME included in the user authentication request which will be sent to the UE. The UE responds to this request with the User Authentication Response. If the random numbers sent in both the request and the response are the same, it proves that both parties have a copy of K_{ASME} . If the UE is successfully verified by the MME, the proxy delegations (m_{UE}, n_{UE}, w_{UE}) encrypted with K_{ASME} will be forwarded to the UE.

5. The UE decrypts the message with K_{ASME} and validates the received delegation by checking if the following equation holds.

$$n_{UE}G = X_{HSS}h_3(w_{UE}, h_2(m_{UE}))G + rG = h_3(w_{UE}, h_2(m_{UE}))Y_{HSS} + m_{UE} \quad (4)$$

If the verification fails, the UE sends an authentication reject message to the HSS to request a valid proxy signature. Otherwise, the UE computes its public and private keys as follows.

$$X_{UE} = n_{UE} \quad (5)$$

$$Y_{UE} = n_{UE}G \quad (6)$$

Similarly, an eNB receives $(m_{eNB}, n_{eNB}, w_{eNB})$ from the HSS and computes X_{eNB} and Y_{eNB} .

The UEs and base stations will have their proxy signatures generated by the HSS after this initial attach phase. These signatures are the tools for the authentication in the handover phase.

3.3 Handover Phase

The handover phase of EPH scheme will be discussed in three different scenarios. The first scenario, the handover from a base station to a base station connected to the same MME as the current base station, is referred to as a normal handover process. The second scenario is the handover process, which occurs when the target base station is a HeNB. The third scenario is the handover process to a base station which is connected to a new MME. Since each of other two handover processes needs to go through the steps in the normal handover process to achieve a mutual authentication first then followed by additional steps, the referred base station could be the eNB or HeNB connected to the same MME and the eNB or HeNB connected to different MME.

3.3.1 Normal Handover Phase

The overall normal handover phase is shown in Figure 2.

1. The UE searches for the legitimate base stations first. It could get a list of public keys of the nearby eNBs from a current eNB. Or, if it enters the coverage of a new MME, it could get a list of the public keys from the MME.
2. After a legitimate base station is found, the UE generates a random number $r_{UE} (\in Z_p^*)$. The authentication signature s_{UE} is then generated using this random number and other parameters as follows.

$$PK_{UE} = r_{UE}Y_{eNB} \quad (7)$$

$$R_{UE} = r_{UE}G \quad (8)$$

$$s_{UE} = X_{UE} - r_{UE}h_3(h_2(PK_{UE}), h_2(R_{UE}), h_1(I_{UE})) \quad (9)$$

Besides, it computes an information parameter I_{UE} which contains the necessary information for the authentication and communication such as its temporary ID, Globally Unique Temporary Identity (GUTI) and the security capabilities of the UE which are sets of identifiers related to ciphering and integrity algorithms applied in the UE.

Then, the handover request $(R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE})$ is sent to the target base station.

3. Receiving the handover request $(R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE})$, the base station first checks whether the proxy delegation is overdue by checking the w_{UE} , which defines the expiration time of the proxy delegation. The definition of the proxy warrant w_{UE} and the way to verify whether it is expired are introduced at the third step in the attach phase. If it is, the handover request is rejected and the UE will request for a new proxy delegation from the HSS. Otherwise, the base station computes PK_{UE} as shown in Equation 10. In case that an attacker could alter the expiration time, the proxy warrant w_{UE} and other handover information will be authenticated by checking if Equation 11 holds.

$$PK_{UE} = r_{UE}Y_{eNB} = r_{UE}X_{eNB}G = R_{UE}X_{eNB} \quad (10)$$

$$s_{UE}G + R_{UE}h_3(h_2(PK_{UE}), h_2(R_{UE}), h_1(I_{UE})) = X_{UE}G = h_3(w_{UE}, h_2(m_{UE}))Y_{HSS} + m_{UE} \quad (11)$$

If the two sides of Equation 11 equal to each other, the authentication of the UE by the base station is successful. If they are not equal, the base station will send a handover failure message.

