IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 15, 2021, accepted May 4, 2021, date of publication May 17, 2021, date of current version June 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3080839

An Identity Privacy Protection Scheme in LTE-WLAN Heterogeneous Converged Network

LILING CAO, ZHANG YU, YUQING LIU, AND SHOUQI CAO
Department of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China
Corresponding author: Shouqi Cao (sqcao@shou.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2019YFD0900805.

ABSTRACT Aiming at to avoid the drawbacks of the identity privacy protection scheme in Long Term Evolution-Wireless Local Area Network (LTE-WLAN) heterogeneous converged network proposed by the 3rd Generation Partnership Project (3GPP), an improved scheme based on identity index is proposed to achieve anonymity, untraceability and dynamic identity. Security analysis shows that our proposed scheme can prevent replay attack and man-in-the-middle attack for network layer authentication. The results of comparison with the related schemes show that security and efficiency of our proposed scheme is prior to some other existing ones with low computation cost and short time delay.

INDEX TERMS Identity privacy protection, LTE-WLAN, identity index.

I. INTRODUCTION

Wireless communication networks can be divided roughly into five types according to the distance of data transmission and network coverage, (i)satellite network [1], (ii)Wireless Wide Area Network (WWAN), such as Long Term Evolution (LTE) wireless cellular network [2], (iii)Wireless Metropolitan Area Network (WMAN) [3], (iv) Wireless Local Area Network (WLAN) [4], (v) Wireless Personal Area Network (WPAN) [5].

Nowadays, the urgent demand for diversified services such as multimedia applications in wireless communication networks have stimulated the appearance of heterogeneous converged networks [6], which will realize the global mobile broadband services with different requirements and seamless mobility by integrating diverse but complementary wireless networks. As such, LTE-WLAN heterogeneous converged network [7], as the most widespread implementation, supports mobile users to enjoy high data rate in WLAN network and switch to LTE network for global roaming in the absence of WLAN. Accordingly, it is desirable and inevitable to meet the strong challenges to ensure security while integrating various wireless networks especially protecting sensitive information of the user in the process of authentication, such as identity, location and movement, with the goal of achieving anonymity and untraceability.

The associate editor coordinating the review of this manuscript and approving it for publication was Tai-Hoon Kim.

To achieve anonymity during the procedure of mobile communication, three methods can be used: (i)assign alias to each user for identification, such as temporary identity or identity index [8], [9], (ii) encrypt the true identity when sending messages containing the identity of the user [10] and. (iii) encrypted identity and identity index are both used to keep anonymity [11]. To achieve untraceability during the procedure of mobile communication, different temporary identities must be used in each authentication process for the same user and cannot be identified as belonging to the same user by attackers.

In the cellular mobile communication development from the traditional 2nd Generation and the 3rd Generation (2G&3G) telecommunication networks to LTE network, user privacy protection has always been concerned. In the LTE network, Temporary Mobile Subscriber Identity (TMSI) is used to replace the permanent International Mobile Subscriber Identity (IMSI), which can hide the true identity of the user and avoid the frequent transmission of IMSI.IMSI consists of three parts: Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Identification Number (MSIN), for a total of 15 digits in decimal. (i)MCC: 3 digits in decimal, used to identify the home country of the user, managed and assigned by International Telecommunication Union (ITU). (ii) MNC: 2 digits in decimal, used to identify the mobile network operator that the user belongs to. (iii) MSIN: 10 digits in decimal, used to identify the particular user in the mobile network.

In the LTE-WLAN heterogeneous converged network proposed by the 3rd Generation Partnership Project (3GPP), Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') protocol [12], which also includes user identity privacy protection, is proposed to realize mutual authentication between communication entities such as the User Equipment (UE) and the Home Subscriber Server (HSS). TMSI is also used to replace the IMSI in EAP-AKA' protocol, which avoids IMSI being intercepted and protects the identity privacy of the user. However, identity privacy protection scheme in LTE R12 still has defects[13]. Attackers can violate the privacy and trace the movement of the users by obtaining the identity, location and messages. Meanwhile, attackers may damage the whole communication network by disguising as legitimate user to launch DoS attacks. Aiming at to avoid the drawbacks of the identity privacy protection scheme in LTE-WLAN network proposed by 3GPP, researchers have put forward various improved schemes based on symmetrical cryptosystem and public key cryptosystem [8]–[11], [14]–[21]

In the public key-based schemes [15]–[21], the user uses the public key of HSS to encrypt and send corresponding IMSI, then, only HSS can obtain IMSI by decrypting the encrypted message. Obviously, it is easy to realize anonymity in public key cryptography scheme, but the computation cost, communication cost and computational complexity increase accordingly. Communication entities including HSS and Authentication, Authorization, Accounting (AAA) have resources to cope with such issue. However, the battery bottleneck still exists in portable user equipment, which makes it impossible to deal with public-key cryptography in user-side. Moreover, user equipment's battery may run out when malicious WLAN Access Network (WLAN AN) and AAA constantly send to the user the identity requests for IMSI.

Therefore, schemes based on symmetrical cryptosystem are more applicable for user equipment with restrained resource and battery [8]–[11], [14].

In this paper, recent identity privacy protection schemes in the process of user authentication have been studied and limitations of these schemes have been analyzed, and an improved scheme based on identity index is proposed to achieve anonymity, untraceability and dynamic identity. Notations used in this paper are listed in Table 11 in appendix.

II. INTRODUCTION OF EAP-AKA

In the LTE-WLAN heterogeneous converged network, the EAP-AKA' protocol including user identity privacy protection is introduced briefly below (shown in FIGURE 1) and detail description can be referred to RFC5448 [12].

(i) On receiving the advertisements from WLAN AN, WLAN-UE starts establishing a connection with the WLAN AN and executing mutual authentication.

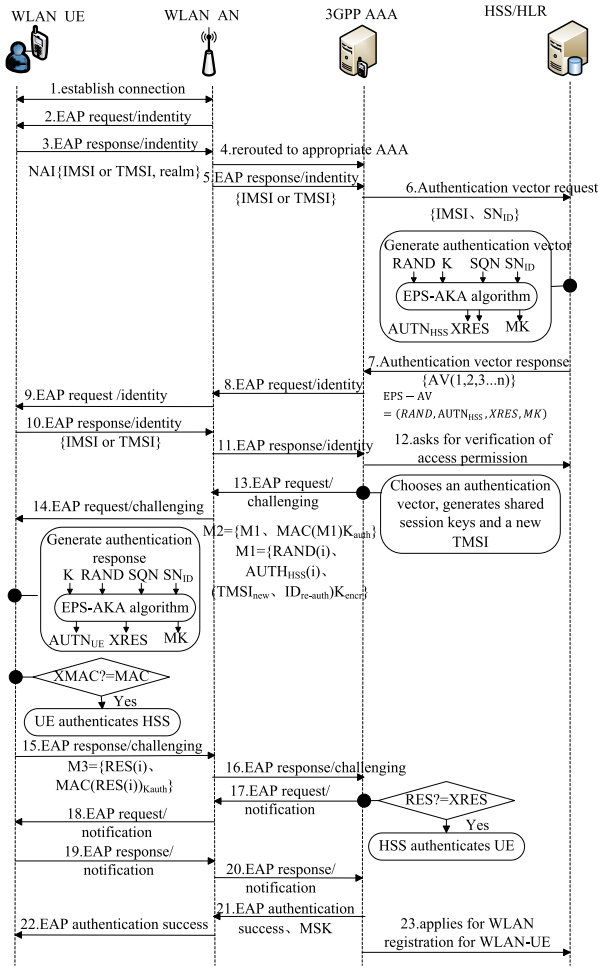

FIGURE 1. EAP-AKA, authentication protocol.

(ii) WLAN AN requests user identity in Extensible Authentication Protocol over LAN (EAPOL) format.

