Egyptian Informatics Journal 18 (2017) 193–203

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Anonymous authentication and location privacy preserving schemes for LTE-A networks

Zaher Jabr Haddad [a,*], Sanaa Taha [b], Imane Aly Saroit [b]

[a] *Department of Computer Science, Al-Aqsa University, Gaza, Palestine*
[b] *Department of Information Technology, Cairo University, Cairo, Egypt*

A R T I C L E I N F O

Article history:
Received 31 July 2016
Revised 15 December 2016
Accepted 17 January 2017
Available online 11 February 2017

Keywords:
LTE-A
Anonymous authentication
Pseudonymes
Schnorr Zero knowledge protocol
IMSI
Privacy
Tracking attack
HSS
MME
BS

A B S T R A C T

Long Term Evaluation Advanced (LTE-A) is the third generation partnership project for cellular network that allows subscribers to roam into networks (i.e., the Internet and wireless connections) using spacial purpose base-stations, such as wireless access points and home node B. In such LTE-A based networks, neither base-stations, nor the Internet and wireless connections are trusted because base-stations are operated by un-trusted subscribers. Attackers may exploit these vulnerabilities to violate the privacy of the LTE-A subscribers. On the other hand, the tradeoff between privacy and authentication is another challenge in such networks. Therefore, in this paper, we propose two anonymous authentication schemes based on one-time pseudonymes and Schnorr Zero Knowledge Protocols. Instead of the international mobile subscriber identity, these schemes enable the user equipment, base-stations and mobility management entity to mutually authenticate each others and update the location of the user equipment without evolving the home subscriber server. The security analysis demonstrate that the proposed schemes thwart security and privacy attacks, such as malicious, international mobile subscriber identity catching, and tracking attacks. Additionally, our proposed schemes preserve the location privacy of user equipment since no entity except the mobility management entity and Gate-Way Mobile Location Center can link between the pseudonymes and the international mobile subscriber identity. Also attackers have no knowledge about international mobile subscriber identity. Hence, the proposed schemes achieve backward/forward secrecy. Furthermore, the performance evaluation shows that the proposed handover schemes impose a small overhead on the mobile nodes and it has smaller computation and communication overheads than those in other schemes.

1. Introduction

As a promising packet-based system, and envisioned toward forth generation cellular networks, the Long Term Evaluation Advanced (LTE-A) system is developed through the Third Generation Partner Project (3GPP) to enhance network's Quality of Service, including [1]: (1) increasing bandwidth up to 100 MHz; (2) enhancing performance using Multiple Input Multiple Output (MIMO) and coordinate scheduling; (3) supporting heterogeneous networks; and (4) providing sufficient services for the cell edge [2]. Moreover, LTE-A systems are open nature networks where a User Equipment (UE) employs different types of connectivity, such wireless and Internet, and of Base Stations (BSs), such as the Home node B (HeNB). Subscribers in LTE-A systems may own HeNBs as well as employ traditional Access Points (APs) used in wireless local area network to roam through different LTE-A networks [3].

Like other cellular systems, LTE-A has different mobility procedures, such as Evolved Packet system Authentication and Key Agreement (EPS-AKA) and location update procedures, to perform system functionalities, include, authentication, call originating, handover, location update, and paging [4]. Despite quality of service enhancement, UE Location in LTE-A network suffers security and privacy issues such as tracking, tracing and impersonating since the International Mobile subscriber Identity (IMSI) is exchanged

* Corresponding author.
E-mail addresses: zj.haddad@alaqsa.edu.ps (Z.J. Haddad), staha@fci-cu.edu.eg (S. Taha), i.saroit@fci-cu.edu.eg (I.A. Saroit).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.eij.2017.01.002
1110-8665/

in clear text between the LTE-A network entities. Therefore, security and privacy adversaries, such as impersonating, IMSI catching, and tracking, may exploit the open nature of the LTE-A connectivity and BSs [5]. In addition, the tradeoff between the UE privacy and authentication make it a challenge to secure such networks.

In this paper, we propose two novel anonymous authentication and location privacy preserving scheme for LTE-A network to thwart potential attacks violating the privacy of LTE-A networks. Both schemes keep the original LTE-A infrastructure.

The reasons behind introducing two anonymous authentication schemes as following: the first scheme, the pseudo random-based authentication scheme, is suitable for call establishment procedure which requires fast authentication to solve the call termination problem. The second scheme, the Zero knowledge authentication scheme, is suitable for the handover procedure where there are two evolving entities, eNBs, that need to verify each other as a prover and verifier [6].

In the first scheme, we use pseudonymes based public key cryptography, named pseud-auth, to perform the authentication procedure. In pseud-auth scheme, only the Mobility and Management Entity (MME) can link the pseudonymes and IMSI, therefore, pseudonymes are used to perform a mutual authentication between the UE, BS and the MME. BSs can verify pseudonymes without knowing the IMSI. pseud-auth scheme allows UE, BS and MME to share a symmetric key to be use for achieving the LTE-A security requirements, such as integrity, confidentiality, and non-repudiation.

The second scheme, relies on schonner zero knowledge protocol and public key cryptography (SZN-auth) to perform the authentication procedure. In SZN-auth, only the Gate-Way Mobile Location Center (GMLC) can extract IMSI, therefore, random numbers are used to perform a mutual authentication between the UE, BS and the MME without revealing the secret information regarding to the UE. SZN-auth scheme allows each entity of the network to verify the correctness of the message without need to reveal secret information of that entity. Table 1 shows the full definition of the abbreviations used throughout the paper.

The remainder of the paper is organized as follows.The related work is outlined in Section 2. Section 3 discusses the network and threat models. Section 4 describes the schnorr zero knowledge protocols. The proposed schemes are explained in Section 5. The security, privacy and performance evaluations are provided in Sections 6 and 7, respectively. Section 8 describes the experimental results of the proposed scheme. Finally, Section 9 concludes the paper and suggests some future works.

Table 1
List of abbreviations.

Acronym	Definition
LTE-A	Long Term Evaluation – Advanced
3GPP	Third Generation Partnership Project
UE	User Equipement
BS	Base Station
eNB	Evolved Node B
HeNB	Home Evolved Node B
EPS-AKA	Evolved Packet System authentication and Key Agreement Protocol
HSS	Home Subscriber Server
MME	Mobility and Management Enitity
E-UTRAN	Evolved universal terrestrial Radio Access Network
2G GSM	Second Generation Global System for mobile
3G UTRAN	Third Generation Universal Terrestrial Radio Access Network
eNB	Evolved Node B
GMLC	Gateway Mobile Location center
SGW	Serving Gateway
SGSW	Serving Gateway Support Node
PDN SW	Packet Data Network Serving Gateway
ME	Mobile Element
PSTN	Public Switching Telephony Network

2. Related work

The importance of the UE privacy preserving in the LTE-A networks attracts the researchers providing work for handling its problems [7]8. The ideas of anonymous authentication and location privacy schemes are divided into three main categories: encrypting IMSI, using dynamic identity, and using pseudonymes.

For encrypting IMSI, in [9], Abdo et al. address the IMSI capturing as privacy problem in LTE network authentication protocol. Therefore, they proposes a self-certified scheme called (SP-AKA) based on the public key cryptography to encrypt the IMSI during their transmission. However, the linkability between two transmitted identity is still a privacy problem. In [10], Sanaa Taha and Xuemin Shen consider the anonymity and location privacy of mobile node in the case of heterogenous networks. They consider the location privacy preserving of mobile node as a problem faced the seamless roaming via heterogenous networks. Therefore, authors introduce anonymous home building update scheme for mobile IPv6 wireless networking. In this scheme, authors achieve mutual authentication and share a symmetric key between two anonymous network entities. In [11], So-In figured that the IP-based architecture of the 4G networks bring several problems such as mobility, multi-homing and location privacy. Therefore, they introduce a proxy protocol as a modification of the standard mobile IPv6 protocol. In this scheme, authors uses virtual identity to achieve location privacy. However, proxy protocols allow home entity to delegate a privilege to other entity in order to sign on behalf of the home entity. Therefore, the presence of impersonating attacks still a big problem faced the delegation authority. In [12], Tuan Ta and John Baras prove that the paging procedure of LTE network suffers a lack of location privacy problem. Therefore, they suggest to embed the user identity information of the mobile into the transmitted signal properties that carry the paging information. However, this scheme requires a modification of the signal recognition in the physical layer, which is not desirable in the network.