4. If the UE is successfully authenticated, the base station chooses a new random number $r' (\in Z_p^*)$ and computes R' and session key K as follows.

$$R' = r'G \quad (12)$$

$$K = r'R_{UE} \quad (13)$$

Besides, the base station chooses another random number $r_{eNB} (\in Z_p^*)$ and computes its own authentication signature s_{eNB} as follows.

$$PK_{eNB} = r_{eNB}Y_{UE} \quad (14)$$

$$R_{eNB} = r_{eNB}G \quad (15)$$

$$s_{eNB} = X_{eNB} - r_{eNB}h_3(h_2(PK_{eNB}), h_2(R_{eNB}), h_2(R'), h_1(I_{eNB})) \quad (16)$$

After the authentication signature s_{eNB} is calculated, the base station computes a I_{eNB} which contains the necessary information such as the selected encryption algorithm. The eNB sends message $(R_{eNB}, s_{eNB}, m_{eNB}, w_{eNB}, R', I_{eNB})$ to the UE. The proxy warrant w_{eNB} for the eNB,

which defines the expiration time of the proxy delegation, is chosen by the HSS for the validation of the effectiveness of the proxy delegation. If the warrant is expired, a message should be sent to the HSS to request a valid warrant.

Figure 2. The Normal Handover Phase

5. Receiving the message, the UE first checks whether the proxy delegation is overdue by checking

the w_{eNB} , which also defines the expiration time of the proxy delegation for eNB. The definition and the verification of proxy warrant w_{eNB} are presented at the fourth step in the normal handover phase. The base station needs to request for a new set of proxy delegations and proxy warrant from the HSS. Otherwise, the UE authenticates the target base station by first computing PK_{eNB} as shown in Equation 17. Then, the proxy warrant w_{eNB} and other handover information are authenticated by checking if Equation 18 holds.

$$PK_{eNB} = r_{eNB}Y_{UE} = r_{eNB}X_{UE}G = X_{UE}R_{eNB} \quad (17)$$

$$\begin{aligned} & s_{eNB}G + R_{eNB}h_3(h_2(PK_{eNB}), h_2(R_{eNB}), h_2(R'), h_1(I_{eNB})) \\ &= X_{eNB}G = Y_{HSS}h_3(w_{eNB}, h_2(m_{eNB})) + m_{eNB} \end{aligned} \quad (18)$$

If the base station cannot be successfully authenticated, a handover failure message will be sent. The UE may then search for a new legitimate base station as the handover process starts from Step 1 again. Otherwise, the session key K is computed at the UE side as follows.

$$K = r_{UE}R' \quad (19)$$

If the computation is correct without a fault, the session key will be the same as what the base station has got from Equation 13. In order to confirm the session key agreement, the UE sends $(h_1(h_2(K) \parallel h_2(PK_{UE}) \parallel h_2(R_{UE})))$ to the target base station.

6. The eNB checks the value of $h_1(h_2(K) \parallel h_2(PK_{UE}) \parallel h_2(R_{UE}))$. If the computed value equals to the received one, the handover process is over and a message is sent to the MME to inform that a new connection has been established.

The normal handover phase ends to make that the new eNB can provide service for the UE.

3.3.2 Handover to a HeNB

If the target base station is a HeNB, there may be some more steps for checking the membership of the UE. If the HeNB is in the open access mode, since its behavior is the same as those normal eNB, the handover process is also the same. Otherwise, the membership of the UE will be checked as follows between Step 3 and 4 of the normal handover phase. Please note that if the HeNB is not associated with the same MME as the current connected base station, the membership of the UE will be checked after the handover between two MMEs is completed.

1. The UE searches for the legitimate base stations first. It could get a list of public keys of the nearby HeNBs from a current HeNB. Or, if it enters the coverage of a new MME, it could get a list of the public keys from the MME.

