Anonymous Authentication and Key Agreement Protocol for LTE Networks

Chun-I Fan[1,2], Yi-Fan Tseng[1], Chen-Hsi Cheng[1], Hsin-Nan Kuo[1], Jheng-Jia Huang[2], and Yu-Tse Shih[1]
National Sun Yat-sen University[1]
Telecom Technology Center[2]
Kaohsiung, Taiwan
e-mail: cifan@mail.cse.nsysu.edu.tw

***Abstract*—In 2008, 3GPP proposed the Long Term Evolution (LTE) in version 8. The standard is used in high-speed wireless communication standard for mobile terminal in telecommunication. It supports subscribers to access internet via specific base station after authentication. These authentication processes were defined in standard TS33.401 and TS33.102 by 3GPP. Authenticated processing standard inherits the authentication and key agreement protocol in RFC3310 and has been changed into authenticated scheme suitable for LTE. In the origin LTE authenticated scheme, subscribers need to transfer its International Mobile Subscriber Identity (IMSI) with plaintext. The IMSI might be intercepted and traced by fake stations. In this work, we propose a new scheme with a pseudo IMSI so that fake stations cannot get the real IMSI and trace the subscriber. The subscriber can keep anonymous and be confirmed by the base station for the legality. The pseudo identity is unlinkable to the subscriber. Not only does the proposed scheme enhance the security but also it just has some extra costs for signature generation and verification as compared to the original scheme.**

Keywords-long term evolution; authentication and key agreement protocol; signature; anonymous; pseudorandom permutation

I. INTRODUCTION

With the increase in demand for Internet services and advanced mobile telecommunication industry, people have higher expectations for the improvement of the Internet access rate and performance. 3GPP releases a new version of the Long Term Evolution (LTE) standard in the version 8. In circuit switch mobile networks, messages are delivered in a dedicates leased line. In LTE mobile networks, all the messages will be transmitted in packet type. Authentication is very important in mobile networks, and RFC3310 has proposed a model to define authentication and key agreement (AKA) protocol for HTTP. This protocol is defined in 2008 and used in TS 33.102 and TS 33.401 for AKA protocol in LTE to ensure the security of identity identification and communications. Certain LTE AKA protocols may suffer from certain security flaws, i.e., impossibility of revoking secret keys and fake base station attack. The scheme will consider above security issues in designing AKA protocol for LTE without a lot of cost.

A. The System Model

The basic architecture of LTE consists of radio access network (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) and core networks (Evolved Packet Core, EPC). In term of message transmission, control-plane and user-plane are divided for the transmission of control packets and data packets. E-UTRAN consists of user equipment and eNodeB. The communication channel of these two elements are LTE-Uu radio interface. The interface is responsible for radio resource management, admission control, scheduling, and enforcement of negotiated QoS. The EPC consists of mobile management entity (MME), serving gateway (SGW), packet data network gateway (PGW), home subscriber server/authentication center (HSS/AuC), policy charging and rules function (PCRF). MME is the key control-node in LTE network. It is responsible for user authentication with HSS/AuC. It is also the termination point in the network for non-access stratum (NAS) signaling. MME is engaged in every authentication and key agreement with HSS/AuC. SGW is responsible for forwarding user data packets. It manages and stores UE context, and replicates of users' traffic under permitted interception. PGW provides external network connection, lawful interception, packet screening, charging support, policy enforcement, and packet filtering for each user. SGW and PGW could be realized as a single network element. HSS/AuC is a database, which stores both static and dynamic data elements related to subscribers. It also provides user profile information and key management to MME. PCRF provides policy control decision and flow based charging controls. PCRF ensures user plane traffic mapping and treatment according to user's profile.

B. Contributions

Some researchers have solved some problems above. Cocktail-AKA protocol solves the congenital defects of the UMTS-AKA protocol. SAK-AKA protocol provides a secure anonymity key of AKA for LTE networks. We will provide a scheme with an anonymous AKA protocol in LTE networks.

II. PRELIMINARIES

In this section, we introduce the AKA protocols defined in 3GPP TS 33.102 and TS 33.401.