For dynamic identity-based privacy schemes, in [13], Hamandi et. al. consider the AP and the Internet connection as untrusted entities. Therefore, attackers, such as active and passive attackers, may disseminate through those untrusted APs and Internet connections to violate the privacy of the UEs. For the purpose of UE privacy preserving, [13] employs a dynamic identity instead of using the traditional IMSI to create the pseudonyms (W-AKA). However, in this scheme, the Home subscriber Server (HSS) entities should initially or periodically be met in each authentication process causing a big overhead on the network. Furthermore, Despite this scheme achieves the forward secrecy, the backward secrecy is not achieved since the next pseudonyms generated by the previous one. Moreover, the IMSI should be transmitted in clear text at the registration process, which makes the IMSI linkable. Additionally, In [14], Gier M. Koien, proposes a privacy enhanced mutual authentication scheme for LTE networks using identity based cryptography. Author considered the privacy of the UE may violated by the tracing attack since these attacks could link the sequence of temporary identities of UE. Therefore, authors used the public key encryption technique using dummy IMSI to make the temporary identity unlinkable and withstands the tracing attack. However, this scheme increases the number of messages required to perform the authentication, therefore, it consumes the bandwidth of the network. In [15], Jo et. al. consider the requirement of achieving location privacy of mobile node causes a big performance problems such as high communication, computation cost and huge revocation list. Therefore, authors introduce a privacy preserving scheme based on the identity based sign-encryption. However, authors claimed that the computation cost is a big problem and back to use the bilinear pairing which is well-known consume much time. Moreover, this scheme is not suitable for LTE-A network. The LTE-A authentication scheme is done between UE and MME with participating of the eNB which does not function as merely connecting between two entities.

For pseudonymes-based privacy schemes, [16], Hamandi et. al. propose pseudonymes in authentication scheme (HSK-AKA) to achieve the privacy of the IMSI. However, this scheme consumes the bandwidth of the network since the proposed authentication scheme should arrive to the HSS. Moreover, the network entities, MME and UE, has no ability to check the correctness of the pseudonymes; therefore, malicious attacker is still a problem. In addition, in [17], Choudhury et al., consider the permanent identity may cause the UE trackable. Therefore, they propose a pseudonym-based authentication scheme to preserve the privacy of the IMSI. However, the proposed authentication scheme should arrive to the HSS which requires more bandwidth consumption. Moreover, the proposed scheme depends on a new set of functions which may not be suitable to the infrastructure of the LTE network. Moreover, in [18], Purkhiabani et al. use the pseudonym to preserve the privacy of the IMSI in the LTE authentication scheme. However, the traceable attack is still a problem since attackers can link between the two permanent pseudonym. In this paper, we propose a pseudonym- based scheme to achieve IMSI privacy with considering the above drawbacks in our novel scheme.

3. System model

3.1. Network model

The architecture of the LTE-A network is mainly composed of two components as depicted in Fig. 1: the evolved packet core (EPC) and evolved universal terrestrial radio access network (E-UTRAN) [19]. The evolved packet core represents the wired part in the network, which is responsible for the overall control of UEs and the bearer establishment. Each entity in the evolved packet core has a responsibility as follows: the MME manages bearer and connection, and the HSS maintains the user subscription data and MME's identities. Packet data network gateway (PDN GW) performs mobility and inter-networking within the 3GPP and non-3GPP technologies respectively. A policy control and charging rule function (PCRF) entity is employed to control decision making of flow and Quality of Service [19]. GMLC is the LTE-A core network entity which is responsible for location services such as location selection, location cache, retrieval of global positioning system reference data from external global positioning system reference data [19]. The Base Station (BS) is the hardware connected to the mobile phone network that communicates directly with UEs. LTE-A supports three types of BS: (1) Evolved Universal Terrestrial Radio Access Network Node B, also known as Evolved Node B, (eNB), is the element in Evolved Universal Terrestrial Radio Access Network of LTE, (2) Home eNB is a special purpose BS installed in a specific area such as office or small building to enhance the service in this area, and (3) the Access Point is the base station of the wireless local area network. HeNB and AP are connected to the LTE-A network via The Internet [19]. Once the UE switches on, it runs an acquisition procedure to identify the nearby BSs and discover how they are configured. In doing so, UE accepts the primary and secondary synchronization signals, and reads the system information of each BS to select the closest one in order to initiate authentication and key agreement procedure over it.

The authentication procedure (EPS-AKA), Fig. 2, is the mobility procedure that is already implemented in the 3GPP release 9 for LTE networks to perform the mutual authentication and key agreement between network entities. EPS-AKA protocol works as follows [20]21:

1. A UE sends an access request message to the MME.
2. Upon receiving a request, the MME launches an authentication procedure by asking the UEs identity (IMSI).
3. In response to the MME, the UE sends its identity (IMSI).
4. The MME sends an authentication data request message containing IMSI to the HSS for acquiring the authentication vectors.
5. The HSS first generates authentication vectors for the MME, an authentication vector comprising a random number, challenge number, authentication challenge and symmetric key (K_{ASME}) instead of an integrity key, and cryptographic key.
6. The HSS sends back an authentication data request message including the generated authentication vector (for the corresponding UE), so that the MME is authorized to authenticate the requesting UE.

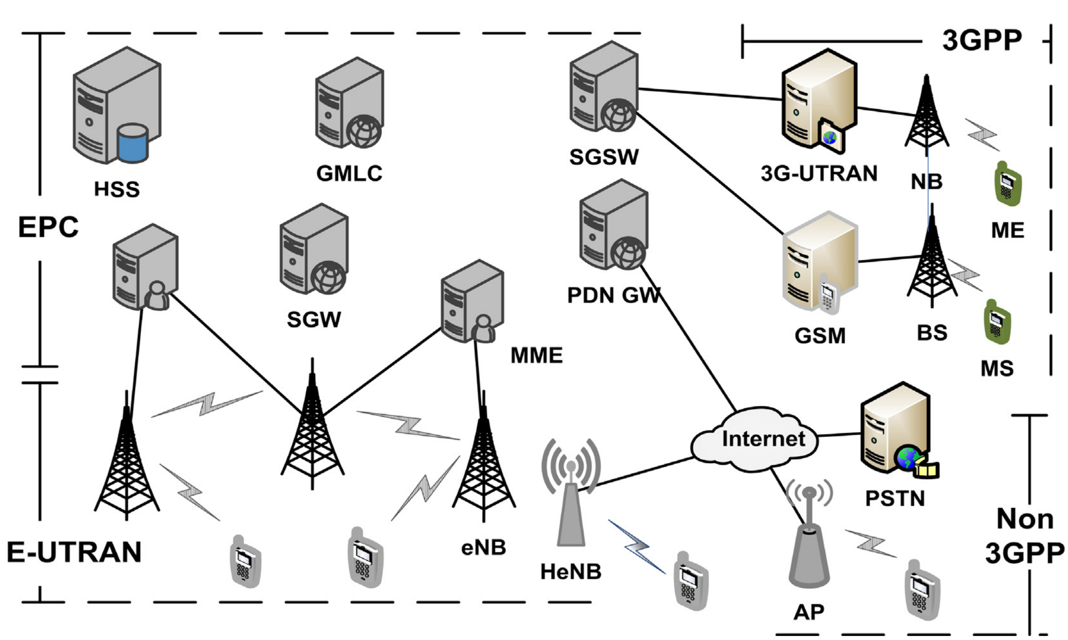

Fig. 1. The network model.

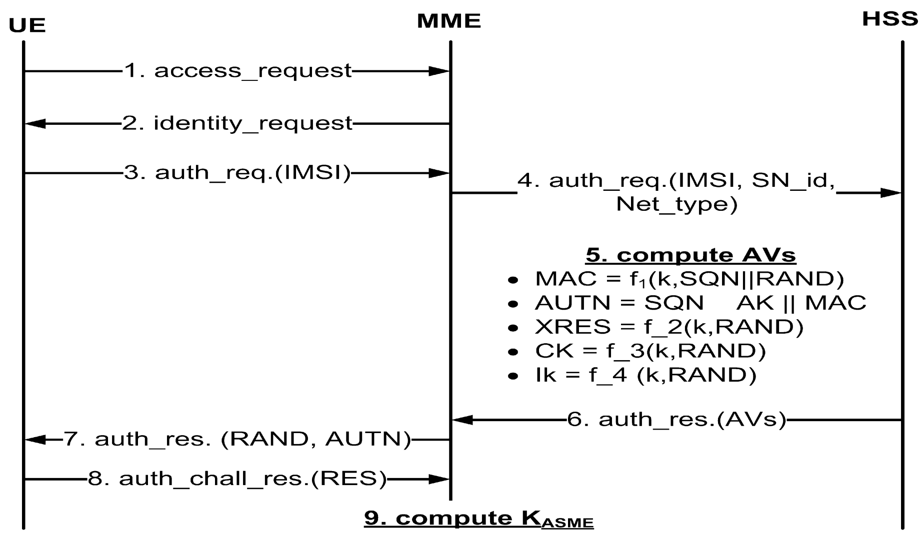

Fig. 2. The EPS-AKA protocol.

