Security Enhanced Authentication and Key Agreement Protocol in Next Generation Mobile Network

Li Xiehua, Wang Yongjun

Abstract

The 3rd Generation Partnership Project (3GPP) standard is developing System Architecture Evolution (SAE) / Long Term Evolution (LTE) for the next generation mobile communication system. In the SAE/LTE architecture, EPS AKA (Evolved Packet System Authentication and Key Agreement) procedure is used to provide mutual authentication between the UE (User Equipment) and the serving network. However, the EPS AKA has several vulnerabilities such as disclosure of user identity, man-in-middle attack, etc. Therefore, this paper analyzes the deficiencies of the EPS AKA, and proposes a Security Enhanced Authentication and Key agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI). Then, the new SE-EPS AKA has been proved with the formal verification method, and the proof result shows that the SE-EPS AKA can satisfy the security and efficiency properties in the SAE/LTE architecture.

Keywords: SAE/LTE Network, EPS AKA, WPKI, Formal Verification

1. Introduction

For the openness of the radio channels and randomness of the user’s mobility, the security of mobile communication system has considered as one of the most challenging problems [1]. As a critical security mechanism, the authentication and key agreement protocol has received considerable attention since its introduction into mobile communication system. With the continuous evolution of mobile communication system, GSM AKA [2], UMTS AKA [3] and EPS AKA [4] had been proposed one after another. UMTS AKA is a development of GSM AKA proposed by 3GPP (the 3rd Generation Partnership Project), which is based on the security characteristics of 2G network and the new security requirements of 3G infrastructure. However, due to processing mechanism and key cryptosystem, there are some deficiencies in this protocol, the subscriber’s identity information is easy to be tapped, the mutual authentication mechanism between wired parties are not provided, the operation of sequence numbers is difficult, and the non-repudiation proof cannot be proved, etc. Recently, to address the existence and latent security flaws of UMTS AKA, 3GPP has researched on the authentication and key agreement protocol which is suitable for the IP-based next generation mobile communication system SAE/LTE. EPS AKA adopted by 3GPP Evolved Packet System is the preliminary research results. The protocol retains the framework of the UMTS AKA, and improves the security and performance by increasing several security elements. But the related researches show that the protocol still has some security flaws, it can’t fulfill the security requirements of SAE/LTE network [5-9].

In order to put fully protection for the SAE/LTE network, this paper analyzes the deficiencies of the EPS AKA protocols, and then proposes a Security Enhanced Authentication and Key agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure [11]. By using the ECC (Ellipse Curve Cipher) encryption, the newly proposed protocol protects the security of user identity and the exchanged information with limited energy consumption. Through the formal verification with the Strand Space Model and Authentication Tests [12,13], the SE-EPS AKA protocol is proved to be secure and efficient.

The rest of this paper is organized as followed: section 2 analyzes the EPS AKA protocol in contrast with UMTS AKA protocol; section 3 puts forwards a security-enhanced authentication and key agreement protocol based on WPKI; section 4 verifies the proposed protocol with strand space model and authentication test; and the last section concludes the whole paper.
2. Analysis of EPS AKA

EPS AKA is evolved from UMTS AKA and follows the realization mode of “challenge/response” under the precondition of mutual successful authentication. Some fundamental elements of UMTS AKA, such as USIM (Universal Subscriber Identity Module), have been reused in EPS AKA. However, compared with UMTS AKA, the security infrastructure and encryption in EPS have been modified for security enhancement.

2.1. Authentication procedure of EPS AKA

In EPS, Mobility Management Entity (MME) plays a role comparable to that of the Visitor Location Register (VLR), moreover, the MME performs additional functions. The User Equipment (UE) and the Home Subscriber Server (HSS) play the similar roles in both EPS AKA and UMTS AKA, in addition, the UE includes the Universal Subscriber Identity Module (USIM) and Mobile Equipment (ME) in this article. An overview of the EPS AKA procedure is shown in Figure 1. There is no self-contained description of the EPS AKA procedure in the main references for EPS security [4], the EPS AKA procedure in Figure 1 is described by adapting and explaining relevant text from [3] and [4].