2. After a legitimate base station is found, the UE generates a random number $r_{UE}(\in Z_p^*)$ and generate the handover request $(R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE})$ as in the step 2 in the normal handover phase. Then the handover request is sent to the target base station.
3. Upon receiving the handover request, the base station first checks whether the proxy delegation is overdue by checking the w_{UE} . If it is, the handover request is rejected and the UE will request for a new proxy delegation from the HSS. Otherwise, the base station computes PK_{UE} and authenticates the UE. If the authentication of the UE by the base station fails, the base station will send a handover failure message.
4. After authenticating the handover request from the UE, the HeNB will send the necessary information, mainly included in I_{UE} , to the MME. Examples of necessary information are the CSG ID and the Cell Access Mode (CAM) of the HeNB.
5. The MME checks the CSG ID and the CAM of the HeNB. If the HeNB operates in the closed access mode, the MME will determine if the UE is allowed to access it. If the HeNB operates in the hybrid access mode, the priority of the UE will be determined and the UE access control is performed. If it is found that the UE is not allowed to access, the MME will send a handover failure message to both the MME and the UE. The UE will then search for another base station. Otherwise, the MME will send a handover request acknowledgement (ACK), which contains the priority level of the UE if the HeNB is in the hybrid access mode, to the HeNB. If a handover request ACK is received, the HeNB will proceed.
6. If the UE is successfully authenticated, the base station chooses a new random number $r'(\in Z_p^*)$ and computes R' and session key K as in the step 4 in the normal handover phase. Besides, the base station chooses another random number $r_{HeNB}(\in Z_p^*)$ and computes its own authentication signature s_{HeNB} . After the authentication signature s_{HeNB} is calculated, the base station sends message $(R_{HeNB}, s_{HeNB}, m_{HeNB}, w_{HeNB}, R', I_{HeNB})$ to the UE.
7. Receiving the message, the UE first checks whether the proxy delegation is overdue by checking the w_{HeNB} . If it fails, the base station needs to request for a new set of proxy delegations and proxy warrant from the HSS. Otherwise, the UE authenticates the target base station by first computing PK_{HeNB} and then verify the signature. If the base station cannot be successfully authenticated, a handover failure message will be sent. The UE may then search for a new legitimate base station as the handover process starts from Step 1 again. Otherwise, the session key K is computed by $K = r_{UE}R'$. If the computation is correct, the session key will be the same as what the base station has. In order to confirm the session key agreement, the UE sends $(h_1(h_2(K) \parallel h_2(PK_{UE})) \parallel$

$h_2(R_{UE}))$ to the target base station.

8. The HeNB checks the value of $h_1(h_2(K) \parallel h_2(PK_{UE}) \parallel h_2(R_{UE}))$. If the computed value equals to the received one, the handover process is over and a message is sent to the MME to inform that a new connection has been established.

3.3.3 Handover to a Base Station Associated with Other MME

If the target base station is not associated with the same MME as the current serving base station, besides the steps of normal handover phase, the handover between two MMEs should be performed between step 3 and 4 in the normal handover phase as follows. If the target base station is a HeNB, the membership of the UE will be checked after the handover between two MMEs is completed.

1. The target base station will send the necessary information mainly included in I_{UE} to the MME that controls it. Examples of the necessary information are the UE's GUTI and the source MME ID (GUMMEI).
2. The target MME checks the GUTI and GUMMEI to determine the current MME address. After the MME address is identified, an identification request is sent to it.
3. The current MME responds to the request by sending an Identification Response message, which contains the information about the UE such as the IMSI number, security context and network capability of the UE.
4. Upon receiving the Identification Response, the target MME sends a Handover Request ACK to the target base station.

If the target base station is a HeNB which is not in the open access mode, it will then proceed with the membership checking of the UE. Otherwise, it will proceed to step 4 of the normal handover phase.

After the handover process is completed, the new MME will send a Forward Relocation Complete Notification to the source MME and the source MME will reply with a Forward Relocation Complete ACK Message.