7. Upon receipt of authentication vectors, the MME sends random number and authentication challenge piggy-backed on authentication request to the UE, enabling the ME to verify the correctness of sequence number and compute the response.
8. The UE verifies the correctness of the sequence number by computing message authentication code and comparing it with the message authentication code carried in the authentication challenge message. If the two message authentication codes are matched, the UE computes and sends the corresponding response back to the MME in an authentication response message.
9. Once the MME receives and verifies response correctly, it chooses the corresponding K_{ASME} as the session key to protect its communication with the UE. In addition, the UE calculates its K_{ASME} accordingly.

3.2. Adversary and trust model

Andrea et al., in [22], analyze the vulnerabilities of the LTE networks and list number of risks related to the privacy of UE such as identity privacy and user location tracking. Therefore, in this paper, we consider that internal and external attacks may exploit the vulnerabilities of the LTE-A to violate the identity and location privacy of the subscribers as follows:

1. Internal attacks: Attacker, who is a legitimate administrator of the HeNB or AP, may use their legitimacy in a malicious way to exhaust the subscriber's privacy. For example, malicious security authorities could install eNB or AP inside their buildings, in such a way when a guest visits a buildings, the authority owned the base station compels the visiting UE to initiate authentication process by sending signal strength more efficient than the outside eNB. After completing this process, the BSs administrator denies the service for this UE by queuing their IMSI to the black list. This attacker succeeds by employing the UE's identity (IMSI) that is transmitted clearly in the authentication process [23].
2. External attacks: Attackers, who is not a network's entity, could violate the privacy of the LTE-A subscribes by exploiting the Internet and wireless connectivity. We define the following attacks as external attacks:
   (A) *CIMSI* catching attack: the LTE-A authentication process starts with the identification process, which is designed to transmit the *IMSI* in plain text over the communication link, wired or wireless, in the case of no temporary identity is valid [24]. Adversaries can catches the IMSIs from the E-UTRAN or the Internet communications, which are well known insecure links [25] and lunch the replay man in the middle attacks
   (B) Tracking attacks: In the initial attachment procedure, UE uses the IMSI to authenticate itself to the network. In the next mobility procedure, UE uses a temporary identity (TMSI). An adversary can link between the IMSI and TMSI using the location information introduced in the attachment procedure. Therefore, the advertises can reveal the real IMSI and trace the UE [25].

We assume that the evolved packet core is secure and trusted to other network entities, because they are owned and controlled by the operator who is interested in the secure operation of the network. In addition, the HSS, MME and the GMLC are not vulnerable to attacks because they are not accessible to subscribers. However, we do not trust the evolved universal terrestrial radio access network part of the LTE-A network because the HeNBs and APs are owned and operated by the subscriber rather than the service providers and the eNBs are deployed in streets and physically can be accessed to public. We consider the BSs are connected to the evolved packet core via insecure links, which bring new risks to the LTE-A network management, but the links between evolved packet core entities are secure.

4. Preliminaries

This section describes the schnorr zero knowledge protocol since the technical part of the proposed scheme depends on. Schnorr zero-knowledge protocol is a cryptographic authentication technique allows entity to demonstrate knowledge of secret to another entity without revealing any useful information about the secret [26]27. Schnorr zero-knowledge protocols security depends on the difficulty of the discrete logarithm problem and mainly has three security properties as follows:

- Completeness: The verifier will convinced of the fact by the prover if and only if the statement introduced by the prover is true.
- Soundness: If the verifier denies the correctness of the statement introduced by the prover, no cheating prover can convince the verifier otherwise.

- Zero-knowledge: If the statement is true, no cheating verifier learns anything other than this fact.

Fig. 3 describes the schnorr zero knowledge protocol. The protocol has mainly four public parameters p,q,α, and β. p, q are two large prime numbers where $p-1$ is divisible by q. α is the generator of finite field $G(p)$ and $\beta = \alpha^{(p-1)/q}\ mod\ p$. Schnorr zero knowledge protocol is running as follows:

1. Entity A choose two random commitments a, r, where $1 \leqslant a, r \leqslant q-1$, computes $X = \beta^r mod\ p$, and $V = \beta^{-a} mod\ p$. A sends B a witness with X and V.
2. B sends A a challenge e, where $1 \leqslant e \leqslant q-1$
3. A computes response $y = a{\cdot}e + r$ mod q and responds response y to A.
4. B computes $z = \beta^y \cdot V^e mod\ p$ and accepts if $z = X$, rejects otherwise. the prove of correctness is illustrated bellow: $z = \beta^y \cdot V^e mod\ p = \beta^{a\cdot e + r} \cdot \beta^{-a\cdot e} mod\ p = \beta^{a\cdot e} \cdot \beta^r \cdot \beta^{-a\cdot e} mod\ p = \beta^r = X$.

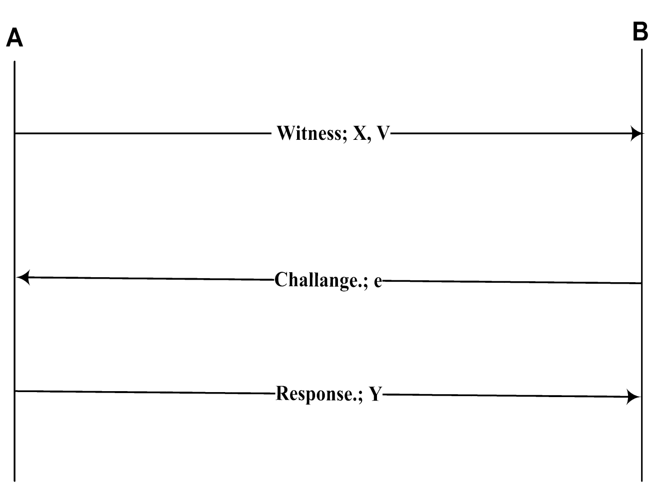

Fig. 3. Schnorr zero knowledge protocol.

5. Proposed schemes

In this section, we describe the proposed schemes as follows:

5.1. P-AKA scheme

In this subsection, the proposed anonymous authentication and location privacy preserving scheme that works based on pseudonyms (P-AKA) is presented.

(A) System Initialization:
HSS bootstraps the system by using a finite field F_q with a large prime number q for initializing a multiplicative cyclic groups of points G over an Elliptic Curve E and g is the generator of G. *HSS* adapts two collision resistant hash functions H and H_1 where $H : \{0,1\}^* \rightarrow F_q$ and $H_1 : \{0,1\}^* \rightarrow G$. *HSS* chooses a random number $\gamma, \gamma_1 \in_R F_q^*, W = g^\gamma, (u, v) = H_1(W, \gamma_1), U = g^u$, and $V = g^v$. Finally, *HSS* considers the $PK_H = \{g, W, U, V\}$ as the public key, and publish G, q, g, PK_H over the network. For each element i in the network (*UE* and *BS*), *HSS* initializes a secret key $ask_i = (A_i, x_i)$, where $x_i \in_R F_q^*$ and $A_i = g^{\frac{1}{\gamma + x_i}}$. For each *UE*, *HSS* computes *IMSI*, *CIMSI*, as $CIMSI = A_i^{x_i u}$. For each *UE* (i) *HSS* initiates a send-record-initiation message to the Gateway Mobile Location Center (GMLC) as $IMSI, CIMSI, LA_i = 0$. *HSS* sends the ask_u, PK_u and $CIMSI_u$ securely to the corresponding UE by encrypting as illustrated in Eq. (1). These parameters using advanced encryption standard algorithm and private key of the HSS, the purpose of AES encryption is to withstand the eavesdropping attacks and the purpose of private key encryption is considered as a signature to ensure integrity and non-repudiation, to the corresponding node and also distributes γ_2 to each Mobility Management Entities ($MME's$).