(iii) Responding to the EAP request/identity, WLAN-UE sends Network Access Identifier (NAI)(3GPP TS 23.003) [22] as a reply message, including IMSI (or TMSI) and realm, where IMSI (or TMSI) is used to identify users and realm is used for message routing. IMSI should be sent when the user executes the authentication for the first time or when TMSI is sent but cannot be identified by AAA. In other cases, TMSI is sent in EAP response/identity message and updated after every round of authentication.

(iv) WLAN-AN will be rerouted to appropriate AAA based on NAI message, perhaps passing through one or more AAA proxy.

(v) The WLAN-UE forwards the EAP response/identity message to AAA, which stores user profile information and collects accounting information.

(vi) Based on IMSI (or TMSI), AAA searches in its database and checks whether there is an unused authentication vectors available for the user. If an unused authentication vector is not available, AAA computes IMSI based on TMSI and requests an authentication vector from HSS. The message includes IMSI and the identity of WLAN-AN SN_{ID}.

(vii) HSS uses the secret key K shared by WLAN-UE and HSS and a random number ($RAND$) to generate Cipher Key (CK), Integrity Key (IK), Anonymity Key (AK), and Expected Response (XRES). In addition, other parameters used in this process are shown as follows, in which SQN is a sequence number produced by the serial number counter owned by HSS, AMF is the authentication management filed of the HSS, which is the domain name of the network to which the user belongs, MAC is the message authentication code, $AUTN$ is the authentication token, Master Key (MK) is used to derive the shared keys between the UE and AAA and between the UE and WLAN AN in the following processes. f_0 is a random number generating function, f_1 and f_2 are authentication functions, f_3, f_4, f_5 and KDF are key derivation functions. Ultimately, HSS generates Evolved Packet System Authentication Vectors ($EPS-AV$) and sends it to AAA. Each vector includes four parameters: $RAND$, $XRES$, $AUTN_{HSS}$ and MK (the same as K_{ASME}) which are the same parameters as those in the LTE-AKA protocol.

$$RAND = f_0\,(seed) \tag{1}$$
$$XRES = f_{2K}\,(RAND) \tag{2}$$
$$CK = f_{3K}\,(RAND) \tag{3}$$
$$IK = f_{4K}\,(RAND) \tag{4}$$
$$AK = f_{5K}\,(RAND) \tag{5}$$
$$MK = K_{ASME} = KDF(CK, IK, SN_{ID}, SQN) \tag{6}$$
$$MAC = f_{1K}\,(SQN||RAND||AMF) \tag{7}$$
$$AUTN_{HSS} = (SQN \oplus AK||AMF||MAC) \tag{8}$$
$$EPS - AV = (RAND, AUTN_{HSS}, XRES, MK) \tag{9}$$

(viii) AAA sends EAP-request/identity message to WLAN-AN one more time to avoid that the message being manipulated once.

(ix) WLAN-AN forwards EAP request/identity message to WLAN-UE one more time.

(x) WLAN-UE sends EAP response/identity message to WLAN-AN.

(xi) WLAN-AN forwards EAP response/identity message to AAA. AAA compares the IMSI (or TMSI) in successive EAP response/identity message. If they are not the same, AAA deletes the authentication vectors and asks for authentication vectors from HSS one more time.

(xii) AAA checks whether there is configuration information to access WLAN for WLAN-UE stored in its database. If no configuration information is available, AAA asks for verification of access permission from HSS.

(xiii) AAA chooses an authentication vector $EPS - AV$, uses the MK to derive the shared secret keys between WLAN-UE and AAA, which includes session key K_{encr} and integrity key K_{auth}. AAA uses the MK to derive the shared secure communication key MSK between WLAN-UE and WLAN AN. Then, AAA updates TMSI and generates $ID_{re-auth}$ for re-authentication. Finally, AAA sends to WLAN AN the challenging request message M2 shown as follows, where $MAC\,(M1)_{Kauth}$ is the message authentication code based on the message $M1$ and the secret key K_{auth}, $(TMSI_{new}, ID_{re-auth})_{Kencr}$ denotes that $TMSI_{new}$ and $ID_{re-auth}$ are encrypted by K_{encr}.

$$M1 = \{RAND, AUTN_{HSS}, (TMSI_{new}, ID_{re-auth})_{Kencr}\} \tag{10}$$
$$M2 = \{M1, MAC(M1)_{Kauth}\} \tag{11}$$

(xiv) WLAN AN forwards EAP challenging request message to WLAN-UE.

(xv) On receiving the message M1, WLAN-UE firstly computes AK based on shared secret key K and received $RAND$ according to formula (5). Secondly, WLAN-UE extracts SQN, AMF and MAC from received $AUTN_{HSS}$ based on AK. Thirdly, WLAN-UE computes $XMAC$ according to formula (7) and compares it with MAC extracted from $AUTN_{HSS}$. Then WLAN-UE accepts HSS when $XMAC = MAC$. Next, WLAN-UE gets MK according to formula (3), (4), (6) to derive K_{encr} and K_{auth}. At this point, WLAN-UE can verify the integrity of message M2, obtain new TMSI by decryption and use MK to derive MSK. At last, WLAN-UE sends challenging reply message M3 to WLAN AN.

$$RES = f_{2K}\,(RAND) \tag{12}$$
$$M3 = \{RES, MAC(RES)_{Kauth}\} \tag{13}$$

(xvi) WLAN AN forwards challenging reply message to AAA.

(xvii) After the validation of the integrity of message M3, AAA compares RES and $XRES$. If they are equal, AAA sends notification request message to WLAN AN.

(xviii) WLAN AN forwards notification request message to WLAN-UE.

(xix) WLAN-UE sends notification response message to WLAN AN.

(xx) WLAN AN forwards notification response message to AAA.

(xxi) AAA sends EAP authentication successful message and MSK to WLAN AN.

(xxii) WLAN AN stores MSK and forwards authentication successful message to WLAN-UE.

(xxiii) AAA applies for WLAN registration for WLAN-UE from HSS.

III. INTRODUCTION OF ANALYSIS OF RECENT SCHEMES

A. INTRODUCTION AND ANALYSIS OF JANG et al.'s SCHEME[10]

In Jang *et al.*'s scheme, authentication information including IMSI is encrypted to achieve privacy protection in LTE network. Access authentication for the first time is divided into two types according to the identity the user uses: (i) uses IMSI. (ii) uses Global Unique Temporary Identifier (GUTI).

The basic idea of Jang *et al.*'s scheme is described below. During the procedure of registration of the UE, a secret function $f()$, which will be shared by the UE and Mobility Management Entity (MME), is produced according to the MNC of the user, and then stored in the UE. During the procedure of authentication, MME chooses Public Land Mobile

TABLE 1. Database of HSS.

User	International Mobile Subscriber Identity	Initial shared secret key	SQN_{HSK}
UE_i	$IMSI$	K_i	$SQN_{HSK(i-1)}$ $SQN_{HSK(i-2)}$ $SQN_{HSK(i-3)}$ $SQN_{HSK(i-4)}$ $SQN_{HSK(i-\cdots)}$ $SQN_{HSK(i-n)}$

Network Identity (PLMN ID)(PLMNID = MCC + MNC), the random number sent from the UE to MME and the random number sent from MME to the UE as the input to function $f()$, and produces function output as the challenge string for the UE. Then, the UE produces response string based on function $f()$, the random number sent from the UE to MME and the random number sent from MME to the UE. If the UE successfully responds to the challenge from MME, the UE and MME will produce the encryption key for IMSI based on part of the function $f()$ outputs. Therefore, Jang *et al.*'s scheme uses the symmetric encryption key to encrypt and send IMSI to achieve privacy protection.