4. Logic Prove and Formal Verification

In this section, we will prove the logic correctness of the proposed scheme by BAN Logic and formally verify the proposal by SPIN.

4.1 Logic Prove

As a logic of belief, BAN Logic is widely used to express, analyze and prove the logic correctness of various protocols including security protocols. The basic intention of BAN Logic is to verify that if honest principals correctly execute a protocol, the expected result of the protocol execution can be reached. [22]

By BAN Logic, there are four steps of proving the logic correctness of a given protocol using BAN logic: 1) Idealize the protocol: By this step, the source of the messages and the plaintexts of the encrypted message will be specified. The protocol is written in the idealized form. 2) Specify the assumptions about the initial state: By this step, initial assumptions are specified, such as which two entities share the session key. 3) Annotate the protocol: Based on step 1 and 2, the idealized protocol is annotated with assertions. 4) Derive the beliefs held by the protocol principals: Based on step 3, the conclusion on whether the security goal has been achieved or not will be derived using the BAN logic rules.

A protocol is usually first idealized into the messages that are suitable to be approved. The idealization process typically involves two changes. The first one is that the messages are transferred into assertions. The second one is that plain text messages will be omitted. After that, the assumptions about beliefs will be made. One example of such kind of assumptions is that “A believes that k is a good key for communication between A and B”. Based on the idealized messages and assumptions, deductions could be reached by using the BAN Logic rules. There are totally six BAN Logic rules, namely, message meaning, nonce verification, jurisdiction, belief conjunction, freshness conjunction and receiving rules.

Both phases of the EPH scheme have been logically proved by BAN Logic. In the model of the two phases, the UE is denoted as ‘ U ’, the base station is denoted as ‘ N ’, and the MME is denoted as ‘ M ’.

4.1.1 Prove of Attach Phase

The attach phase is idealized to six messages as follows.

Message 1: $U \rightarrow M: \{U\}_{Y_{MME}}$ from U

The UE sends its identifier, IMSI to MME for the authentication.

Message 2: $M \rightarrow H: \{U\}_{K_{MH}}$ from M

If the identifier is valid, this message is forwarded to HSS for the computation of proxy delegations.

Message 3: $H \rightarrow M: \{m_{UE}, n_{UE}, w_{UE}\}_{K_{MH}}$ from H .

H computes the proxy delegation and sends it to M .

Message 4 and 5 are not included because they are similar to the authentication request and response of the EPS-AKA. The most important effect of these two messages is that the MME authenticates the UE and both parties have a copy of K_{ASME} .

Message 6: $M \rightarrow U: \{m_{UE}, n_{UE}, w_{UE}\}_{K_{ASME}}$ from M .

In order to analyze the attach protocol, following assumptions are made.

A1. U believes $PK(M, Y_{MME})$

A2. H believes $M \xleftrightarrow{K_{MH}} H$

A3. M believes $M \xleftrightarrow{K_{MH}} H$

A4. U believes $PK(H, Y_{HSS})$

A5. U believes $M \xleftrightarrow{K_{ASME}} U$

The idealized protocol can be expressed as follows.

B1. M received (U) .

B2. H received $\{U\}_{K_{MH}}$.

B3. M received $\{m_{UE}, n_{UE}, w_{UE}\}_{K_{MH}}$.

B4. After authentication, M believes U said $\{U, n, U \xleftrightarrow{K_{UM}} M, \text{fresh}(K_{UM})\}_p$.

B5. U received $\{m_{UE}, n_{UE}, w_{UE}\}_{K_{ASME}}$.

Finally, the following derivations can be made.

C1. Using A2 and B2, by Receiving Rules:

H received (U) .

C2. Using A3 and B3, by Receiving Rules:

M received (m_{UE}, n_{UE}, w_{UE}) .

C3. Using A5 and B5, by Receiving Rules:

U received (m_{UE}, n_{UE}, w_{UE}) .

C4. Using A4 and C3, by Message Meaning:

U believes H said (m_{UE}, n_{UE}, w_{UE}) .