$$par = E_{ask_{HSS}}[E_{IMSI}[CIMSI||pk_u||ask_u]] \tag{1}$$

(B) Anonymous authentication:
Fig. 4 decries the flows of the pseudo-auth scheme, it is done in six steps as follows:

1. *UE* picks a set of random numbers $r_1, \alpha, r_\alpha, r_x, r_\delta \in_R F_q^*$, q is not secret, it is known to the network, computes $T_1 = U^\alpha, T_2 = A_i^{x_i} V^\alpha, \delta = x_i\alpha, R_1 = U^{r_\alpha}, R_2 = \frac{T_1^{r_x}}{U^{r_\delta}}$, and $c = H(g_1^{r_1}||T_1||T_2||R_1||R_2||LA_i||TS_i)$, where TS_i is a time stamp generated by the UE_i to ensure the freshness of the message. LA_i is the current location of the UE_i. UE_i computes s_α, s_x, s_δ, and the signature σ_i as illustrated in Eqs. (2)–(5), respectively. Finally, as illustrated in Fig. 4, UE_i sends authentication request to the BS_j. (see Fig. 5)

$$s_\alpha = r_\alpha + c\alpha \tag{2}$$

$$s_x = r_x + cx_i \tag{3}$$

$$s_\delta = r_\delta + c\delta \tag{4}$$

$$\sigma_i = E_{ask_i}(g_1^{r_1}||T_1||T_2||R_1||R_2||LA_i||TS_i) \tag{5}$$

2. BS_j checks TS_i to verify the freshness of the message. Stale message are dropped. Then, it computes $\hat{R_1} = \frac{U^{s_\alpha}}{T_1^c}$ and $\hat{R_2} = \frac{T_1^{s_x}}{U^{s_\delta}}$. The proof of correctness is illustrated Eqs. (6) and (7) and BS_j verifies the signature of the UE_i by checking whether $D_{PK_i}(\sigma_i) \stackrel{?}{=} (g_1^{r_1}||T_1||T_2||\hat{R_1}||\hat{R_2}||LA_i||TS_i)$. If the verification is correct, BS_j computes the aggregated signature $\sigma_{ij} = E_{ask_j}(\sigma_i)$. Finally, as illustrated in Fig. 4, BS_j sends authentication request to the MME_k.

$$\begin{aligned}\hat{R_1} &= \frac{U^{s_\alpha}}{T_1^c} \\ &= \frac{U^{r_\alpha + c\alpha}}{U^{\alpha c}} \\ &= \frac{U^{r_\alpha} U^{c\alpha}}{U^{\alpha c}} \\ &= U^{r_\alpha} \\ &= R_1\end{aligned} \tag{6}$$

$$\begin{aligned}\hat{R_2} &= \frac{T_1^{s_x}}{U^{s_\delta}} \\ &= \frac{T_1^{r_x + cx_i}}{U^{r_\delta + c\delta}} \\ &= \frac{T_1^{r_x} T_1^{cx_i}}{U^{r_\delta + c\delta}} \\ &= \frac{T_1^{r_x} U^{\alpha c x_i}}{U^{r_\delta} U^{c\delta}} \\ &= \frac{T_1^{r_x} U^{c\delta}}{U^{r_\delta} U^{c\delta}} \\ &= \frac{T_1^{r_x}}{U^{r_\delta}} \\ &= R_2\end{aligned} \tag{7}$$

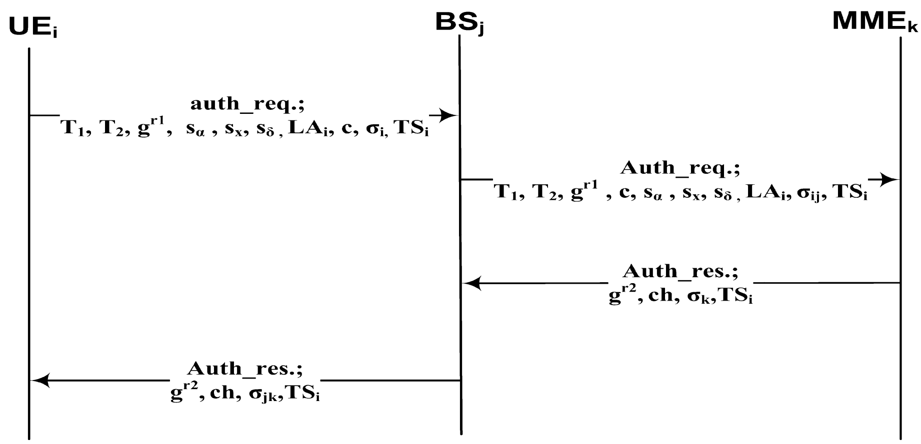

Fig. 4. P-AKA.

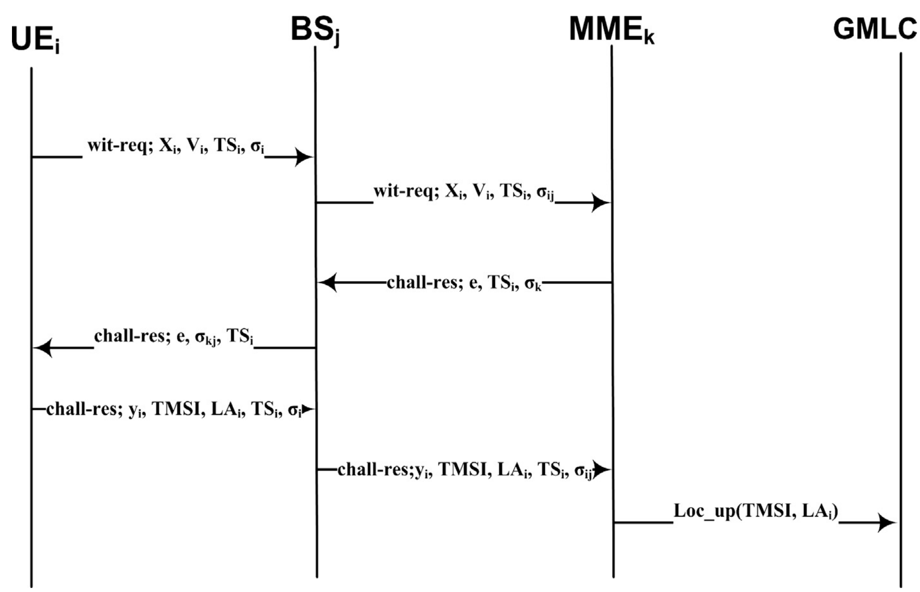

Fig. 5. SZN-AKA scheme.

3. MME_k checks TS_i to verify the freshness of the message. Then, it computes $\hat{R}_1 = \frac{U^{s_\alpha}}{T_1^c}$ and $\hat{R}_2 = \frac{T_1^{s_x}}{U^{s_\delta}}$. MME_k verifies the aggregated signature $D_{PK_j}(D_{PK_i}(\sigma_{ij}) \stackrel{?}{=} (g_1^{r_1}||T_1||T_2||\hat{R}_1||\hat{R}_2||LA_i||TS_i))$. If the verifications are correct, MME_k extract the $CIMSI = \frac{T_2^u}{T_1^v}$, the prove of correctness is illustrated as Eq. (8). MME_j sends location update request to the $GMLC$ as illustrated in Fig. 4.

$$
\begin{aligned}
CMSI &= \frac{T_2^u}{T_1^v} \\
&= \frac{(A_i^{x_i}V^\alpha)^u}{(U^\alpha)^v} \\
&= \frac{(A_i^{x_i}g^{v\alpha})^u}{(g^{u\alpha})^v} \\
&= \frac{A_i^{x_iu}g^{vu\alpha}}{g^{uv\alpha}} \\
&= A_i^{x_iu} \\
&= CIMSI
\end{aligned}
\tag{8}
$$

4. MME_k chooses random number $r_2 \in_R F_p^*$, computes shared key $K_{ASMI} = H(g^{r_1r_2})$, and compute $ch = H(k_{ASMI}, 1)$. MME_k computes $\sigma_k = E_{ask_k}(ch, TS)$ and as illustrated in Fig. 4, MME_k sends authentication response to the BS_j
5. BS_j checks TS to verify the freshness of the message. Then, it verifies the signature of the MME_k as $D_{PK_k}(\sigma_k) \stackrel{?}{=} (ch, TS)$. If the verification is corrects, BS_j compute a aggregated signature $\sigma_{jk} = E_{ask_j}(\sigma_k)$. Finally, as illustrated in Fig. 4, sends a confirmation request to the UE_i
6. UE_i checks TS to verify the freshness of the message. UE_i computes $K_{ASMI} = H(g^{r_1r_2})$, and $ch = H(k_{ASMI}, 1)$. Then, it verifies the aggregated signature of the BS_j and MME_k as $\sigma_j k \stackrel{?}{=} D_{PK_j}(D_{PK_k}(ch, TS))$.If the verification is correct, UE_i ends the procedures, otherwise, UE_i returns the paging procedure.it is correct, UE does not trust the BSs and the wireless medium, therefore, UE should verify the authenticating of the BS by checking the signature. if the verification is not correct mean some problem happened such as attacks or false BS