![Figure 1. Procedure of EPS AKA protocol](image)

The detailed procedure of EPS AKA protocol is described as follows:

1. When the user registers for the first time in a serving network, the user identity request is invoked by MME in the serving network;
2. As the response, UE sends its IMSI to MME. And MME transmits the authentication data request to the HSS with the IMSI, SNID (Serving Network Identity) and the serving network type.
3. Upon the receipt of the Authentication Information Request from MME, the HSS may have pre-computed authentication vectors available and retrieve them from the HSS database, or it may compute them on demand.
4. The HSS sends an Authentication Information Answer back to the MME that contains an ordered array of \( n \) EPS authentication vectors \( AV(1…n) \). If \( n > 1 \) the EPS authentication vectors are ordered based on sequence number. Standard [4] recommends \( n = 1 \), so that only one authentication vector is sent at a time, because the need for frequently containing the HSS for fresh AVs has been reduced in EPS through the availability of the local master key \( K_{ASM} \) which is not exposed in a way similar to CK and IK in UMTS, and hence, does not need to be renewed very often. The Authentication Information Answer consises of 4 parts: a random number RAND, an expected response XRES, a local master key \( K_{ASM} \) and an authentication token AUTN.
5. UE verifies AUTN and computes RES, CK and IK, then sends the Authentication Response with RES to MME.
6. MME compares RES and XRES for the UE authentication, If matches, the authentication procedure succeeds, otherwise, MME denies the access request.
2.2. Security analysis of EPS AKA

Compared with UMTS AKA, EPS AKA can get additional security performance as follows [5][6]:
1) EPS AKA provides implicit serving network authentication, which UMTS AKA does not.
2) The protocol has adopted the layer level cipher key creation mechanism to improve the safety strength of session key;
3) The protocol has adopted the independent serial number \( SQN \) management mechanism and the sequencing storage and usage mechanism of the authentication vector is used to avoid the failure phenomenon of \( SQN \) pseudo synchronization [7].

Nevertheless, EPS AKA still has some key weaknesses:
1) During the subscriber’s first time registration, network access, or SN cannot resume the \( IMSI \) via Globally Unique Temporary UE Identity (GUTI), SN shall request the UE to send \( IMSI \) in plain text, thus \( IMSI \) has the risk of leakage, which may suffer the attacks as subscriber location, business tracking and “man-in-middle attack”, etc.
2) The wired link among network entities also lacks necessary protection, especially the authentication vector \( AV \) transmitted between HSS and MME via plain text can be easily intercepted.
3) The protocol is still based on symmetric key cryptosystem to realize the mutual authentication between HSS and UE, and create the session cipher key. While the security of long-term shared cipher key relies on the network and can be easily leaked, which has very big impacts on the security of the subsequent local communication.
4) The protocol ignores the protection to service network identity \( SNID \). Both air interface and wired link have the phenomenon of plain text transmission of \( SNID \), the attacker can easily eavesdrops the legal \( SNID \) to positively initiate the attacks as pseudo base station or network fraud, etc.
5) The protocol does not support digital signature, and cannot provide the incontestable business. Therefore, it is extremely hard to meet the reliability and flexibility of the next generation network.

3. Security Enhanced EPS AKA protocol

Aiming at the above mentioned security flaws existed in EPS AKA, this paper proposes a Security-Enhanced Authentication and Key Agreement protocol (SE-EPS AKA) based on WPKI.

3.1. Notes on nomenclature

- \( CA \) : denotes the Certification Agency;
- \( K \) : denotes the long term key shared between UE and HSS;
- \( PK_U, PK_M, PK_H \) : denotes the public key of UE, MME and HSS, respectively;
- \( SK_U, SK_M, SK_H \) : denotes the cipher key of UE, MME and HSS, respectively;
- \( f_3, f_4, f_{10} \) : denotes the key generating functions;
- \( f_3(m), f_4(m), f_{10}(m) \) : denotes the creation of cipher key by key generating functions \( f_3, f_4, f_{10} \) with cipher key \( K \) and parameter \( m \);
- \( K_{ASME} \) : denotes the intermediate key;
- \( KSI_{ASME} \) : denotes the key identification allocated by MME for \( KSI_{ASME} \);
- \( \{m\}_K \) : denotes the encrypted computation to message \( m \) via cipher key \( K \);
- \( \{m\}_{mg} \) : denotes the signature to message \( m \);
- \( \oplus \) : denotes bit-wise exclusive-or operation;
- \( || \) : denotes the concatenation of messages.