As shown above, the UE could finally receive its proxy delegation and it believes that the proxy delegations have been really sent by the HSS. Therefore, these proxy delegations are assumed to be legitimate. After C4 is verified, the UE will then verify the proxy signatures.

4.1.2 Prove of Handover Phase

The handover phase is analyzed as follows.

The handover phase is first idealized to three messages as follows.

Message 1: $U \rightarrow N$: $R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE}$ from U

The UE sends handover request to the eNB. The eNB checks the validity of w_{UE} .

Message 2: $N \rightarrow U$: $R_{eNB}, s_{eNB}, m_{eNB}, w_{eNB}, I_{eNB}, R', n$

The eNB sends back its own signature and proxy delegations.

Message 3: $U \rightarrow N$: $\{SKA\}_{Y_{UE}^{-1}}$

As a result, both parties will get the same copy of session key.

In order to analyze the handover protocol, following assumptions are made.

D1. U believes $PK(N, Y_{eNB})$.

D2. U believes $fresh(n)$.

D3. If the UE is authenticated, N believes U said $(R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE})$ and $PK(U, Y_{UE})$.

D4. If the eNB is authenticated, U believes N said $(R_{eNB}, s_{eNB}, m_{eNB}, w_{eNB}, I_{eNB}, R')$.

The idealized protocol can be expressed as follows.

E1. N received $\{R_{UE}, s_{UE}, m_{UE}, w_{UE}, Y_{UE}, I_{UE}\}$.

E2. U received $\{R_{eNB}, s_{eNB}, m_{eNB}, w_{eNB}, I_{eNB}, R'\}$

E3. N received $\{SKA\}_{Y_{UE}^{-1}}$

Therefore, we could deduce the following conclusion.

F1. Using D3 and E3, by Message meaning,

N believes U said (SKA) .

As shown above, the base station believes that the session key agreement received is sent by the UE. It will then verify the session key agreement. Both parties now have a copy of session key and the

following conversation can be encrypted with it.

4.2. Formal Verification

As one of the most popular tools for verifying the logic correctness of software models, SPIN is capable of a couple of powerful features [23]. It is a design tool to develop complex system models. It is also an automatic verification tool to simulate the designed system described by the SPIN model. SPIN is capable of checking the logic correctness of a system by checking the fact that if there are any deadlocks or unreachable states presented by the SPIN model. The PROMELA language is the specification language used by SPIN to describe the system under the verification.

In this section, the proposed EPH scheme has been modeled and verified by using the SPIN model checker. In order to verify the EPH Scheme, two models, including the model of the process of proxy delegations generation and the model of the actual handover process, have been developed. Eventually, it has been proved that both processes can reach the expected end states and there is no endless loop or unexpected end state existing in the model executions. It indicates that the proxy delegation can be successfully distributed and the handover process can be carried out successfully.

4.2.1. Verification of the Proxy Delegation Generations

To verify the proxy delegations generations, three processes have been created. These three processes are called HSS, UE and MME, each of which represents an entity in the system as indicated by the title of the process. Each of the processes holds certain necessary data objects as variables. The global data objects are the generator G and the public key of HSS, Y_{HSS} . The hashing functions are defined at the very beginning. Again, all of them are represented by simple functions. Five channels have been defined for the processes to exchange message among each other.

In the specification, the UE sends the first message to the MME and starts the entire process. Upon receiving the message, the MME sends another message to the HSS. The HSS then computes the proxy delegation, which is sent to the MME. Since the process for authentication of the UE is the same as EPS-AKA, it is modeled only by two messages exchange between the UE and the MME. After this process, the MME forwards the proxy delegation data to the UE. The UE then checks the received data. In the execution of the models, the scheme is shown to be comprised of 31 steps. It has been shown that there are totally 20 states in the verification.