The limitation of Jang *et al.*'s scheme is described below. (i) the secret function $f()$ is produced according to the MNC of the user. However, some other legal users such as UE′, who owns the same MNC and PLMN ID as the UE, stores the same secret function $f()$ as the UE. By intercepting the random numbers transmitted between the UE and MME, UE′ can successfully calculate the encryption key shared by the UE and MME, and obtain the IMSI for the UE by decrypting the message. (ii) owing to the knowledge of encryption key, MME can obtain the IMSI. Therefore, Jang *et al.*'s scheme does not have the security character that no third party knows the IMSI except the UE and HSS.

B. INTRODUCTION AND ANALYSIS OF HAMANDI et al.'s SCHEME[8]

Hamandi *et al.* put forward a HSK-AKA scheme for LTE network based on hybrid cryptosystem including symmetrical cryptosystem and asymmetrical cryptosystem. Hamandi *et al.* indicated that the research[23] existed limitations such as cannot avoid attacks from vicious MME, and presented an improved scheme based on identity index.

The basic idea of Hamandi *et al.*'s scheme is described below. The secret key K, IMSI and corresponding parameter SQN_{HSK} is shared by the UE and HSS. The parameter K, IMSI and SQN_{HSK} are stored in the database of HSS for every user, listed as follows in Table 1. SQN_{HSK} distributed for different user has special data scope. An IMSI belongs to a range i with $nSQN_{HSK}$ values, then this IMSI can be associated only with one of these n values each time.

The user sends SQN_{HSK}, insteading of IMSI in the EAP response/identity message. Then, HSS identifies the user according to the scope of SQN_{HSK} and obtains corresponding IMSI and K. After each authentication for the user, SQN_{HSK} will be updated within the scope according to the database of HSS. Therefore, Hamandi *et al.*'s scheme uses an identity index for corresponding IMSI to each user to achieve privacy protection.

When the UE makes a request for network access, MME sends a random number to UE, and the UE also sends a random to MME. Then, the UE produces $RMSI$ as the random factor of TMSI based on the above random numbers and initial shared secret key K to achieve the update of TMSI in each authentication. Therefore, Hamandi *et al.*'s scheme uses the updated TMSI in each authentication to achieve untraceability.

Although Hamandi *et al.* have made important contributions to achieve anonymity and untraceability, However, Hamandi *et al.*'s scheme still has its flaws.

(i) Hamandi *et al.* indicated that random factor $RMSI$ was shared by the UE and MME. But attackers can easily obtain $RMSI$ via $SQN \oplus AK$ and $RMSI \oplus SQN \oplus AK$ by segmenting the authentication vector $AUTN$ in bits.

$$AUTN = SQN \oplus AK \,||\, \left|SQN_{HSK} \oplus AK\right| \,||\, RMSI \oplus SQN \oplus AK \,||\, AMF \,||\, MAC \quad (14)$$

(ii) New security parameters such as $\mathrm{SQN_{HSK}}$ in Hamandi *et al.*'s scheme increases the cost of storage and management.

(iii) The authentication vector AV has been increased in length by adding the parameter RMSI, which leads to an increase in communication information capacity.

(iv) Researchers[9] have indicated that introducing changes in HSS and the UE minishes the burden of middle networking components, which is beneficial for the application and implementation of the schemes. However, Hamandi *et al.* have introduced changes in the middle communication entities such as MME, which is unwieldy in practice.

(v) In Hamandi *et al.*'s scheme, IMSI, K and SQN_{HSK} are stored in the database of HSS without any other protection. Insteading of IMSI, SQN_{HSK} is sent in EAP response/identity message. Such scheme does not achieve forward secrecy in case of the threat to the database.

C. INTRODUCTION AND ANALYSIS OF CHOUDHURY et al.'s SCHEME[9]

In order to solve problems in EAP-AKA scheme, an improved identity privacy protection scheme based on identity index is proposed by Choudhury *et al.* The basic idea of Choudhury *et al.* 's scheme is described below. As the identifier of the shared secret key, a random number RIC is shared by HSS and WLAN-UE. The HSS stores the mapping relationship between IMSI and RIC. Rather than storing RIC in clear format, the user encrypts the RIC and a random number $RAND$ with initial shared secret key K by function f_e and stores the ciphertext $ERAND$ in Universal Integrated Circuit Card (UICC)(Formula 15). When sending messages containing the identity, the user decrypts the ciphertext $ERAND$ by secret key K and gets the Dynamic Mobile Subscriber

Identity (DMSI) by formula 16 and sends DMSI insteading of IMSI.

$$ERAND = f_{eK}(RIC, RAND) \tag{15}$$

$$DMSI = MCC||MNC||RIC||ERIC \tag{16}$$

where $ERIC$ is generated by encrypting a padded RIC (RIC_{padded}) with encryption function f_n such as AES using initial shared secret key K. Thus,

$$ERIC = f_{nK}(RIC_{padded}) \tag{17}$$

And,

$$RIC_{padded} = RIC||CNT_{UE}||RN \tag{18}$$

CNT_{UE} is a 32 bits counter which gets incremented when a fresh DMSI is generated by the WLAN-UE, RN is a $128 - (32 + n)$ bits value, where n is the number of bits in RIC. The inclusion of RN completes the block size of 128 bits necessary to feed into the AES cipher and ensures the randomness of RIC_{padded}.

On receiving the DMSI, HSS searches this RIC in the database to identify the IMSI, and gets RIC_{padded} with decryption function f_d using the initial shared secret key K of corresponding user. $RIC_{padded} = f_{dK}(ERIC)$.

Then, HSS extracts CNT_{UE} from RIC_{padded}, updates $ERAND$ with new randomly chosen $RAND$ and RIC and sends to the UE $ERAND$ insteading of $RAND$ in authentication vector AV. To ensure the updating of $DMSI$, HSS stores RIC_{new}, RIC_{pre}, RIC_{old} for every user in case the same RIC is assigned to the same user in two successive authentication.

On receiving updated $ERAND$ from HSS, the UE updates DMSI according to formulas (15) $\sim$ (17) for EAP response/identity message in a new round of authentication.

Choudhury *et al.* 's scheme provides identity protection. Only WLAN-UE and HSS can obtain IMSI. HSS uses CNT_{UE} to prevent replay attack. However, Choudhury *et al.* 's scheme still has its flaws.

(i) Management of RIC increases the cost of storage and computation.

(ii) RIC is assigned to every UE, which increases network bandwidth capacity.

(iii)DMSI is updated in every round of authentication, which increases the cost of computation in mobile devices.

(iv) MCC and MNC in DMSI is sent in plaintext, which although fails to point to a particular user, yet useful information is provided for attackers, which means that the scheme does not provide identity privacy protection completely and does not achieve complete untraceability.

D. INTRODUCTION AND ANALYSIS OF DEGEFA et al.'s SCHEME[11]

Degefa *et al.* proposed a scheme based on identity encryption and identity index to achieve anonymity. The basic idea of Degefa *et al.* 's scheme is described below.

The UE and HSS pre-share parameters, including (i) secret function f' is used to generate shared secret key S for authentication. (ii) encryption function E is chosen and can be public. (iii) initial secret key K is shared like traditional LTE network. (iv) key identifier KI, which is chosen pointed to special secret key K, should be updated after every round of AKA authentication.

When responding to the request of identity, the UE chooses K and KI as input to function f', and produces function output S as the shared secret key for authentication for the UE and HSS. Then, the UE encrypts IMSI with encryption function E using shared secret key S and sends encrypted IMSI and KI to HSS.

On receiving above identity response message, HSS searches KI in the database to get corresponding K and produces S with function f'. Then, HSS decrypts the message to get the IMSI and updates KI. Next, HSS sends $S||KI_{new}$ to MME via secure channel. Thus, MME can obtain IMSI with secret key S and generates authentication vectors AV. Then, MME sends to the UE the encrypted KI_{new} and AV with secret key S.

Degefa *et al.*'s scheme realizes privacy protection by identity encryption and identity index. However, it still has its flaws.