3.2. Procedure of SE-EPS AKA protocol

Based on WPKI, prior to communication, UE, MME and HSS shall acquire the digital certificate via CA, and acquire the public key. The process of digital certificate acquisition is not described in this
paper, for the detailed acquisition process should refer to REF [8]. Figure 2 shows the process of the SE-EPS AKA, Step 1-Step 7 are the detailed descriptions of this protocol.

**Figure 2.** The process of SE-EPS AKA

1) **UE → HSS:** \( A = \{\text{IMSI}\}_H, \text{ID}_{\text{HSS}} \)

   The subscriber initiates access request: Firstly, UE uses the HSS public key \( PK_H \) which is stored in smart card to encrypt \( \text{IMSI} \) and get \( A \). Then UE sends \( \{A, \text{ID}_{\text{HSS}}\} \) in access request to MME.

2) **MME → HSS:** \( A, B = \{\text{SNID}\}_H \)

   After MME receives the access request from subscriber, it adopts the public key \( PK_H \) to encrypt its own network identity \( \text{SNID} \), and derive the encryption information \( B \). Then \( A \) and \( B \) are regarded as authentication data request and delivered to HSS.

3) **HSS → MME:** \( C = \{AV(1,...,n), \text{IMSI}\}_H \)

   After receiving the authentication data request from MME, HSS uses its own private key \( SK_H \) to decrypt \( A \) and \( B \) to get \( \text{IMSI} \) and \( \text{SNID} \). Then HSS checks the validation of \( \text{IMSI} \) and \( \text{SNID} \) from registration subscriber list and authorization service network list maintained in the database. If the MME and SN identities have been verified, HSS will generate the random number array \( RAND(1,...,n) \), and the group of authentication vector \( AV(1,...,n) \). Figure 3 is the authentication vector generation algorithm.

**Figure 3.** The SE-EPS AKA authentication vector generation algorithm
According to the description of Figure 2, the SE-EPS AKA protocol needs to calculate the following parameters:

\[ K_{\text{ASME}} = s10_{k}(f3_{k}(\text{RAND}), f4_{k}(\text{RAND}), \text{SNID}); \]

\[ XRES = \text{RAND} \oplus \text{SNID}; \]

\[ AV = \text{RAND} \| \text{SNID} \| K_{\text{ASME}} \| XRES . \]

Then, HSS calculates the encryption information \( C = \{AV(1,...,n), \text{IMSI}\}_{PK_{UE}} \), and sends \( C \) to MME as the response.

4) MME → UE: D = \{RAND(i), SNID, KSI_{ASME}(i), S−TMSI\}_{PK_{UE}}.

Firstly, MME decrypts \( C \) to derive the \( AV(1,...,n) \) and \( \text{IMSI} \), and store \( AV(1,...,n) \) in database. Then, among \( AV(1,...,n) \), MME selects one authentication vector \( AV(i) \) which is never used, and extracts the random number \( RAND(i) \) and \( SNID \) therein. Then MME shall allocate the exclusive cipher key identifier \( KSI_{ASME}(i) \) to \( K_{\text{ASME}}(i) \) of the authentication vector \( AV(i) \), and utilize \( \text{IMSI} \) and the algorithm shared by MME and UE, to create \( S−TMSI \) for the scene of access once more. After completing one-time authentication and cipher key negotiation, UE and MME shall both store the corresponding relation between \( KSI_{ASME}(i) \) and \( K_{\text{ASME}}(i) \). If it is the once-more access, UE and SN shall at first take into account this identifier to verify \( K_{\text{ASME}}(i) \), thus the confidential communication can be realized without initiating authentication process [3]. Finally MME shall encrypt, \( RAND(i) \), \( S−TMSI \), \( KSI_{ASME}(i) \) and \( \text{SNID} \) by public key of UE to calculate data \( D \), and send \( D \) in subscriber authentication request to UE.