4.2.2 Verification of Handover Process

To verify the handover process, two processes have been created. The title of one process is called the UE and the other is the eNB. Each of them represents an entity in the system as indicated by the

title of the process. Each of the processes holds certain necessary data objects as variables. The global data objects are the generator G , the public key the HSS Y_{HSS} and the public key of the base station Y_{eNB} . The hashing functions have been defined at the very beginning. Again, all of them are represented by simple functions. Three channels have been defined for the processes to exchange information from each other. Only the normal handover phase has been modeled to be verified because the additional steps for handover to a HeNB or a base station associated with a new MME will not have significant impact over the verification.

In the model, the UE first initiates the whole process by computing its own authentication signature. It then sends the corresponding parameters to the eNB. Since the parameter I_{UE} is not used in computation, it is omitted in the model. Upon receiving the message, the eNB checks them and its own signature is generated and necessary data will be sent back to the UE. The UE then checks the received data to compute a session key agreement and sends it to the eNB. The eNB ends the whole process by checking the correctness of it. In the execution of the verification, the whole scheme is shown to be comprised of 61 steps. It has been shown that there are totally 27 states in the verification.

5. Security and Performance Analysis

5.1 Security Analysis

Besides the logic prove and the formal verification of the proposed scheme, we further carry out security analysis to evaluate the proposed EPH scheme to satisfy various security properties. The attackers assumed in the EPH scheme are able to decrypt or encrypt messages if obtaining the corresponding secret key. Attackers can alter, construct, decompose or inject any messages and send them to any legitimate entity. However, the adversaries are unable to guess a random number, which is chosen from a sufficiently large space. The attacker also cannot retrieve the information from a given ciphertext or generate a valid ciphertext from a given plaintext without a complete and correct key. Besides, a private key that matches a given public key cannot be calculated.

The scheme can provide strong unforgeability. Unforgeability is one of the main properties of the proxy signature. Since only the party who has been delegated the signing ability is able to generate a proxy signature, it is impossible for an unauthorized party to forge a proxy signature. This unforgeability is ensured by the security of the ECC because the proxy delegations are generated using the private key of the HSS and the proxy signature algorithm works based on ECC.

The scheme can provide authenticity to both the base station and the UE. As mentioned above, it is

impossible to forge a proxy delegation given by the HSS and the HSS issues proxy delegation only to the legitimate base stations and UEs. Therefore, both of them can authenticate each other by checking the validity of the proxy signature and the authenticity of both parties can be ensured.

The HSS cannot deny the fact that it has issued a proxy signature to an UE or base station. Since the proxy delegations are generated using the private key of the HSS and they will then be checked by the corresponding public key, the HSS is unable to deny its proxy delegation.

The scheme can protect the network against man-in-the-middle attacks. In the process of key agreement, instead of sending the value of the session key itself, the value of R' is sent. Besides, the message is sent with the public key of the UE. Therefore, even though an attacker manages to intercept the message, he cannot get the session key.

Again since by the EPH scheme, the session key is not directly sent by the base station, the replay attacks can be prevented. An attacker may be able to capture a copy of the UE's connection request. He, however, will not be able to reply the message sent back by the base station. In addition, an attacker may also be able to capture the base station's reply message and try to masquerade as the base station. Nevertheless, since random numbers have been used in each connection, the UE will not accept the replay responses.

Lastly, the proposed EPH scheme can provide a strong backward and forward security. Even if a communication party is compromised, the attacker is not able to obtain the historical information because a random number is used in the authentication process and the generation of the session keys. Therefore, even if the private key of an UE or a base station has been leaked out, the historical data could not be leaked out. Besides, one might argue that since the public key of the target base station is obtained from the serving base station, it is possible that the serving base station is compromised and the public key list kept at it is altered so that the attacker can masquerade as a base station. However, since the proxy signature of the base station has also been verified in the authentication process, the UE will refuse to communicate with the forged base station and get the public key of another base station from the MME. Last but not least, the backward security is also ensured by the fact that the key chain structure is not used in the EPH scheme. This is because even if the session key of one session is obtained by the attacker, he is able to derive the forward session key with it because the previous keys have no connection with the current key.