(i) New security parameters such as key identifier KI increases the cost of storage and management.

(ii) Authentication vectors are generated by MME, which decrease the cost of communication between MME and HSS. However, MME can obtain IMSI, which results in that the scheme does not have the security character that no third party knows the IMSI except the UE and HSS.

(iii) The scheme exists on a premise: trust relationship between HSS and MME should be established.

E. INTRODUCTION AND ANALYSIS OF GHAFGHAZI et al.'s SCHEME[14]

Ghafghazi *et al.* hides IMSI in a bit string and introduces index for secret key to protect privacy. The basic idea of Ghafghazi *et al.* 's scheme is described below.

The UE chooses the shared secret key K_S, random number n, timestamp T_C and operation pattern P_S as input to message authentication code function HMAC, and generates function output bit string H_{K_S,P_S}.

$$H_{K_S,P_S} = HMAC(P_S||n||T_C)_{K_S} \tag{19}$$

Then, the UE generates bit string $SHMAC$. Consider the following example shown in Figure 2: checks the first bit of IMSI (the bit is 1), sequentially searches H_{K_S,P_S} until the first opposite bit from the bit of IMSI is found (the second bit of H_{K_S,P_S} is 0), and reverses the bit of H_{K_S,P_S}. Then, checks IMSI one bit by one bit and repeats the operation above. Thus, $SHMAC$ will be generated. Obviously, $SHMAC$ contains IMSI indirectly.

$$\begin{array}{rl} H_{K_S,P_S} = & 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ IMSI = & 1\quad 1\,0\,1\quad 1\,0\quad 0\,0 \\ \hline SHMAC = & 1\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1 \end{array}$$

FIGURE 2. Computation of SHMAC.

$$H_{K_S,P_S} = 1010101010111111111$$
$$SHMAC = 1111011100011111111$$
$$IMSI = 1\ 101\ 10\ 00$$

FIGURE 3. Computation of IMSI.

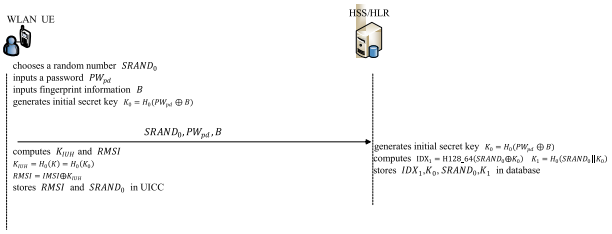

FIGURE 4. Registration phase.

Finally, the UE generates M_{ir} that has implication for IMSI to respond to the request of identity.

$$M_{ir} = SHMAC||n||T_C||K_C||P_C \tag{20}$$

where K_C is the index of secret key K_S, P_C is the index of operation pattern P_S. HSS stores K_C,K_S, P_C, P_S and those mapping relationships.

On receiving M_{ir} from the UE, HSS searches database for K_S and P_S according to K_C and P_C, computes H_{K_S,P_S} and obtains IMSI. Consider the following example shown in Figure 3: compares H_{K_S,P_S} and $SHMAC$ one bit by one bit, takes the bit of $SHMAC$ as one bit of IMSI when the bit of $SHMAC$ is different from that of H_{K_S,P_S}. In the example, $IMSI = 11011000$.

Ghafghazi *et al.*'s scheme still has its flaws.

(i) Although the researchers indicated that P_S and K_S should be updated for one-time key to achieve anonymity, no updating mechanism was introduced in the scheme. Thus, as the temporary identity, $SHMAC$ could not be updated.

(ii) New security parameters such as K_S, P_S, K_C and P_C in Ghafghazi *et al.*'s scheme increase the cost of storage and management.

(iii) Timestamp is used, which has synchronization issue between the UE and HSS.

IV. IMPROVED SCHEME FOR IDENTITY PRIVACY PROTECTION

In this section, an improved scheme based on identity index is proposed to achieve anonymity, untraceability and dynamic identity.

In the registration phase as shown in Figure 4, WLAN-UE chooses a random number $SRAND$ recorded as $SRAND_0$, inputs a password PW_{pd}. Then, HSS generates initial secret key K recorded as K_0 shared with WLAN-UE based on PW_{pd} and the fingerprint information B collected by an equipment which is shown as follows, where H_0 is a hash function.

$$K = K_0 = H_0(PW_{pd} \oplus B) \tag{21}$$

WLAN-UE computes K_{IUH} and initial temporary identity $RMSI$ as follows and stores $RMSI$ and $SRAND_0$ in the universal integrated circuit card.

$$K_{IUH} = H_0(K) = H_0(K_0) \tag{22}$$
$$RMSI = IMSI \oplus K_{IUH} \tag{23}$$

Then, When receiving the EAP request/identity message for the first time in the authentication phase, WLAN-UE inputs PW_{pd} and$B$ and computes K_0, K_{IUH} and IMSI according to formula (21-24), generates identity index IDX, temporary identity HMSI and shared secret key K recorded as IDX_1, HMSI_1 and K_1 according to formula (25-27) for the next round of authentication.

$$IMSI = RMSI \oplus K_{IUH} \tag{24}$$
$$\text{IDX}_1 = \text{H128\_64}(SRAND_0 \oplus K_0) \tag{25}$$
$$\text{HMSI}_1 = \text{IDX}_1||\text{L128\_64}(SRAND_0 \oplus K_0 \oplus IMSI) \tag{26}$$
$$K_1 = H_0(SRAND_0||K_0) \tag{27}$$

where, function H128_64 () is used to take out the first 64 bits of the function variable and function L128_64 is used to take out the last 64 bits of the function variable.

According to the length of security parameters in EPS-AKA scheme, length of parameters in our proposed scheme are listed in Table 2 and Table 3. In IMSI, MSIN consists of 10 digits in decimal. Therefore, the identity index IDX, which consists of 64 bits, can cover all mobile users.

Besides, in the registration phase, parameters listed in Table 4 have been stored in the database of HSS for every user. And the initial datas are recorded as IDX_1, K_0,$SRAND_0$, K_1.

TABLE 2. Length setting of security parameters for EPS-AKA protocol.

Security parameters	Length(bit)
K、CK、IK、$IMSI$、$RAND$	128
AK、AMF、SQN	48
$AUTN$	160
SN_{ID}、MAC、$XMAC$、RES、$XRES$	64
K_{ASME}	256

TABLE 3. Length setting of security parameters for protocol in this paper.

Security parameters	Length(bit)
K_{IUH}、$HMSI$、$SRAND$	128
IDX	64

TABLE 4. HSS database in improved scheme.

Security parameters	
User equipment	UE
International mobile user identification code	$IMSI$
identity index	IDX_1
Initial/current shared secret key	K_0
Random number	$SRAND_0$
Updated shared secret key	K_1

TABLE 5. Updation of HSS database in our improved scheme ($i \geq 1$).

Security parameters	
User equipment	UE
International mobile user identification code	$IMSI$
identity index	$IDX_{(i+1)1}$
	$IDX_{(i+1)2}$
	$IDX_{(i+1)3}$
	...
	$IDX_{(i+1)N}$
current shared secret key	K_i
Random number	$SRAND_{i1}$
	$SRAND_{i2}$
	$SRAND_{i3}$
	...
	$SRAND_{iN}$
Updated shared secret key	K_{i+1}

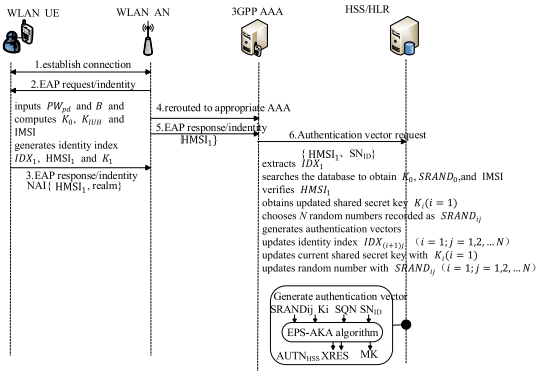

FIGURE 5. Authentication phase when UE sends HMSI for the first time (steps 7 to 23 are similar to that shown in Figure 1).