5) UE → MME: RES(i)

When UE receives the subscriber authentication request from MME, it decrypts \( D \) by \( SK_{UE} \) to resume \( RAND(i) \), \( S−TMSI \) and \( \text{SNID} \). Then UE calculates \( S−TMSI \) and compares it with \( S−TMSI \) derived from the decryption of \( D \), so as to realize the authentication to HSS. If these two ones are not consistent, it means that HSS is not invalid, and the protocol shall be terminated. Otherwise UE shall compute

\[ RES(i) = RAND(i) \oplus \text{SNID} \]

and

\[ K_{\text{ASME}}(i) = s10_{k}(f3_{k}(\text{RAND}(i)), f4_{k}(\text{RAND}(i)), \text{SNID}) \]

and \( RES(i) \) is regarded as response to subscriber authentication request sent to MME.

6) MME shall compare the \( RES(i) \) received with the \( XRES(i) \) of \( AV(i) \), if these two ones are consistent, it means that the subscriber is valid, in the next, MME and UE shall regard \( K_{\text{ASME}}(i) \) as intermediate cipher key to create the encryption cipher key \( (CK(i)) \) and integrity cipher key \( (IK(i)) \) for subsequent local communication, otherwise the whole process shall be terminated.

7) UE → MME → HSS: E = \{\text{IMSI}\|\text{SNID}\|\text{bill}\|\text{sig}\}_{PK_{HSS}}.

Finally, MME stores the corresponding relation between \( S−TMSI \) and \( (\text{IMSI}, AV(1,...,n), KSI_{ASME}(i), K_{\text{ASME}}(i), CK(i), IK(i)) \). The subscriber stores the corresponding relation between \( S−TMSI \) and \( (\text{IMSI}, \text{SNID}, KSI_{ASME}(i), K_{\text{ASME}}(i), CK(i), IK(i)) \) in UE. After the subscriber and service network complete the business interaction, UE can also utilize its own cipher key \( SK_{UE} \) to sign \( IMSI \), \( \text{SNID} \) and business charging information \( \text{bill} \) for creating charging evidence \( [\text{IMSI}\|\text{SNID}\|\text{bill}\|\text{sig}] \). Furthermore, in order to prevent from leakage of \( \text{IMSI} \) and \( \text{SNID} \), public key \( PK_{HSS} \) of HSS is once more used, and the digital envelope \( E \) is created. Lastly, this information is transferred to HSS via MME, which can be used as evidence for presence and business participation of MME and subscriber as well as creation of related charging relation.

4. Formal verification of SE-EPS AKA

The authentication test method is one of the fairly perfect verification methods of authentication protocol at present. Herein this method is used to verify the safety and security of SE-EPS AKA protocol. The initial definition of authentication test method is as followed:
4.1. Authentication of UE to MME

**Proposition:** Suppose that \( s \) is UE strand, \( K_s \) is the cipher key set controlled by attacker, \( PK_U, PK_H \not\in K_p \), and IMSI is originated uniquely by \( s \).

**Proof:** ① Construct test component. Initiator strand \( s = UE[A, ID_{HSS}, D, RES] \), IMSI is originated uniquely in node \( < s,1 > \), therefore \( \{ IMSI \}_{PK_s} \) is the test component of \( < s,1 > \) about IMSI, according to Fig. 1 it can be seen that, since \( S - TMSI \) is originated by IMSI, \( S - TMSI \subset IMSI \), \( < s,1 > \rightarrow + < s,2 > \) is the outgoing test for IMSI in \( \{ IMSI \}_{PK_s} \). ② Apply the authentication test rule 1[9]. It has the existence of normal node \( m, m' \in C \), term(m) = \{ IMSI \}_{PK_u} \) and \( m \Rightarrow + m' \) is the transforming edge of IMSI. ③ Define the node \( m \). According to result of step ②, \( m \) is a negative node. Suppose that \( m \) is the node of certain MME strand \( s' \), \( m \leftarrow < s',1 > \), \( s = MME[A, ID_{HSS}, B, C, D, RES'] \), term\( < s',1 > \) = \{ IMSI \}_{PK_u} \). ④ Compare the content of strands. Compare term\( < s',1 > \) with the related content in MME strand, it can get \( A' = A , ID_{HSS} = ID_{HSS'} , HSS = HSS' \). ⑤ Proof of SNID = SNID' According to 2nd part of authentication test method[9], \( t_1 = D \leftarrow \{ RAND, SNID, KSI_{SGME}, S - TMSI \}_{PK_s} \). ⑥ Define the node \( m \). Suppose that \( m \) is the node of certain initiator strand \( s'' \), \( m \leftarrow < s'',2 > \), sign\( < s'',2 > \) = \( - \), term\( < s'',2 > \) = \{ RAND, SNID, KSI_{SGME}, S - TMSI \}_{PK_u} \). ⑦ Compare the contents of \( s \) and \( s'' \), since IMSI is originated uniquely in initiator strand \( s \), and \( PK_u \not\in K_p \), so \( s = s'' \). As \( \{ RAND, SNID, KSI_{SGME}, S - TMSI \}_{PK_u} \) = term\( < s,2 > \). Finally it can get \( SNID = SNID' \). It can be seen that, UE can authenticate the identity of MME.