A. The AKA Protocols in 3GPP Standards

This subsection introduces the LTE AKA protocol [1, 2] (Evolved Packet System - Authentication and Key Agreement, EPS-AKA) as follows and the notations are defined in TABLE I.

978-1-7281-1439-2/19/$31.00 ©2019 IEEE

TABLE I. NOTATIONS FOR AKA

Notation	Definition
IMSI	International Mobile Subscriber Identity
K_0	Long Term Key shared between UE and HSS/AuC
RAND	Random Number
RES	Response
XRES	Expected Response
CK	Cipher Key
IK	Integrity Key
Skey	Session Key
AUTN	Authentication Token
AV	Authentication Vector
HE	Home Environment
MAC	The message authentication code included in AUTN
SQN	Sequence number
SNid	Identity number of MME

- **Request Phase**

The steps of the protocol:

1) The mechanism is initiated by MME that requests the user to send its permanent identity. The user responds *IMSI* to MME.
2) MME sends *IMSI* and *SNid* to HSS/AuC where *SNid* is the identity of MME.

- **HSS/AuC Computes Phase**

Let K_0 be the key shared between UE and HSS/AuC.

1) After receiving *IMSI* and *SNid* from MME, HSS/AuC chooses a random number *RAND*.
2) HSS/AuC computes the message authentication code $MAC \leftarrow f_1(SQN_H \parallel RAND)$ where f_1 is a message authentication function and generates AUTH $\leftarrow SQN_H \parallel MAC$.
3) HSS/AuC computes the expected response $XRES \leftarrow f_2(K_0(RAND))$ where f_2 is a (possibly truncated) message authentication function.
4) HSS/AuC computes $CK \leftarrow f_3(K_0(RANK))$ and $IK \leftarrow f_4(K_0(RAND))$ and generates $SKey \leftarrow$ CK $\parallel$ IK.
5) HSS sends *RAND*, *AUTN*, *XRES* and Skey to MME as auth data response.

- **Verification Phase**

The steps of the protocol:

1) After MME receiving *auth data response* from HSS, it sends *RAND* and *AUTN* to UE.
2) UE computes *XMAC* and compares XMAC $\stackrel{?}{=} MAC$.
3) UE computes $RES \leftarrow f_2(K_0(RAND))$ and sends it to MME.
4) MME compares $RES \stackrel{?}{=} XRES$

III. THE PROPOSED PROTOCOL

This section presents an anonymous authentication and key agreement Protocol for LTE networks, where UE uses a pseudo-identity in authentication. In our scheme, there are three parties: UE, MME and HSS/AuC. The proposed scheme consists of five steps: *Setup*, *IMSI-request*, *Set-XRES*, *Verify-HSS*, *Verify-UE*. The notations used in the proposed scheme are defined in TABLE II.

TABLE II. THE NOTATIONS FOR THE PROPOSED PROTOCOL

Notation	Meaning
UE	User equipment
MME	Mobile management entity
HSS/AuC	Home subscriber server /Authentication center
PK_H	A public key for HSS/AuC
SK_H	A secret key for HSS/AuC
K_0	A long term key shared between UE and HSS/AuC
σ	A signature
Pseudo-IMSI	A pseudo-identity
NPseudo-IMSI	A new pseudo-identity
RAND	Random number
RES	Response
AMF	Authentication management eld
XRES	Expected Response
CK	Session key
IK	Integrity key
SKey	A session key combined with *CK* and *IK*
AUTN	Authentication token
HE	Home environment
MAC	The message authentication code included in *AUTN*
SQN	Sequence number
f_1	A generating function to compute *MAC*
f_2	A generating function to compute *XRES*
f_3	A generating function to compute *CK*
f_4	A generating function to compute *IK*
KDF	A key derivation function

The details of our scheme are described as follows. We use $\sigma(M)$ to denote a signature on M Given a symmetric key$K$, we use $K(m)$ to denote a symmetric encryption on m. We use $\pi = (KeyGen, Sign, Verify)$ to denote signature function where $KeyGen$ is key generation function, $Sign$ is sign function and $Verify$ is verification. After authentication pass, the session key will be generated to the next communication. We illustrate the proposed protocol in Figure 1. The details of our scheme are described as follows:

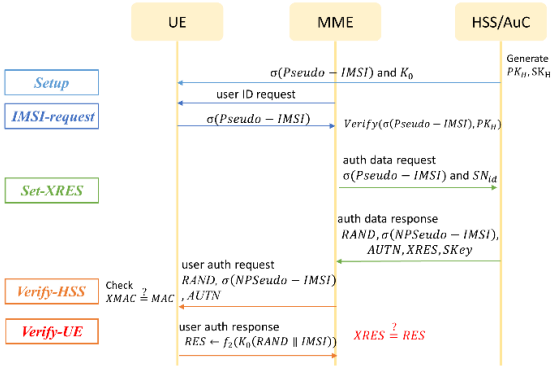

Figure 1. The Proposed Protocol.

A. Setup

1) HSS/AuC runs *KeyGen* and gets the PK_H and SK_H.
2) HSS/AuC chooses a pseudo-identity $Pseudo-IMSI$ and computes a signature $\sigma = sign(SK_H, Pseudo-IMSI)$ with the private key of HSS/AuC.
3) HSS/AuC chooses a long term key K_0.

4) HSS/AuC stores the signature $\sigma(Pseudo-IMSI)$ and the long term key K_0 in the SIM card.
5) HSS/AuC sends the SIM card to UE via a secure manner.

B. IMSI-Request

1) MME sends a signal *IDrequest* to UE for invoking the authentication.
2) UE sends back $\sigma(Pseudo-IMSI)$ to MME instead of the real IMSI.
3) MME verifies $Verify(\sigma(Pseudo-IMSI), PK_H)$ to confirm that UE is legitimate user.

The Request phase is shown in Figure 2.

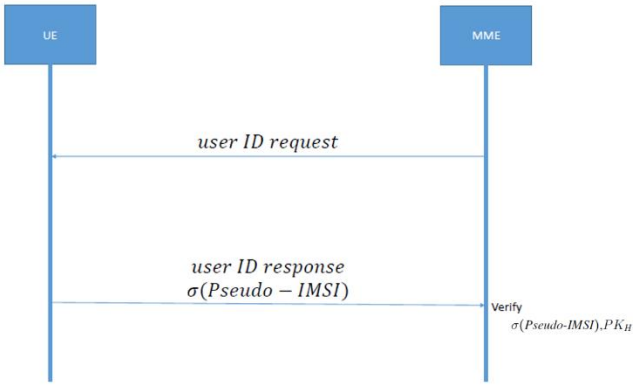

Figure 2. Request Phase

C. Set-XRES

1) MME sends $\sigma(Pseudo-IMSI)$ and MME's own SN_{id} to HSS/AuC.
2) After receiving the packet from MME, HSS/AuC confirms the real *IMSI* for UE on the stored table and chooses a random number *RAND*.
3) HSS/AuC computes *MAC* with a hash function f_1, where $MAC \leftarrow f_1(K_0(SQN_H \parallel RAND \parallel IMSI))$.
4) HSS/AuC sets $AUTN \leftarrow SQN_H \parallel MAC$.
5) HSS/AuC computes $XRES \leftarrow f_2(K_0(RAND \parallel IMSI))$.
6) HSS/AuC computes $CK \leftarrow f_3(K_0(RAND))$ and $IK \leftarrow f_4(K_0(RAND))$.
7) HSS/AuC computes $SKey \leftarrow KDF(SQN_H \parallel CK \parallel IK \parallel SN_{id})$.
8) HSS/AuC generates a new pseudo IMSI $NPseudo-IMSI$ and $\sigma = Sign(SK_H, NPseudo-IMSI))$ with the private key of HSS/AuC.
9) HSS/AuC sends back to MME with *RAND*, $\sigma(NPSeudo-IMSI)$, *AUTN*, *XRES* and *SKey*.

The Set XRES phase is shown in Figure 3.