In our proposed protocol, when IMSI is needed, $HMSI$ will be sent and updated in a new round of authentication. $HMSI_i$ represents for the i-th time the user sends $HMSI$ in identity response message. For example, when accessing to the network for the first time, the UE sends HMSI_1.

As shown in Figure 5, when $i = 1$, on receiving $HMSI_1$ from AAA, HSS extracts IDX_1 according to formula 26, searches the database in Table 4, obtains K_0, $SRAND_0$,and IMSI according to the mapping relation and verifies $HMSI_1$ by checking whether $L128\_64(HMSI_1) = (SRAND_0 \oplus K_0 \oplus IMSI)$ or not. Let N be the number of authentication vectors that HSS generates in one time. HSS obtains updated shared secret key $K_i(i = 1)$, chooses N random numbers recorded as $SRAND_{ij}(i = 1; j = 1, 2, \ldots N)$, generates authentication vectors for authentication in this round. Then, as listed in Table 5, HSS updates identity index $IDX_{(i+1)j}(i = 1; j = 1, 2, \ldots N)$ according to formula (28), updates current shared secret key with $K_i(i = 1)$, updates random number with $SRAND_{ij}(i = 1; j = 1, 2, \ldots N)$ to build the mapping relationship for a new round of entire EAP-AKA authentication.

$$IDX_{(i+1)j} = H128\_64\left(SRAND_{ij} \oplus K_i\right) \tag{28}$$

Instead of $RAND$ in authentication vectors in EAP-AKA, $SRAND$ is used in our proposed scheme. HSS uses $K_i(i = 1)$ and $SRAND_{ij}$ $(i = 1; j = 1, 2, \ldots N)j$ to generate N vectors and sends them to AAA. AAA forwards authentication challenging message to the UE. The UE uses $K_i(i = 1)$ to compute corresponding parameters to reply to authentication challenging.

As shown in Figure 6,when the UE needs to send HMSI for the (i+1)th ($i \geq 1$)j time, the UE computes the following parameters using any $SRAND_{ij}$ received in the last authentication. Then, the UE sends $HMSI_{i+1}$ to HSS.

$$IDX_{i+1} = H128\_64\left(SRAND_{ij} \oplus K_i\right) \tag{29}$$

$$HMSI_{i+1} = IDX_{i+1} || L128\_64(SRAND_{ij} \oplus K_i \oplus IMSI) \tag{30}$$

Then, HSS extracts IDX_{i+1} from $HMSI_{i+1}$, searches database and finds that IDX_{i+1} is equal to one of the values $IDX_{(i+1)1} \sim IDX_{(i+1)N}$. Supposing that $IDX_{i+1} = IDX_{(i+1)j}$, HSS obtains $SRAND_{ij}$ and K_i according to the mapping relationship from the database and computes K_{i+1} according to the formula 31 and updates updated shared secret key with K_{i+1} in Table 5. Then, HSS obtains updated shared secret key K_{i+1}, chooses new N random numbers $SRAND_{(i+1)j}(j = 1, 2, \ldots N)$, generates authentication vectors for this round of authentication. Finally, updates identity index $IDX_{(i+2)j}$ according to formula (28), updates current shared secret key with K_{i+1}, updates random number with $SRAND_{(i+1)j}(j = 1, 2, \ldots N)$ to build mapping relationship for new round (the (i+2)th time) of entire EAP-AKA authentication listed in Table 5.

$$K_{i+1} = H_0\left(SRAND_{iJ} || K_i\right) \tag{31}$$

HSS generates authentication vectors and sends them to AAA. AAA forwards authentication challenging message to the UE. Then, the UE uses K_i and $SRAND_{ij}$ to compute K_{i+1} as shown in formula 31 and corresponding parameters to reply to authentication challenging.

V. ANALYSIS ON SCHEMES FOR IDENTITY PRIVACY PROTECTION

A. SECURITY ANALYSIS

1) CORRECTNESS

In our proposed protocol, $IMSI$ is hidden in HMSI based on formula 26, which provides the identity privacy protection without transmitting IMSI in plaintext. Then, HSS stores the corresponding relationship in database as shown in Table 4 and Table 5. On receiving $HMSI_i$ from AAA, HSS extracts IDX_i according to formula 26, searches the database in Table 4, obtains K_i, $SRAND_i$,and IMSI according to the mapping relation and verifies $HMSI_i$ by checking whether $L128\_64(HMSI_i) = (SRAND_{(i-1)j} \oplus K_{i-1} \oplus IMSI)$ or not. Such checking makes that HMSI is used to identify the UE with specified IMSI.

2) ANONYMITY

The proposed scheme achieves anonymity based on identity index. Instead of transmitting IMSI in plaintext when sending

TABLE 6. Comparation between different schemes (including security).

	Solution ideas	With no change in the implementation of intermediate network components	IMSI cannot be obtained by any third party	With no change in the structure of authentication vectors and communication information in EAP-AKA scheme
Jang's scheme	Encrypt *IMSI*	×	×	×
Hamandi's scheme	*IMSI* index	×	√	×
Choudhury's scheme	*IMSI* index	√	√	√
Degefa's scheme	*IMSI* index and Encrypt *IMSI*	√	×	√
Ghafghazi's scheme	Hide *IMSI* in bit strings、encryption key index for *IMSI*	√	√	×
Our scheme	*IMSI* index	√	√	√

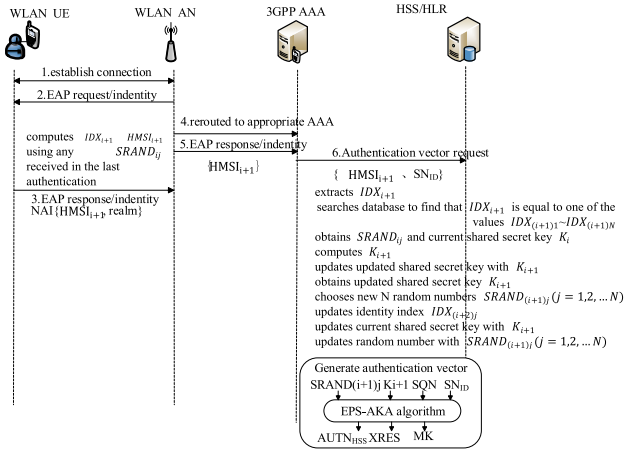

FIGURE 6. Authentication phase when UE sends HMSI for the (i+1)th (i ≥ 1) time (steps 7 to 23 are similar to that shown in Figure 1).

EAP response/identity message in step 3 in Figure 1, *HMSI* is used to identify the particular user. According to Formula 26 and 31, attackers cannot obtain the IMSI without the knowledge of the shared secret key K_i, while identity index *IDX* is used to provide corresponding relationship between IMSI and *HMSI* for the user. Besides, *HMSI* and *IDX* are both updated in every round of authentication. Therefore, the proposed scheme gives the user the privilege of anonymity, which eliminates any chance for attacker to identify the past identity requests and responses of the same subscriber.

3) IDENTITY DYNAMICS AND UNTRACEABILITY

The calculation of *HMSI* involves a random number *SRAND*, which ensures that the correlation of *HMSI* in every round of authentication is zero. So, different temporary identities *HMSI* will be used in each authentication process for the same user and cannot be identified as belonging to the same user by attackers. Therefore, our scheme achieves identity dynamics and untraceability during the procedure of mobile communication.