5.2. SZN-AKA scheme

In this subsection, we will describe the proposed anonymous authentication and location privacy preserving scheme that works based on schnorr zero knowledge proof (SZN-AKA), which is composed of three phases; system initialization, Anonymous authentication, and CIMSI extraction as follows:

(A) System initialization:
HSS, the capital entity in the LTE-A network, bootstraps the system by using S-ZNK protocol with large prime number p such as $p-1$ is divisible by another large prime number q. *HSS* selects random number α as secret key, where $1<\alpha<q$ and computes public key $\beta=p^{\alpha}$ mod q. For each UE, x, HSS selects a random number r and computes $CIMSI_x=p^{r_x}$ mod q. For each node,x, of the network, *HSS* chooses random number ask_x as a private key and computes public key $PK_x = p^{ask_x}$. *HSS* dismiss p,q,β to all network entities and transmit r to the corresponding *UE* in a secret manner, also *HSS* sends α to the *GMLC*. HSS sends the ask_x, PK_x and $CIMSI_x$ securely to the corresponding node by encrypting these parameters using the advanced encryption standard algorithm (AES) and private key of the HSS, the purpose of AES encryption is to withstand the eavesdropping attacks and the purpose of private key encryption is considered as a signature to ensure integrity and non-repudiation as as illustrated in Eq. (9) to the corresponding node. Finally, each node in the network dismiss its public key to network and keeps the private key secure.

$$par=E_{ask_{HSS}}[E_{IMSI}[CIMSI_x||pk_x||ask_x]] \tag{9}$$

(B) Anonymous authentication:

1. UE_i selects δ_i,ω_i and TS_i as two random numbers less than q and time stamp, respectively. UE_i computes X_i and V_i as illustrated in Eqs. (10) and (11), respectively. UE_i sign the message by signature σ_i as described in Eq. (12). UE_i sends a witness request; $wit-req;(X_i,V_i,TS_i,\sigma_i)$, to the corresponding the BS_j.

$$X_i=\beta^{\omega_i} modp \tag{10}$$

$$V_i=\beta^{-\delta_i} modp \tag{11}$$

$$\sigma_i=E_{ask_i}(X_i,V_i,TS_i) \tag{12}$$

2. Once BS_j receive the message, it verifies the signature of the UE_i as $D_{PK_i}(\sigma_i)$?= X_i,V_i,TS_i. if the verification is correct, BS_j computes the aggregated signature σ_{ij}= $E_{ask_j}(\sigma_i)$. BS_j sends a witness request; $wit-req(X_i,V_i,TS_i,\sigma_{ij})$ to the MME_k.
3. Once MME_k receives the message, it verifies the correctness of the aggregated signature $D_{PK_j}(D_{PK_i}(\sigma_{ij}))$?= X_i,V_i,TS_i. if the verification is correct, MME_k selects challenge $e, 1<e<q$, computes $\sigma_k=E_{ask_k}(e,TS_i)$, and sends challenge request; $chall-res(e,TS_i,\sigma_k)$ to the BS_j.
4. BS_j verifies the correctness of MME_k signature $D_{PK_j}(\sigma_k)=e,TS_i$. if the correctness is satisfied, BS_j computes the aggregated signature $\sigma_{kj}=E_{ask_j}(\sigma_k)$ and sends challenge request message $chall-res(e,TS_i,\sigma_{kj})$ to the UE_i
5. Once UE_i receives the challenge request, it checks the aggregated signature as $D_{PK_j}(D_{PK_k}(\sigma_{kj}))=e,TS_i$. If the verification is correct, UE_i computes challenge y_i , the temporary *IMSI TMSI*, and sign by the signature σ_i as described in Eqs. (13)–(15), respectively. Finally UE_i sends a challenge response; $chall-res(y_i,TMSI,LA_i,TS_i,\sigma_i)$ to the BS_j.

$$y_i=(\delta_i e+\omega_i)modp \tag{13}$$

$$TMSI=\beta^{r+y_i} \tag{14}$$

$$\sigma_i=E_{ask_i}(y_i,TMSI,LA_i,TS_i) \tag{15}$$

6. BS_j checks the signature σ_i as $D_{PK_i}(\sigma_i)=y_i,TMSI,LA_i,TS_i$. If the verification is satisfied. BS_j aggregates the signature $\sigma_{ij}=E_{ask_j}(\sigma_i)$, and sends challenge response $chall-res;(y_{ij},y_i,TMSI,LA_i,TS_i,\sigma_i j)$ to MME_k.
7. MEE_k verifies the aggregated signature σ_{ij} as $D_{PK_j}(D_{PK_i}(\sigma_{ij}))=y_i,TMSI,LA_i,TS_i$. if the verification is correct, MME_k checks the correctness of challenge y_i as $X_i=\beta^{y_i}V_i^e$, the proof of correctness is illustrated bellow in Eq. (16) if y_i is true then MME_k sends location update request $Loc_u p;TMSI,LA_i$ to the *GMLC*.

$$\begin{aligned} X_i &= \beta^{y_i}V_i^e \\ &= \beta^{\delta_i e+\omega_i}\beta^{-\delta_i e} \\ &= \beta^{\delta_i e}\beta^{\omega_i}\beta^{-\delta_i e} \\ &= \beta^{\omega_i} \\ &= X_i \end{aligned} \tag{16}$$

(C) CIMSI extraction:
Once the *GMLC* receives the location update request from the MME_k, it extract the real *IMSI* of the UE_i as $CIMSI=(TMSIX_i^{-1}V_i^e)^{-\alpha}$. The prove of correctness is illustrated in Eq. (17).

$$\begin{aligned} CIMSI &= (TMSIX_i^{-1}V_i^e)^{-\alpha} \\ &= (\beta^{r+y_i}X_i^{-1}V_i^e)^{-\alpha} \\ &= (\beta^r\beta^{y_i}X_i^{-1}V_i^e)^{-\alpha} \\ &= (\beta^r\beta^{\delta e\omega}X_i^{-1}V_i^e)^{-\alpha} \\ &= (P^{r\alpha}\beta^{\delta\omega e}\beta^{-\omega}\beta^{-\delta e})^{-\alpha} \\ &= CIMSI \end{aligned} \tag{17}$$

6. Security and privacy evaluations

This section describes the security and privacy evaluation of our proposed schemes. In order to prove that, we want to analyze the possibility of attacks for violating the communication security and revealing the location privacy of the UE.

6.1. Communication security

Both of pseudo-auth and SZN-auth schemes achieve the communication security requirements by using two aspects; time stamps (TS) and signature. Each message of the proposed schemes is attached with *TS* in order to deny any internal or external of reusing the message. *TS* consists of the date and the time of the message initiation as $mm/dd/yyyHH:MM:SS$.

Signature is the process that allows a network entity to sign message and any other entity can verify this messages with completely ascertainably that this signature never be made by entities except the legal one.

Our schemes withstand these types of attack by signature as; when the attacks catches the messages, he tries to take one of the two possibility. In one hand, attacker attempts to change one of the message content without changing signature. Therefore, the other side fails to verify the signature as the variety of the transmitted variable and the computed variables causing message rejection. on the other hand, attacker tries to extract the private key of the network node to sign the new message. To reveal the private key, attacker has to try an exhaustive search with at least half of the key size. Based on [28], if $n/2 \geqslant 80$, where n is the size of secret key, then it is infeasible to break the security of the system. Therefore, we can say that our schemes withstands the exhaustive and birthday attacks. Table 2 describes a security comparison between the proposed scheme and the others.