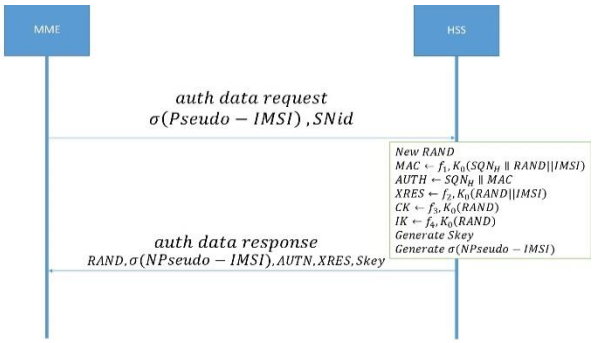

Figure 3. Set XRES Phase

D. Verify-HSS

To verify HSS/AuC by MAC which has been verified by MME, UE performs the following steps:

1) After receiving parameters from HSS, MME keeps *XRES* to verify UE.
2) MME sends RAND, $\sigma(NPSeudo-IMSI)$, and AUTN to UE.
3) UE computes $XMAC \leftarrow f_1(K_0(SQN_H \parallel RAND \parallel IMSI))$ and checks $XMAC \stackrel{?}{=} MAC$. Note that *AUTN* includes SQN_H to compute *XMAC*.
4) UE keeps $\sigma(NPseudo-IMSI)$ and computes $\sigma(Pseudo-IMSI) \leftarrow \sigma(NPseudo-IMSI)$.
5) UE computes $RES \leftarrow f_2(K_0(RAND \parallel IMSI))$ and sends it to MME.

E. Verify-UE

1) The MME outputs "valid" if *XRES* = *RES*; otherwise, it outputs "invalid".
2) If the authentication fails, the MME replaces *NPseudo-IMSI* with *Pseudo–IMSI* so that the pseudo identity will not be changed by failure authentication.

The Verify phase is shown in Figure 4.

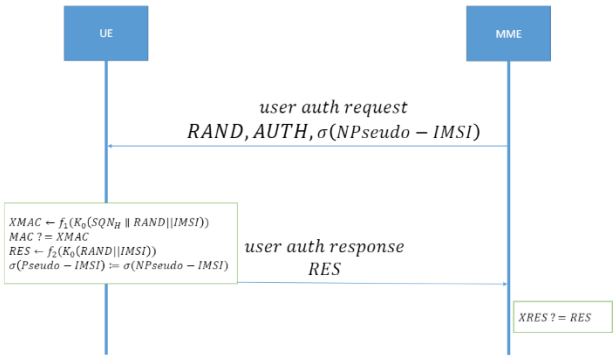

Figure 4. Verify Phase

F. Correctness

The long term key K_0 is shared between UE and HSS. The generating function f_1 to f_4 is public. $MAC = f_1(K_0(SQN_H \parallel RAND \parallel IMSI))$, where SQN_H is the sequence number of HSS/AuC, *IMSI* is the real identity of UE. HSS/AuC stores the mapping between real identity and *Pseudo-IMSI*. UE stores it at SIM card. So UE is able to

compute $XMAC$ with the parameters received from MME. $XRES$and RES can also be computed correctly.

IV. Security Analysis

A. Anonymity Analysis

In our scheme, we use pseudo IMSI to hide the real IMSI of the user. If the attacker eavesdrops the LTE internet and get the $\alpha(Psudeo - IMSI)$, it cannot still pretend the user because it does not have the long term key and IMSI to compute the authenticated parameters. Even though the attacker gets the long term key and IMSI, the pseudo IMSI is changed every authentication so the attacker cannot still pass the authentication. The pseudo IMSI and the user have unlinkability so that the scheme provides anonymity and the user can defeat the man-in-the-middle attack.

B. Mutual Authentication

Since the messages sent by HSS/AuC and UE are encrypted by a secure symmetric encryption algorithm where the corresponding key is shared between HSS/AuC and UE, only HSS/AuC and UE can generate valid messages, which pass the verification.