4) IMPERSONATION ATTACK

According to section III, information stored in the universal integrated circuit card which will be used for authentication can completely protect the privacy of user identity. In our identity privacy protection scheme, although attackers can get *RMSI* by cracking the information in UICC, they cannot obtain *HMSI* without the knowledge of all the three authentication attributes, including UICC, PW_{pd} and B according to formulas 21∼26. Therefore, attackers fail to be authenticated by HSS without correct EAP response/identity message. That is, only the legal individual user can compute the *HMSI* with UICC, PW_{pd} and B and accomplish successful authentication.

Hence, our protocol can resist impersonation attack.

5) REPLAY ATTACK

The attacker captures the previous transmitted message to launch the replay attack to make the received entity believe that the transmitted message is from legal entity and fresh. For WLAN-UE, *HMSI* and shared secret key K_i are both updated in every round of authentication, which means that the attacker who replays the previous login message in step (iii) and the response challenging message in step (xv) in Figure 1 cannot achieve connection to HSS and be authenticated by HSS. As the previous messages contains invalid *HMSI* and *RES* for a new round of authentication.

Hence, our protocol can resist replay attack.(vi) man-in-the-middle attack.

The update mechanism of *HMSI* makes our scheme resist replay attacks. Therefore, if the attacker sends *HMSI* to HSS to request connection through replay attacks, HSS will judge the attacker as an illegal user. Then, the attacker cannot obtain authentication vectors to accomplish man-in-the-middle attacks.

Comparation with the identity privacy protection schemes proposed by recent researchers and our scheme is made as follows.

Table 6 lists the security performance of each scheme. Where, the symbol "X" in the table indicates that the scheme does not support the corresponding security performance, and the symbol "√" indicates that the scheme supports the corresponding security performance. As the existing mobile operators use EAP-AKA/EAP-AKA' protocol in 3GPP standard in practical application for many years, which has

certain efficiency and security characteristics. Therefore, the improvement of IMSI identity privacy protection should not change the original protocol structure, nor change the implementation of intermediate network components, but simply make configuration at the the communication end such as mobile operators and clients.

As can be seen from the datas in Table 6, the scheme in this paper and the Choudhury's scheme have the most complete security features.

B. SECURITY PROOF ON ANONYMITY

In previous researches, many researchers devoted on evaluating and quantifying the anonymity of anonymous communication protocols and systems [24]. The efforts on the formalization of anonymity can be divided into methods based on process calculi [25], epistemic logic [26], UC framework [27], differential privacy [28], probabilistic automata [29], [30] and I/O automata [31]. Many Backes *et al.* [28] proposed a framework AnoA for analyzing anonymity properties relying on the notion of computational differential privacy. A thorough analysis of the sender anonymity property of our proposed protocol will be conducted in this subsection. The main notion in AnoA is summarized as below.

(1) Denote that a protocol with a user space U, a recipient space R and an auxiliary information space Aux. Users' actions are modeled as an input to the protocol and represented in the form of an ordered input table D of tuples $d_j = (u_j, (r_{ji}, aux_{ji})_{i=1}^{l})$ where $u_j \in U$, $r_{ji} \in R$, $aux_{ji} \in Aux$.

(2) Definiton($\mathcal{A}^{SACH(P,u)}$). $\mathcal{A}^{SACH(P,u)}$ denotes the interaction of $\mathcal{A}$ and $SACH\ (P, u)$ in which $SACH\ (P, u)$ is a challenger. Place user u in the input table for a challenge, run protocol P on the input table and forward all messages that are sent from P to $\mathcal{A}$ and all messages that are sent from $\mathcal{A}$ to P.

(3) Definition(δ-sender anonymity). A protocol P with user space U of size N has δ-sender anonymity if for all PPT-adversaries $\mathcal{A}$

$$\Pr\left[u^* = u : u^* \leftarrow \mathcal{A}^{SACH(P,u)}, u \xleftarrow{R} U\right] \leq \frac{1}{N} + \delta,$$

where $\alpha \leftarrow \beta$ denotes that a value is drawn from the distribution β and α is assigned the outcome. $\alpha \xleftarrow{R} \beta$ denotes that α is drawn uniformly at random from the set β.δ depends on the probability of corruption of the network.

Proof: According to the EAP-AKA' authentication protocol showed in FIGURE 1, the ordered input table $D = (d_1, d_2, d_3, \ldots d_{23})$. In our improved protocol, *HMSI* is used to identify the UE with specified *IMSI*. Then, the security analysis can be defined as an attack game between an adversary $\mathcal{A}$ and the challenger $SACH\ (P, u)$ against the $d_1 = \{u, WLANAN, HMSI\}$ where $u = WLANUE$.

Step 1: The adversary $\mathcal{A}$ launches a challenge to the challenger $SACH\ (P, u)$.

Step 2: The challenger $SACH\ (P, u)$ chooses the user u^* with International Mobile Subscriber Identity $IMSI^*$ for the challenge, runs protocol P on $d_1 = \{u^*, WLANAN, HMSI\}$ and forwards all messages that are sent from P to $\mathcal{A}$ and all messages that are sent from $\mathcal{A}$ to P.

Step 3: The adversary $\mathcal{A}$ guesses the value of u^* with International Mobile Subscriber Identity $IMSI^*$.

According to formula 26, the adversary $\mathcal{A}$ cannot get the explicit mapping relation between *HMSI* and *IMSI*. By running protocol P on $d_1 = \{u^*, WLANAN, HMSI\}$, the adversary $\mathcal{A}$ guesses the value of u^* with $IMSI^*$ based on *HMSI*. However, according to Table 3, *HMSI* consists of 128 bits, which means that the number of users to send EAP request/identity at the same time with different *HMSI* can be 2^{128}, and also means that one value of *HMSI* maps to one of 2^{128} users who is the user u^* with $IMSI^*$, then

$$\Pr\left[u^*(IMSI^*) = u : u^* \leftarrow \mathcal{A}^{SACH(P,u)}, u \xleftarrow{R} U\right] = \frac{1}{2^{128}}$$

As the world population is less than 2^{36}, denote that the user space U of size $N = 2^{36}$.

Obviously, in our improved protocol,

$$\Pr\left[u^*(IMSI^*) = u : u^* \leftarrow \mathcal{A}^{SACH(P,u)}, u \xleftarrow{R} U\right] \leq \frac{1}{N} + \delta.$$

Therefore, our improved protocol provide δ-sender anonymity.

C. PERFORMANCE ANALYSIS

1) STORAGE COST

In Hamandi's scheme, new security parameter SQN_{HSK} increases the cost of storage in HSS. It is indicated the range count of SQN_{HSK} should be bigger than the number of users in order to allow SQN_{HSK} change without having repetition or frequent collision when choosing a random value from the range. But the length of SQN_{HSK} is not set specifically. According to our definition and analysis above, as MSIN consists of 10 digits in decimal, we assume that SQN_{HSK} which consists of 64 bits, can cover all mobile users. According to Table 1, n is the number of SQN_{HSK} values, and $n \geq 2$ apparently, while each user has N authentication vectors in each authentication process. Therefore, the storage increasement for each user with N authentication vectors in Hamandi's scheme will be $64{*}n{*}N$ bits, and at least $64 * 2{*}N$ bits.

In Choudhury's scheme, new security parameter *RIC* increases the cost of storage in HSS. However, the length of *RIC* is not set specifically. According to the analysis above, we also assume that *RIC* which consists of 64 bits, can cover all mobile users. Then, the storage increasement for each user with N authentication vectors to store *RIC* will be $64 * N$ bits. Besides, as HSS stores $RIC_{new}, RIC_{pre}, RIC_{old}$ for every user in case the same *RIC* is assigned to the same user in two successive authentication, the storage increasement for each user with N authentication vectors in Choudhury's scheme will be $64{*}N * 3$ bits.

In Degefa's scheme, new security parameter *KI* increases the cost of storage in HSS. However, the length of *KI* is not set

TABLE 7. Comparation between different schemes(including storage capacity).