In $P-AKA$ scheme, let us consider the first message of the our scheme, auth-req; $auth-req.; T_1, T_2, g^{r_1}, s_\alpha, s_x, s_\delta, LA_i, c, \sigma_i, TS_i$. Insecure wireless, Internet connectivity, and the heterogenous Network compatibility suffer different sort of attacks such as man in the middle,and modification attacks. These attacks attempt to make undesirable actions on the transmitted packet as content modification. Therefore, Attack tries to extract the private key ask_i of the UE_i to sign the new message. To reveal the ask_i, attacker has to get the x_i and computes A_i. x_i is a random number belong the finite filed ($x_i \in_R F_p^*$). p is a large prime number with length 160$bits$, therefore, To get x_i, attacker have to tries an exhaustive search with at least half of the number of the $F_p^*; 2^{159}$ rounds. 2^{159} rounds is a big probability and infeasible to perform. $A_i = g^{\frac{1}{\gamma+x_i}}$, Also it is infeasible to compute A_i even if attacker gets the x_i because of the difficulty of the discrete time logarithm problem. In addition, birthday paradox attack needs $2^{\frac{n}{2}} = 2^{\frac{160}{2}} = 2^{80}$ to link pseudonymes.

In SZN-auth scheme, challenge, y_i, is the third level of security that our scheme achieved. y_i is computed based on e, ω, and δ, and challenge e has been sent securely from MME_k using the signature. ω and δ are two random number that are not been sent before.

6.2. Location privacy preservation

Location privacy is defined as the ability to prevent attackers form deducing a user's location [29]. In both proposed schemes, $P-AKA$ and $SZN-AKA$ Scheme, attacker has no capability to deduce the UE_i since the IMSI of the UE_i is not transmitted over transmission media. Also, attackers has no capability to corrupt the transmitted message by modifying the UE_i location, LA_i, since it is included in the assigned message, which is secured by the signature. Therefore, we do not need to hide LA_i since the transmission of the LA_i is meaningless.

Likability is the process of revealing the CIMSI by links a two transmitted messages. In pseudo-auth scheme, attacker has no capability to reveal the IMSI using the likability properties, since a new T_1 and T_2 are used based on a new pseudonymes numbers as $r_1, \alpha, r_\alpha, r_x, r_\delta \in_R F_p$, computes $T_1 = U^\alpha, T_2 = A_i^{x_i} V^\alpha, \delta = x_i\alpha$, $R_1 = U^{r_\alpha}$, $R_2 = \frac{T_1^{r_x}}{U^{r_\delta}}$. Therefore, we do not need to hide LA_i since the transmission of the LA_i is meaningless since the attacker has no capability to link between the LA_i and the identity of the UE_i. In $SZN-AKA$ Scheme, attacker has no capability to reveal the $CIMSI$ using the likability properties, since a new $TMSI$ is generated based on a new pseudonymes numbers as δ and ω.

7. Performance evaluation

In this section, we analysis the performance of the proposed scheme by comparing it with the other schemes.

Table 2
Comparison of communication overhead.

Attacks	Exhaustive	Birthday
EPS AKA	Null	Null
W-AKA	2^{255}	2^{128}
HSK-AKA	2^{127}	2^{64}
P-AKA	2^{159}	2^{80}
SZN-auth	2^{159}	2^{80}

7.1. Communication overhead

For communication overhead, as illustrated in Table 3, the proposed schemes, $P-AKA$ and SZN-auth, achieve the authentication and key agreement protocol by number of messages, 4 and 7 respectively, while the $EPC-AKA, W-AKA$ and $HSK-AKA$ schemes perform the purpose by 9, 5, and 6 messages respectively. By the other hand, the size of the messages of the proposed schemes, $P-AKA$ and SZN-auth, are 4480 bits and 395 bits respectively, while the $EPC-AKA, W-AKA$ and $HSK-AKA$ schemes consume 3072 bits, 2245 bits, and 2016 bits respectively. However, the proposed schemes achieve a security level higher than the other schemes. Moreover, unlike the other schemes, the proposed schemes does not require the HSS evolving in the authentication and location update procedures, Therefore, the proposed schemes decrease the overhead on the core network since it does not need to arrive HSS.

7.2. Computation overhead

According to the security cryptographic namespace coded in visual studio.Net 2012, compiled with Microsoft Visual Basic.Net 2012, and run in a device with Intel(R) Core(TM) i7-4510U CPU@2.00 GHz 2.60 GHz, 16 GB RAM and 46-bit operating system x64-based processor, the computation overhead of the cryptographic algorithm being used in our scheme are computed as the following: single MD5 and SHA256 hash functions consume 4 and 5 ms, respectively to hash 5 bytes, AES and ECC consumes 20 and 1 ms to encrypt 5 bytes, the single modulus operation consumes 0.005 ms to consumes to relocate a large number to the finite field and finally, any MILENAGE cryptographic algorithms, the cryptographic algorithms being use in LTE-A network to generate the security parameters [30], consumes 36 ms to generate LTE-A security parameter such as integrity key, response, and confidentiality key.

As illustrated in Fig. 6, the proposed schemes consume a computation overhead less than those consumed in the $EPC-AKA, W-AKA$ and $HSK-AKA$ since the proposed schemes depend on low computation cryptographic tools such as MD5 hash function, ECC encryption, and modulus operation, while the $EPC-AKA, W-AKA$ and $HSK-AKA$ schemes depend on the MILENAGE cryptographic algorithms and SHA256 hash function. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form. Despite the $EPC-AKA$ transmits the IMSI in clear text, it consumes a computation time in computing the security parameters such as AVs. Each registration process, the authentication and authorization and accounting server computes five authentication vectors (AVs) for the MME and UE computes at least one AV. The computing of these AVs is done based on a special purpose cryptographical functions which use advanced encryption standard as the kernel function [30].

Consider MD5 hash function, SHA256, AES encryption, ECC encryption, cryptographic function and modulus operation consume $\Psi, \Omega, \xi, \Upsilon, \mu$ and Δ computation time. Table 4 describe the time required for each network node such as UE, eNB, MME and HSS to execute the authentication protocol.

Table 3
Comparison of communication overhead.

Scheme	Number of messages	Total packets sizes (bits)
EPS AKA	9	3072
W-AKA	5	2245
HSK-AKA	6	2016
P-AKA	4	4480
SZN-AKA	7	395

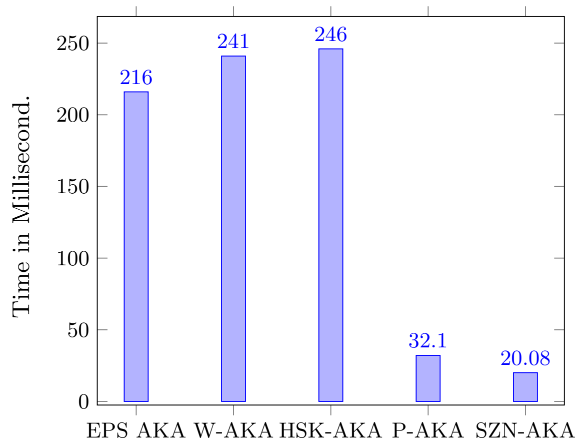

Fig. 6. Computation overhead.

Table 5
Simulation parameters.

Parameter	Value
Number of UEs	1–100
Number of eNBs	One
Number of MMEs	One
Rate of attacks	20%
Physical Network	LTE-A
Average network Ratio Delay	One second
Processor	Intel(R) Core(TM) i7-4510U
CPU Speed	2.60 GHz
RAM Size	16 GB
Operating System	Windows 46-bit x64-based processor

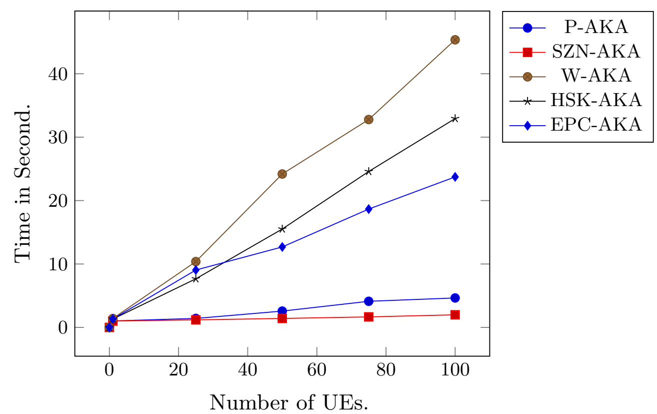

Fig. 7. Total network delay.