5.2. Performance Analysis

In this section, the performance of the proposed EPH scheme is evaluated in terms of the computation costs of major cryptography algorithms required to complete the authentication for the

handovers. Furthermore, the computation cost of the proposed EPH scheme is compared with the Jing's scheme in [10], the Cao's scheme in [11], the Choi's scheme in [25] and the Secure Fast Roaming Scheme in Wireless LAN Using ID-based Cryptography (SFRIC) scheme in [24]. These schemes have been selected to compare the performance differences due to their similarity in the system architecture and the handover scenarios.

The computational cost of each primitive cryptography algorithm has been estimated by using C/C++ OPENSLL library [26]. In the evaluation, we have taken the parameters with the values same as those in the evaluation in [11]. The UE is modeled using a Celeron 1.1 GHz processor and the eNB is modeled using a Dual-Core 2.6 GHz processor. The cost of certain kinds of computation such as arithmetic multiplication has been negligible compared to other major computation. The individual time taken to perform the security algorithms for the execution of the proposed EPH scheme is shown in Table 1, while the performance comparison among different security schemes has been shown in Table 2, where only the solutions by asymmetric encryption methods have been listed. Although it is true that the solutions by the symmetric cryptography can achieve a better performance, the solutions by the asymmetric cryptography can offer higher secure protections and more flexible key establishments. As shown in Table 2, the computational cost, which is crucial for a mobile network, of the EPH scheme is significantly smaller than that of the solutions in [11][24][25]. Although the computational cost of the solutions in [10] is the same as ours scheme, by the solutions in [10], the authenticity of the eNB, which the UE is going to attach to, cannot be verified.

Table 1. Computational Costs of the Primitive Cryptography Functions

Computation type	Symbol	Cost of UE (ms)	Cost of eNB (ms)
Modular exponentiation	T_e	1.7	0.5
RSA verification	T_{RV}	1.0	0.3
Elliptic Curve Point Multiplication	T_M	1.5	0.5
Tate Pairing	T_P	38	16

Table 2. Computational Costs of Different Schemes

	Jing (ms)	Cao (ms)	SFRIC (ms)	Choi (ms)	EPH (ms)
UE	$2T_M = 3$	$5T_e + T_M = 10$	$T_M + 2T_P = 77.5$	$4T_e + T_{RV} = 7.8$	$3T_M = 4.5$
eNB	$6T_M = 3$	$5T_e + T_M = 3$	$T_M + 2T_P = 32.5$	$4T_e + T_{RV} = 2.3$	$3T_M = 1.5$
Total	6	13	110	10.1	6

6. Conclusion

In this paper, an authentication scheme for the handover in LTE cellular networks, EPH, has been proposed which works based on a proxy signature algorithm. The logic correctness of the EPH scheme has been proved and formally verified. By the security analysis, the EPH scheme is able to provide strong unforgeability, authenticity, backward security and several other security properties. Besides, the performance of the EPH scheme has been evaluated in term of computation cost to show that the proposed scheme has a lower computation resource requirement compared to other existing asymmetric authentication solutions.