	Storage capacity of HSS	Increasement for each user
Jang's scheme	Has no change	0
Hamandi's scheme	increase	$128 * N$
Choudhury's scheme	increase	$192 * N$
Degefa's scheme	increase	$64 * N$
Ghafghazi's scheme	increase	$256 * N$
Our scheme	increase	$64 * N + 128$

specifically. We also assume that *KI* which consists of 64 bits, can cover all mobile users. Then, the storage increasement for each user with N authentication vectors in Degefa's scheme will be $64 * N$ bits.

In Ghafghazi's scheme, new security parameters such as K_S, P_S, K_C and P_C increase the cost of storage in HSS, length of which are also not set specifically. As mentioned above, we also assume that they all consist of 64 bits. Then, the storage increasement for each user with N authentication vectors in Ghafghazi's scheme will be $64 * N * 4$ bits.

According to Table 4 and 5, new security parameters including identity index IDX (64bits) and updated shared secret key K_{i+1} (128bits) in our proposed scheme increase the cost of storage in HSS. And the storage increasement for each user with N authentication vectors will be $64 * N + 128$ bit.

Table 7 briefly introduces the storage capacity of HSS in different identity privacy schemes in the 3GPP system. As can be seen from the datas in Table 7, Jang's scheme has no change in storage increasement of HSS compared with EAP-AKA scheme. Degefa's scheme and our scheme increase less than others, while Ghafghazi's scheme increase the most.

2) EFFICIENCY

Table 8 shows the calculation time of relevant cryptography operations used in the identity privacy protection schemes mentioned above [8], [32]. In EPS-AKA protocol, function *HMAC-SHA*-256 is used in function $f_1 \sim f_5$ and *KDF*. [8], [23]. In this paper, we assume that the symmetric encryption/decryption functions not explicitly specified in each scheme adopt AES function, and the Hash function adopts SHA1 function.

In Table 9, since TMSI are not introduced in the schemes using encrypted IMSI, the TMSI in "calculation time of *TMSI* " and "required communication to calculate TMSI" is equivalent to the ciphertext for encrypted IMSI. In addition, in Jang's scheme, IMSI is calculated by MME rather than HSS.

It can be seen from the performance comparison in Table 9 that the encryption method to achieve the protection of user identity privacy requires the use of encryption and decryption function, which requires a large amount of calculation and a long time delay. The identity index method to achieve the protection of user identity privacy has a small amount of calculation and a short time delay, which is more suitable for the mobile communication network. As the limited resources and bottleneck of power supply in the UE, calculation time in each communication entity should be reduced especially for the UE, while ensuring the basic security performances. Then, Figure 7 only shows the calculation time of TMSI(DMSI) for the UE in different protocols. According to datas in Table 9 and Figure 7, Ghafghazi's scheme and ours are superior to other schemes in terms of efficiency in calculation and communication.

TABLE 8. Calculation time of relevant cryptography operations.

	description	calculation time（us）
T_{HMAC}	calculation time of function HMAC-SHA-256	0.55
T_E/T_D	calculation time of Symmetric encryption/decryption function AES	130.3
T_h	calculation time of function SHA1	0.4
T_{sch}	Search time for IMSI based on identity index	Based on search algorithm, calculation time is unknown
T_{fe}	calculation time of encryption/decryption function f_e in Choudhury's scheme	Without deterministic algorithm, calculation time is unknown and set as traditional AES

In this section, analysis in security, storage cost and efficiency among different identity privacy protection schemes have been made. TABLE 10 shows the comparison result that which protocols provides the more outstanding performance in corresponding factor. According to all the data in TABLE 6, 7, 9 and 10, although Jang's scheme has no change in storage increasement of HSS compared with EAP-AKA scheme, it provides worst security. Although Ghafghazi's scheme provides outstanding performance in efficiency, it increases the most storage cost in HSS and brings changes in communication information in EAP-AKA scheme. Although Choudhury's scheme provides the most complete security features, it provides the highest calculation time for the UE, which is not appropriate for the portable UE.

Although the performance evaluation of protocols above is difficult to calculate accurately, analysis in this section shows that comprehensively considering all the factors above, our proposed protocol provides optimized security and outstanding performance in storage cost and efficiency compared to other schemes. Besides, our improved protocol provides more security properties without structure modification from EAP-AKA protocol, the storage capacity of HSS should be improved to accomplish the identity privacy protection in our protocol. However, according to the analysis results in TABLE 7, let $N = 10$, the storage increasement for each user with N authentication vectors in our scheme will be

TABLE 9. Comparation between different schemes(including efficiency).

	calculation time of *TMSI*（*DMSI*） for the UE（*us*）	communication required to calculate initial *TMSI* for the UE	calculation time of *IMSI* for HSS（*us*）	communication required to obtain *IMSI* for HSS
Jang's scheme	$1T_h + 1T_E$（130.7）	4	$1T_h + 1T_D$（130.7）	5
Hamandi's scheme	$3T_{HMAC}$（1.65）	8	$1T_{HMAC}$（0.55）	3
Choudhury's scheme	$1T_{fe} + 1T_E$（260.6）	0	$1T_{sch}$	2
Degefa's scheme	$1T_{HMAC} + 1T_E$（130.85）	0	$1T_{HMAC} + 1T_D$（130.85）	2
Ghafghazi's scheme	$1T_{HMAC}$（0.55）	0	$1T_{HMAC}$+$1T_{sch}$(0.55+$1T_{sch}$)	2
Our scheme	$2T_h$（0.8）	0	$1T_{sch}$	2

TABLE 10. Outstanding schemes in terms of security, storage cost and efficiency.

Security	Storage cost	Efficiency
Our scheme	Jang's scheme	Our scheme
Choudhury's scheme	Degefa's scheme	Ghafghazi's scheme
	Our scheme	

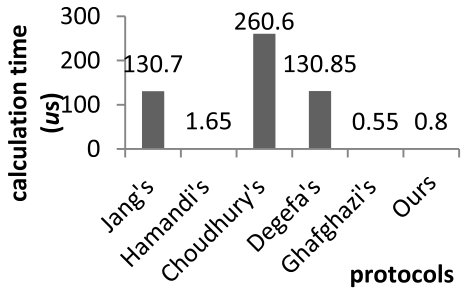

FIGURE 7. Calculation time of TMSI(DMSI) for the UE in different protocols.

nearly 100B. Assume that the number of the UE is nearly 10 billion, which is less than 2^{36}, the total storage increasement of HSS is only $2^{36} * 100B = 6400GB <$ 7TB. Therefore, such increase is very limited for HSS with abundant resources as computer performance continues to increase.

VI. CONCLUSION

Aiming at to avoid the drawbacks of the identity privacy protection scheme in LTE-WLAN heterogeneous converged network proposed by 3GPP, some typical improved identity privacy protection schemes have been analyzed. And on the basis of the study, an improved scheme based on identity index is proposed to achieve anonymity, untraceability and dynamic identity. In addition, the user identity information updation mechanism is provided, which provides the foundation for the design of the authentication schemes to resist replay attacks, man-in-the-middle attack and so on. The results of comparison with the related schemes show that security and efficiency of our proposed scheme is prior to some other existing ones with low computation cost and short time delay.

APPENDIX

TABLE 11. Notations in this paper.

Notation	Description
3GPP	The 3rd Generation Partnership Project
AAA	Authentication、Authorization、Accounting
AKA	Authentication Key Agreement
AUTN	Authentication Token
AV	Authentication Vector
DMSI	Dynamic Mobile Subscriber Identity
EAP	Extended Authentication Protocol
GUTI	Global Unique Temporary Identifier
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
WLAN	Wireless Local Area Network
XRES	Expected Response

REFERENCES

[1] A. A. Ajibesin, F. O. Bankole, and A. C. Odinma, "A review of next generation satellite networks: Trends and technical issues," in *Proc. AFRICON*, Sep. 2009, pp. 1–7.
[2] D. Astely, E. Dahlman, A. Furuskär, Y. Jading, M. Lindström, and S. Parkvall, "LTE: The evolution of mobile broadband," *IEEE Commun. Mag.*, vol. 47, no. 4, pp. 44–51, Apr. 2009.
[3] H. Safa, H. Artail, M. Karam, R. Soudah, and S. Khayat, "New scheduling architecture for IEEE 802.16 wireless metropolitan area network," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, vol. 1, May 2007, pp. 203–210.
[4] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks," *IEEE Commun. Mag.*, vol. 35, no. 9, pp. 116–126, Sep. 1997.
[5] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 70–77, Aug. 2002.