8. Experimental results

In this section, we describe the experimental results of the proposed schemes. By using the security cryptographic namespace, we use the visual studio.Net to develop a network simulation platform running in a device with Intel(R) Core(TM) i7-4510U CPU@2.00 GHz 2.60 GHz, 16 GB RAM and 46-bit operating system x64-based processor. The experimental results that we had measured focuss on the total routing delay and the individual network nodes include UE and HSS. We consider number of UEs attached to the network as 1, 25, 50, 75 and 100 in the presence of 20% of attacks and number of eNBs and MMEs as only one in the network. Based on [31], we consider the LTE-A average network ratio delay of the authentication protocol is one second, the physical network is the LTE-A network. Table 5 shows our simulation parameters. Our experimental results are presented as the following:

8.1. Total network authentication delay

The total network authentication delay is defined as the overall time required to execute the authentication protocol all over a network. Fig. 7 illustrates the total delay (in second) for different number of UEs. It is clear in the figure that our schemes, $P-AKA$ and $SZN-AKA$, attain better delay computation overheads than those of other schemes. On one hand, Our $P-AKA$ protocol requires the execution of twenty modulus operations, six MD5 hash function and and eight ECC public key encryption for signature. Additionally, our $SZN-AKA$ protocol requires to execute fifteen modulus operation, three MD5 hash function and eight ECC public key encryption for signature. On the other hand, the $EPC-AKA$ requires at least six MILENAGE cryptographic functions, $W-AKA$ requires two MILENAGE cryptographic functions and five SHA256 hash function and $HSK-AKA$ requires six MILENAGE cryptographic functions and six SHA256 hash functions. As illustrated in subSection 7.2, MILENAGE cryptographic function consumes long time to execute multiple advanced encryption standard algorithm. Similarly, SHA256 hash function also consumes long time.

Moreover, in our network model, we consider 20% of the UEs as attacks, therefore, our schemes are capable to settle these attacks in the first verification check on the eNB by signatures and time stamps, and hence decrease the routing time. However, other schemes allow these attackers to consume more routing delay for instance the $EPC-AKA$ consumes a time of five MILENAGE cryptographic function before the HSS deny the attack, also the $W-AKA$ and $HSK-AKA$ consume a time of five SHA256 functions and three MILENAGE cryptographic functions before HSS deny the attack. As a matter of fact, with the increasing number of devices that need to execute the authentication protocol, the $EPC-AKA, W-AKA$, and $HSK-AKA$ may bring a big computation overhead risk to the LTE-A network.

In conclusion of this experiment, the simulation results demonstrate that our schemes, $P-AKA$ and $SZN-AKA$, enhance the total network authentication delay compared to those of other schemes, $EPC-AKA, W-AKA$, and $HSK-AKA$, as the following: first, $P-AKA$ enhances the total network authentication delay by 85.809%, 85.89%, and 89.75% compared to $EPC-AKA, W-AKA$, and $HSK-AKA$ schemes, respectively. Second, $SZN-AKA$ enhances

Table 4
Comparison of computation time in each node.

Scheme	UE	eNB	MME	HSS
P-AKA	$2\Psi + 2\Upsilon + 7\Delta$	$1\Psi + 2\Upsilon + 5\Delta$	$2\Psi + 2\Upsilon + 4\Delta$	$1\Psi + 2\Upsilon + 4\Delta$
SZN-AKA	$1\Psi + 2\Upsilon + 4\Delta$	$1\Psi + 2\Upsilon + 4\Delta$	$1\Psi + 2\Upsilon + 4\Delta$	$2\Upsilon + 4\Delta$
EPS AKA	1μ	0	0	5μ
W-AKA	$2\Omega + 2\mu$	0	0	$3\Omega + 3\mu$
HSK-AKA	$3\Omega + 2\mu$	0	0	$3\Omega + 3\mu$

Ψ: MD5 hash function, Ω: SHA256 hash function, ξ: AES encryption,
Υ: ECC encryption, μ: cryptographic function and Δ: modulus operation.

the total network authentication delay by 93.97%, 93.97%, and 95.61% compared to $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, respectively.

8.2. Node routing delay

In this subsection, we compute the authentication overhead of each node at the network include UE and HSS as follow:

UE Delay: According to our scenario, when UE roams to a network that 20% of their entities are seam to attacks, the UE should make a complex computation to authenticate itself to other entity and should verify the other entity correctly. Fig. 8 illustrates that our schemes introduce less UE side authentication delay than that introduced in the $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, In our schemes, $P-AKA$ and $SZN-AKA$, each message that are routed via the network should signed by the sender and equipped with time stamps. Therefore, UE could verify the correctness of the message before running heavy computation, and hence fake messages are settled. As a matter of fact, with the increasing number of messages that need to execute the authentication protocol in the UE side, the $EPC-AKA$, $W-AKA$, and $HSK-AKA$ can not verify the correctness of the message early, and hence may bring a big overflow risk to the UE device.

In conclusion of this experiment, the simulation results demonstrate that our schemes, $P-AKA$ and $SZN-AKA$, enhance the authentication delay at the UE side compared to those of other schemes, $EPC-AKA$, $W-AKA$, and $HSK-AKA$, as the following: first, $P-AKA$ enhances the authentication delay at the UE side by 95.22%, 92.16%, and 92.16% compared to $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, respectively. Second, $SZN-AKA$ enhances the total network authentication delay by 95.22%, 92.16%, and 92.16% compared to $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, respectively.

HSS Delay According to our scenario, our schemes, $P-AKA$ and $SZN-AKA$, require HSS to only prepare the overall system at the registration stage, therefore, HSS does not require to involve each authentication protocol. the original LTE-A authentication protocol, $EPS-AKA$, requires HSS to compute five MILENAGE cryptographic functions. $W-AKA$ and $HSK-AKA$ schemes require HSS to compute three MILENAGE cryptographic functions and three SHA256 hash functions. Therefore, as illustrated in Fig. 9, our schemes, $P-AKA$ and $SZN-AKA$, introduce better HSS authentication delay than that introduced in the $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes.

In conclusion of this experiment, the simulation results demonstrate that our schemes, $P-AKA$ and $SZN-AKA$, enhance the authentication delay at the HSS side compared to those of other schemes, $EPC-AKA$, $W-AKA$, and $HSK-AKA$, as the following: first, $P-AKA$ enhances the authentication delay at the HSS side by 93.68%, 89.68%, and 89.7% compared to $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, respectively. Second, $SZN-AKA$ enhances the total network authentication delay by 93.07%, 89.69%, and 89.69% compared to $EPC-AKA$, $W-AKA$, and $HSK-AKA$ schemes, respectively.

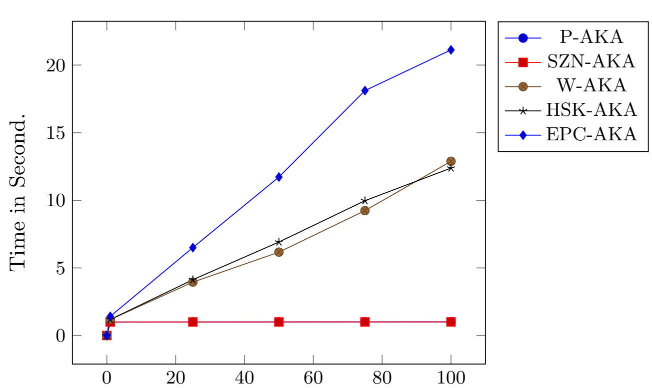

Fig. 8. Routing delay at UE.

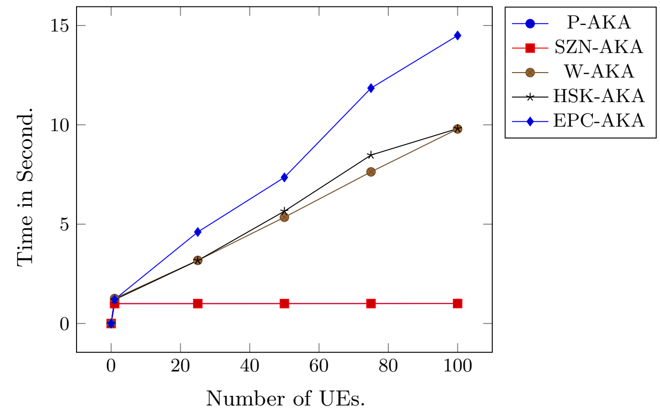

Fig. 9. Routing delay at HSS.

9. conclusion and future works

In this paper, we introduce entailing two Anonymous authentication and location privacy preserving scheme for LTE-A network. In the first scheme, $P-AKA$, we use pseudonymes based public key cryptography to perform the authentication procedure because the finite field used in the public key cryptography has a prime number big enough to be secure, also the public key cryptography has a difficulties hard enough to withstands attacks such as the discrete time logarithm which we use in this scheme.