Reference

- [1] S. Sesia, I. Toufik, and M. Baker (Eds.), *LTE: The UMTS Long Term Evolution: from Theory to Practice*, John Wiley and Sons, 2011.
- [2] D. Forsberg, "LTE Key Management Analysis with Session Keys Context", *Computer Communications*, Vol. 33, No. 16, Oct. 2010, pp. 1907-1915.
- [3] C. K. Han, H. K. Choi, and I. H. Kim, "Building Femtocell More Secure with Improved Proxy Signature," *Proceedings of IEEE GLOBECOM 2009*, Dec. 2009, pp.1-6
- [4] J. Cao, M. Ma, H. Li, and Y. Zhang, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Communications Surveys & Tutorials*, No.99, pp.1-20
- [5] A. Mishra, M. Shin, and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", *ACM SIGCOMM Computer Communication*, Vol.33, No. 2, Feb. 2003. pp. 93-102.
- [6] Z. Wang, C. Fan, Y. Wang, and D. Yang, "A Novel Network Architecture for 3G Evolution," *Proceedings of IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications 2006*, Sept. 2006, pp.1-5.
- [7] A. Bohk, L. Butryn, and L. Dra, "An Authentication Scheme for Fast Handover between WiFi Access Points," *Proceedings of ACM Wireless Internet Conference 2007*, Oct. 2007, pp.22-24.
- [8] A. Mishra, H. S. Min, N. L. Petroni, Jr, T.C. Clancy, and W. A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," *IEEE Wireless Communications*, Vol. 11, No.1, Feb. 2004, pp.26-36.
- [9] Y. E. H. E. Idrissi, N. Zahid, and M. Jedra, "Security Analysis of 3GPP (LTE) — WLAN Interworking and A New Local Authentication Method Based on EAP-AKA," *Proceedings of International Conference on Future Generation Communication Technology 2012*, Dec. 2012, pp.137-142.
- [10] Q. Jing, Y. Zhang, A. Fu, and X. Liu, "A Privacy Preserving Handover Authentication Scheme for EAP-Based

Wireless Networks," *Proceedings of IEEE GLOBECOM 2011*, Dec. 2011, pp.1-6.

[11] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks," *Computer Networks*, Vol. 56, No. 8, May 2012, pp. 2119-2131.

[12] C. Ma, K. Xue, and P. Hong, "A Proxy Signature-Based Re-authentication Scheme for Secure Fast Handoff in Wireless Mesh Networks", *International Journal of Network Security*, Vol. 15, No.1, Jan. 2013, pp.104-114.

[13] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Proceedings of ACM Communications* 1978, Feb. 1978, pp. 120-126.

[14] Y. S. Chen, T. Y. Juang, Y. T. Lin, "A Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6 in 3GPP LTE Systems," *Wireless Personal Communications*, Vol. 61, No. 4, Dec. 2011, pp 629-656.

[15] I. E. Bouabidi, I. Daly and F. Zarai, "Secure handoff protocol in 3GPP LTE networks," *Proceedings of Third International Conference on Communications and Networking*, 2012, pp. 1-6.

[16] M. Mambo, K. Usuda, and E. Okamoto,"Proxy signatures: Delegation of the Power to Sign Messages", *IEICE Transaction of Fundamentals*, Vol. E79-A, No. 9, Sep. 1996, pp. 1338-1353.

[17] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited", *Proceedings of, International Conference on Information and Communications Security 1997, Lecture Notes in Computer Science*, LNCS 1334, 1997, pp.223-232,

[18] C. P. Schnorr, "Efficient Signature Generation by Smart Cards", *Journal of Cryptology*, Vol. 4, No. 3, Mar. 1991, pp. 161-174.

[19] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol.48, No.177, 1987, pp. 203-209.

[20] V. Miller, "Use of Eliptic Curves in Cryptography". *CRYPTO 85*, 1985, pp. 417-426.

[21] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); *Security architecture (Rel 11)* 3GPP TS 33.401 V11.0.1 (2011).

[22] P. Syverson and I. Cervesato, "The Logic of Authentication Protocols", *Foundations of Security Analysis and Design*, 2001.

[23] G. J. Holzmann, *The SPIN Model Checker - Primer and Reference Manual*, Addison-Wesley, 2003.

[24] Y. Kim, W. Ren, J. Jo, M. Yang, Y. Jiang, and J. Zheng, "SFRIC: A Secure Fast Roaming Scheme in Wireless LAN Using ID-based Cryptography," *Proceedings of IEEE ICC 2007*, June 2007, pp. 1570-1575.

[25] J. Choi, and S. Jung, "A Handover Authentication Using Credentials Based on Chameleon Hashing," *IEEE Communications Letters*, Vol.14, No.1, Jan. 2010, pp.54-56.

[26] OPENSSL, <http://www.openssl.org/>.