[6] M. Jo, T. Maksymyuk, R. L. Batista, T. F. Maciel, A. L. F. de Almeida, and M. Klymash, "A survey of converging solutions for heterogeneous mobile networks," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 54–62, Dec. 2014.

[7] D. Laselva, D. Lopez-Perez, M. Rinne, and T. Henttonen, "3GPP LTE-WLAN aggregation technologies: Functionalities and performance comparison," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 195–203, Mar. 2018.

[8] K. Hamandi, I. Sarji, A. Chehab, I. H. Elhajj, and A. Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, L. Barolli, F. Xhafa, M. Takizawa, T. Enokido, H. H. Hsu, Eds., Mar. 2013, pp. 929–934.

[9] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Improving identity privacy in 3GPP-WLAN," in *New Trends in Networking, Computing, E-Learning, Systems Sciences, and Engineering* (Lecture Notes in Electrical Engineering), vol. 312. Berlin, Germany: Springer, 2015, pp. 217–224.

[10] U. Jang, H. Lim, and H. Kim, "Privacy-enhancing security protocol in LTE initial attack," *Symmetry*, vol. 6, no. 4, pp. 1011–1025, Dec. 2014.

[11] F. B. Degefa, D. Lee, J. Kim, Y. Choi, and D. Won, "Performance and security enhanced authentication and key agreement protocol for SAE/LTE network," *Comput. Netw.*, vol. 94, pp. 145–163, Jan. 2016.

[12] *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and key Agreement (EAP-AKA')*, IETF, document RFC 5448, 2009. [Online]. Available: https://www.rfc-editor.org/info/rfc5448

[13] C. Dong and C. Wang, "A new amended authentication protocol in 3G-WLAN interworking," in *Proc. 3rd Int. Conf. Instrum., Meas., Comput., Commun. Control*, Sep. 2013, pp. 1261–1265.

[14] H. Ghafghazi, A. El Mougy, and H. T. Mouftah, "Enhancing the privacy of LTE-based public safety networks," in *Proc. 39th Annu. IEEE Conf. Local Comput. Netw. Workshops*, Sep. 2014, pp. 753–760.

[15] J. B. B. Abdo, H. Chaouchi, and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for EPS," in *Proc. Symp. Broadband Netw. Fast Internet (RELABIRA)*, May 2012, pp. 73–77.

[16] X. Li and Y. Wang, "Security enhanced authentication and key agreement protocol for LTE/SAE network," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–4.

[17] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA," in *Proc. Wireless Telecommun. Symp.*, May 2009, pp. 309–316.

[18] C.-M. Huang and J.-W. Li, "Reducing signaling traffic for the authentication and key agreement procedure in an IP multimedia subsystem," *Wireless Pers. Commun.*, vol. 51, no. 1, pp. 95–107, Oct. 2009.

[19] G. M. Koien, "Mutual entity authentication for LTE," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, Jul. 2011, pp. 689–694.

[20] M. Abdelkader, M. Hamdi, and N. Boudriga, "A novel advanced identity management scheme for seamless handoff in 4G wireless networks," in *Proc. IEEE Globecom Workshops*, Dec. 2010, pp. 2075–2080.

[21] Y. P. Deng, H. Fu, X. Z. Xie, J. H. Zhou, Y. C. Zhang, and J. L. Shi, "A Novel 3GPP SAE Authentication and Key Agreement Protocol," in *Proc. IEEE Int. Conf. Netw. Infrastruct. Digit. Content*, J. Guo, Ed., Nov. 2009, pp. 557–561.

[22] *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, Addressing and Identification*, 3GPP, document TS 23.003 V9.1.0, 2009. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.003/

[23] C. K. Huan, "Security analysis and enhancements in LTE-advanced networks," Ph.D. dissertation, Dept. Inf. Comput. Eng., Sungkyunkwan Univ., Seoul, South Korea, 2011.

[24] T. Lu, Z. Du, and Z. J. Wang, "A survey on measuring anonymity in anonymous communication systems," *IEEE Access*, vol. 7, pp. 70584–70609, 2019.

[25] M. Moran, J. Heather, and S. Schneider, "Verifying anonymity in voting systems using CSP," *Formal Aspects Comput.*, vol. 26, no. 1, pp. 63–98, Jan. 2014.

[26] J. Y. Halpern and K. R. O'Neill, "Anonymity and information hiding in multiagent systems," *J. Comput. Secur.*, vol. 13, no. 3, pp. 483–514, Aug. 2005.

[27] M. Backes, P. Berrang, O. Goga, K. P. Gummadi, and P. Manoharan, "On profile linkability despite anonymity in social media systems," in *Proc. ACM Workshop Privacy Electron. Soc.*, Oct. 2016, pp. 25–35.

[28] M. Backes, A. Kate, P. Manoharan, S. Meiser, and E. Mohammadi, "ANOA: A framework for analyzing anonymous communication protocols unified definitions and analyses of anonymity properties," in *Proc. IEEE 26th Comput. Secur. Found. Symp.*, Jun. 2013, pp. 163–178.

[29] M. E. Andrés, C. Palamidessi, P. van Rossum, and A. Sokolova, "Information hiding in probabilistic concurrent systems," *Theor. Comput. Sci.*, vol. 412, no. 28, pp. 3072–3089, Jun. 2011.

[30] K. Qiao, H. Tang, W. You, and Y. Zhao, "Blockchain privacy protection scheme based on aggregate signature," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Big Data Anal. (ICCCBDA)*, Apr. 2019, pp. 492–497.

[31] J. Feigenbaum, A. Johnson, and P. Syverson, "A model of onion routing with provable anonymity," in *Proc. Financial Cryptogr. Data Secur.*, Scarborough, Trinidad and Tobago, 2007.

[32] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Comput. Electr. Eng.*, vol. 45, pp. 274–285, Jul. 2015.

LILING CAO was born in Hengyang, Hunan, China, in 1982. She received the B.S. degree in electronic information science and technology and the M.S. degree in physics electronics from Central South University, in 2004 and 2007, respectively, and the Ph.D. degree in testing technology and automation from Tongji University, in 2017.

Since 2017, she has been a Senior Engineer with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include network security and authentication protocol.

ZHANG YU was born in 1996. She received the bachelor's degree in mechanical design and manufacturing and its automation from the Huaiyin Institute of Technology, in 2019. She is currently pursuing the master's degree with the Department of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include communication security and the Internet of Things technology.

YUQING LIU was born in 1976. She received the B.S. degree in industry automation, the M.S. degree in control theory and control engineering, and the Ph.D. degree in structural engineering from the Wuhan University of Technology, in 1999, 2002, and 2005, respectively.

She is currently an Associate Professor with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include marine Internet of Things engineering, fisheries engineering, and automation technology research.

SHOUQI CAO was born in 1973. He received the B.S. degree in mechanical manufacturing technology and equipment and the M.S. degree in mechanical manufacturing and automation from Sichuan University, in 1996 and 1999, respectively, and the Ph.D. degree in control science and engineering from Shanghai University, in 2009.

He is currently a Professor and a Doctoral Supervisor with the College of Engineering Science and Technology, Shanghai Ocean University. His main research interests include marine Internet of Things engineering, fisheries engineering, and automation technology research.