In the second scheme, $SZN-AKA$, we study enabling Anonymous authentication and location privacy preserving scheme for LTE-A network using aggregated schnorr zero knowledge protocol and the public key cryptography to perform the authentication and location update procedure.

Our schemes can eliminate the overhead of core network since the authentication procedure does not need to arrive to the HSS each time. Extensive evaluations demonstrate that our proposals are preserve the privacy of the location of the UE and require low communication and computational overhead.

The experimental results demonstrates that our schemes element the total time delay required to execute the authentication protocols comparing with the other schemes by 90.84%. Also, the exterminate result demonstrates that our scheme decreases the time of authentication protocol by decreasing the computation especially on the UE side by 93.18%, which battery consumption is a critical factor related to operation being execute. In addition, the experimental result demonstrate that our schemes decreases the computation required to execute in the core network node by 90.92%, since it does not need to meet the HSS, therefore our schemes eliminate the possibility of HSS overflow problem.

At the end, as a future work, we can recognize this scheme to achieve secure and seamless handover. Moreover, we can recognize the anonymous authentication scheme for the fifth generation network.

References

[1] Olsson Magnus, Sultana Shabnam, Rommer Stefan. Lars Frid and Catherine Mulligan. EPC and 4G Packet Networks: Driving the Mobile Broadband Revolution. United States: Elsevier; 2013.

[2] Nagata Satoshi, Campoy Luis, Berberana Ignacio, Derham Thomas, Liu Guangyi, Shen Xiaodong, Zong Pingping, Yang Jin. LTE-advanced: an operator perspective. IEEE Commun Mag 2012;50(2):104–14.

[3] Haddad Zaher, Mahmoud Mohammed, Saroit Imane Aly, Taha Sanaa. Secure and efficient uniform handover scheme for LTE-A networks. In: IEEE communications and networking conference (WCNC 2016), Qater, April. p. 1202–7.

[4] 3GPP. Technical specification group services and system aspects: general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access (Rel-11), vol. 10.4.0, no. 23.401; June 2011. <http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/11.03.00_60/ts_123401v110300p.pdf>.

[5] Park Yongsuk, Park Taejoon. A survey of security threats on 4G networks. In: IEEE globecom workshops, USA. p. 1–6. Nov.

[6] Jagwani Priti, Kaushik Saroj. Defending location privacy using zero knowledge proof concept in location based services. In: 2012 IEEE 13th international conference on mobile data management, India, July. p. 368–71.

[7] Brassil Jack, Pearson Chris, Fuller Lee. Indoor positioning with an enterprise radio access network. Proc Comput Sci 2014;34(1):313–22.

[8] Klaus Rechert, Konrad Meier, Benjamin Greschbach, Dennis Wehrle, Dirk Suchodoletz. Assessing location privacy in mobile communication networks. In: 14th International conference on information security, China. p. 309–24.

[9] Abdo Jacques Bou, Demerjian Jacques, Ahmad Kassem, Chaouchi Hakima, Pujolle Guy. EPS mutual authentication and crypt-analyzing (SPAKA). In: 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Vietnam, Jan. p. 303–8.

[10] Taha Sanaa, Shen Xuemin. Anonymous home binding update scheme for mobile IPv6 wireless networking. In: IEEE global telecommunications conference (GLOBECOM 2011), USA, Dec. p. 1–5.

[11] So-In Chakchai, Jain Raj, Paul Subharthi, Pan Jianli. Virtual ID: a technique for mobility, multi-homing, and location privacy in next generation wireless networks; Jan 2010. p. 1–5.

[12] Ta Tuanand, Baras John S. Enhancing privacy in LTE paging system using physical layer identification. Data Privacy Manage Autonom Spont Security 2013;7731(1):15–28.

[13] Hamandi Khodor, Sarji Imad, Elhajj Imad H, Chehab Ali, Kayssi Ayman. W-AKA: privacy-enhanced LTE-AKA using secured channel over Wi-Fi. In: IEEE international conferance on wireless telecommunications symposium (WTS), Chaina, April. p. 1–6.

[14] Koien Geir. Privacy enhanced mutual authentication in LTE. In: IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), France, Oct. p. 614–21.

[15] Jo Hyo Jin, Paik Jung Ha, Lee Dong Hoon. Efficient privacy-preserving authentication in wireless mobile networks. IEEE Trans Mobile Comput 2014;13(7):1469–81.

[16] Hamandi Khodor, Sarji Imad, Chehab Ali, Elhajj Imad H, Kayssi Ayman. Privacy enhanced and computationally efficient HSK-AKA LTE scheme. In: IEEE 27th international conference on advanced information networking and applications workshops (WAINA), Spain, March. p. 929–34.

[17] Choudhury Hiten, Roychoudhury Basav, Saikia Dilip. Enhancing user identity privacy in LTE. In: IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom), UK, June. p. 949–57.

[18] Purkhiabani Masoumeh, Salahi Ahmad. Enhanced authentication and key agreement procedure of next generation evolved mobile networks. In: IEEE 3rd international conference on communication software and networks (ICCSN), Chaina, May. p. 557–63.

[19] Cox Christopher. An introduction to LTE: LTE, LTE-advanced, SAE, VoLTE and 4GMobile communication, Chirs Cox Communication Ltd, UK, Ed.. John Wiley and sons Ltd; 2014.

[20] Laia Chengzhe, Lia Hui, Luc Rongxing, (Sherman) Shen Xuemin. SE-AKA: a secure and efficient group authentication and key agreement protocol for {LTE} networks. Comput Netw 2013;57(17):3492–510.

[21] Cao Jin, Ma Maode, Li Hui, Zhang Yueyu, Luo Zhenxing. A survey on security aspects for LTE and LTE-A networks. IEEE Commun Surveys Tutor 2014;16(1):283–302. Jan.

[22] Andreu Gin'es Escudero, Raphael Phan, Parish David. Analysis and design of security for next generation 4G cellular networks. In: Proceedings of the 13th annual post graduate symposium on the convergence of telecommuni-cations, networking and broad-casting (PGNET), UK, June. p. 25–8.

[23] Tallapally Shirisha. Imporsonation attack on EKE protocol. Int J Netw Security Its Appl (IJNSA) 2010;2(2):114–21. April.

[24] 3GPP. Generic authentication architecture (GAA); generic bootstrapping architecture (GBA) (Release 11), vol. 11.2.0, no. 33.220; March 2012. <http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/11.03.00_60/ts_123401v110300p.pdf>.

[25] Tawil Rami, Demerjian Jacques, Pujolle Guy. A trusted handoff decision scheme for the next generation wireless networks. Int J Comput Sci Netw Security, IJCSNS 2008;8(6):174–82. Jun.

[26] Jawurek Marek, Kerschbaum Florian, Orlandi Claudio. Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently. In: Proceedings of the 38 ACM SIGSAC conference on computer communications security, Germany, Jan. p. 955–66.

[27] Martín-Fernández Francisco, Caballero-Gil Pino, Caballero-Gil Cándido. Authentication based on non-interactive zero-knowledge proofs for the internet of things. Sensors Mag 2016;16(1):75.

[28] Su Shenghui, Xie Tao, Lv Shuwang. A new non-MDS hash function resisting birthday attack and meet-in-the-middle attack. CoRR Magazine, vol. abs/1408.5999; Augst 2014. <https://arxiv.org/ftp/arxiv/papers/1408/1408.5999.pdf>.

[29] Mahmoud Mohamed, Taha Sanaa, Misic Jelena, Shen Xuemin. Lightweight privacy-preserving and secure communication protocol for hybrid ad hoc wireless networks. IEEE Trans Parallel Distrib Syst 2014;25(8):2077–90. Aug.

[30] 3GPP. Technical specification: unversal mobile telecommunications system (UMTS); LTE; 3G security; specification of MILENAGE algorithm set: an example algorithm set for 3GPP authentication and key generation functions f1, f2,f3,f4, f5 and f5∗; document 1: general (Rel-13), vol. 13.0.0, no. 35.205; Jan 2016. <http://www.etsi.org/deliver/etsi_ts/135200_135299/135205/13.00.00_60/ts_135205v130000p.pdf>.

[31] Nokia. Future work: technology vision 2020 reducing network latency to milliseconds, no. C401-011916-WP-201508-1-EN; Dec 2015. <http://www.google.com.eg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi2kpnN0ujMAhXGMhoKHbO5CXkQFggaMAA>.