4.2. Authentication of MME to HSS

**Proposition:** Suppose that \( s \) is MME strand, \( PK_M \not\in K_p \), and SNID is originated uniquely by \( s \).

**Proof:** ① Construct test component. MME strand \( s = MME[A, ID_{HSS}, B, C, D, RES] \), since SNID \( \in B \) is originated uniquely in \( < s,2 > \), \( B = \{ SNID \}_{PK_H} \) is the test component in \( < s,2 > \) about SNID, according to Fig. 1 it can be seen that: \( < s,2 > \rightarrow + < s,3 > \) is the outgoing test for SNID. ② Apply the authentication test rule 1[9]. It has the existence of normal node \( m, m \in C \), term\( m \) = \{ SNID \}_{PK_u} \), and \( m \Rightarrow + m' \) is the transforming edge of SNID. ③ Define the node \( m \). According to result of step ②, the node \( m \) is a negative node, therefore \( m \) is the node of certain HSS strand, suppose that the initiator strand is \( s \), \( s = HSS[IMSI, SNID, A, B, C, D, ID_{HSS}], m \leftarrow < s,2 > \), and term\( < s,2 > \) = \{ IMSI \}_{PK_H} \). ④ Compare the contents of strands. Through comparing the contents of term\( < s,2 > \) with the related content in HSS strand, \( ID_{HSS} = ID_{HSS} , IMSI = IMSI' , SNID = SNID' \) can be derived, and it can be seen that MME can authenticate the identity of HSS. Using the same method, the authentication of MME to UE is also can be validated.

According to formal analysis of above mentioned, it is verified that SE-EPS AKA protocol realizes the mutual authentication among UE, MME and HSS, protects the transmission of private and
confidential information among entities, resolves various safety problems incurred by leakage of IMSI and SNID, and increases the safety strength of session cipher key. Furthermore, SE-EPS AKA also has following two distinctive characteristics.

1. The public key encryption is used to resist the replay attack. Compared with EPS AKA, the improved protocol no longer needs to import SQN in AV to ensure the freshness of authentication vector, since $AV(1,\ldots,n)$ cannot be decrypted, and $K_{ese}$ cannot be acquired, even the attacker eavesdrops the data between HSS and MME, or data between UE and MME, it cannot be accessed to the system via the mode of message replay. Therefore, the public key encryption can thoroughly resolve the problem of difficult operation of SQN, and effectively defend the SQN DOS attacks.

2. Since the protocol adopts the public key system, it has good extensibility, furthermore it supports digital signature and can provide the incontestable business.

5. Conclusions

Aiming at the wireless security, 3GPP propose EPS AKA for supporting the next generation all-IP wireless network. However, by thoroughly analyzing, this paper has found some fatal weaknesses in EPS AKA, which can lead to the information leakage, pseudo base-station attack, etc. In order to prevent the user and access network from malicious attacks, this paper proposes a new WPKI based SE-EPS AKA protocol, which can provide the undeniable digital signature and protect the exchanged information comprehensively. In addition, the new scheme can support the system extension much more efficient than other symmetric key systems. At the end of this paper, the formal verification of the SE-EPS AKA protocol indicates that our new scheme can satisfy the integrity and security.

6. Acknowledgement

This paper is supported by the China Postdoctoral Science Foundation and the Fundamental Research Funds for the Central Universities.

7. References