V. Comparison

In this section, the proposed scheme is compared with some existing A-AKA schemes [2,3,4,5]. Table III presents the comparisons between the proposed scheme and A-AKA authentication schemes in security properties and efficiency. In 2008, GSMA defines the Authentication and Key Agreement protocol in LTE network. In 2010, Ou *et al.* proposed a cocktail protocol [4] that mix two varieties of *Authentication Vector* and made the computation phase more effective. In 2012, Tsay *et al.* show a vulnerability in the UTMS and LTE Authentication and Key Agreement Protocol [6]. They claimed that the inside attacker can be authenticated as other honest subscriber to serving network, and use the wireless services on it's behalf. In 2017, Haddad *et al.* propose anonymous authentication and location privacy preserving scheme for LTE-A networks [3]. It has already achieved user anonymity, but the scheme is much different from the original. It is not useful to the AKA protocol. The scheme we proposed is simpler and effective. The computation cost on UE is the same as EPS-AKA and much less than other AKA protocols. On HSS and MME, we increase the computation cost of signature and verification to make users anonymous. The computation cost on HSS and MME is less that of the others. The comparison is shown in TABLE III.

TABLE III. The Comparisons between [2,3,4,5] and Our Scheme

	UE computation cost	HSS and MME computation cost
A-AKA[3]	$2\phi + 2\varphi + 7\psi$	$3\phi + 4\varphi + 8\psi$
cocktail-AKA[4]	5υ	8υ
SAK-AKA[5]	$6\phi + 4\upsilon$	$8\phi + 4\upsilon + 1\omega$
EPS-AKA [2]	$2\upsilon + 2\phi$	$4\upsilon + 4\phi$
Ours	$2\upsilon + 2\phi$	$4\upsilon + 4\phi + \mu + \lambda$

ϕ: MD5 hash function
φ: ECC encryption
ψ: Modulus operation
υ: AES encryption
ω: AES decryption
μ: Sign computation
λ: Sign verification

VI. Conclusion

This work presents an anonymous Authentication and Key Agreement scheme for LTE to enhance the security level for the protocol. Compared with SAK-AKA and the original protocol, the proposed scheme provides a simpler way to make it anonymous. The scheme is more lightweight and simpler than SAK-AKA. We use fake IMSI provided by HSS with its signature. After authentication, HSS will generate another fresh fake IMSI with its signature to the user. By using the fake IMSI, the communications reveal nothing about the user's IMSI. On the other hand, the real IMSI is still embedded in the communications through an encrypted form. Thus, the protocol is able to reject all the invalid requests. In summary, we have propose a scheme that by just making a few modifications on the original one but it can avoid many kinds of attacks and make users anonymous. In the future, we will focus on implementing the proposed protocol and making it more feasible for real-world applications.

Acknowledgment

This work was supported in part by the Ministry of Science and Technology of Taiwan under grants MOST 105-2923-E-110-001-MY3 and MOST 107-2218-E-110-014, and in part by the Information Security Research Center at National Sun Yat-sen University and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan. This work was also partially supported by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

References

[1] 3g security; security architecture (2008), www.3gpp.org/dynareport/33102.htm ,2018/05/13

[2] 3gpp system architecture evolution (sae); security architecture (2008), www.3gpp.org/dynareport/33401.htm ,2018/05/12

[3] Haddad, Z.J., Taha, S., Aly, S.I.: Anonymous authentication and location privacy preserving schemes for lte-a networks. Egyptian Informatics Journal 18(3), 193-203 (2017), https://www.sciencedirect.com/science/article/pii/S111086651730014, 2018/05/15

[4] Ou, H.H., Hwang, M.S., Jan, J.K.: A cocktail protocol with the authentication and key agreement on the umts. J. Syst. Softw. Https://www.sciencedirect.com/science/article/pii/S01641212090019 9X ,2018/05/10

[5] Shadi, N.: SAK-AKA: a secure anonymity key of authentication and key agreement protocol for LTE network. Int. Arab J. Inf. Technol. Https://link.springer.com/article/10.1007/s10916-015-0258-7, 2018/05/12

[6] Tsay, J.K., F., M.S.: A vulnerability in the umts and lte authentication and key agreement protocols. In: Igor, K., Skormin, V. (eds.) Computer Network Security. Springer Berlin Heidelberg (2012)