Wireless Personal Communications (2018) 103:2317–2352
https://doi.org/10.1007/s11277-018-5912-1

A Proxy Signature Based Efficient and Robust Handover AKA Protocol for LTE/LTE-A Networks

Shubham Gupta[1] · **Balu L. Parne**[1] · **Narendra S. Chaudhari**[1,2]

Published online: 30 July 2018

Abstract
An efficient and robust handover is one of the essential requirements of several applications in LTE/LTE-A network. These applications are reliable only after a successful authentication of communication entities. Hence, the third generation partnership project has recommended the handover schemes for different mobility scenarios with a new key management approach that increases the complexity of the overall system. To overcome the above problems, researchers have proposed various handover authentication protocols. But, most of the handover protocols can't avoid the key escrow problem and suffers from key forward/backward secrecy. Also, these protocols are vulnerable to various malicious attacks and incur high computational overhead during the authentication process. Therefore, these protocols don't suit for handover authentication in LTE/LTE-A networks. However, researchers have proposed the proxy signature based handover protocols but, these protocols fail to achieve an adequate solution for proxy revocation and necessary security demands. In order to mitigate the aforesaid problems, we propose a proxy signature based efficient and robust handover authentication and key agreement protocol with revocation in LTE/LTE-A network. To prove the correctness of the proposed protocol, the formal analysis is carried out by BAN logic and simulated using the AVISPA tool. Moreover, the security analysis illustrates that the proposed protocol fulfills all the security features and avoids the identified attacks. Finally, the performance analysis of the proposed protocol is shown with existing handover protocols. The analysis shows that the protocol has improved results in terms of transmission, storage, message and computation overhead.

Keywords LTE/LTE-A network · Handover authentication · Proxy signature · Revocation · AVISPA

✉ Shubham Gupta
shubham.gupta@students.vnit.ac.in

Balu L. Parne
balu.parne@students.vnit.ac.in

Narendra S. Chaudhari
nsc0183@yahoo.com

[1] Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India

[2] Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Indore, Madhya Pradesh (M.P.), India

1 Introduction

From recent few years, there are various forthcoming wireless network technologies such as Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution-Advanced (LTE-A) are evolving to accomplish the increasing demands of various mobile services for higher data rates [1, 2]. In order to provide a strong support for the evolution of the mobile devices/ wireless equipments, LTE/LTE-A technology achieves lower access latency and flexible bandwidth compared to all other wireless communication technologies [3, 4]. Due to the mobility of wireless equipments in the LTE/LTE-A network, there are various handover applications such as mobile multimedia service, tracking and tracing system, etc. To achieve the security in various applications, it is essential to execute the efficient and secure handover authentication protocol in the communication network [5, 6].

The architecture of LTE/LTE-A network is proposed by the Third generation partnership project (3GPP) committee to acquire the aforementioned security demands. The architecture consists of Evolved Universal Terrestrial Access Networks (EUTRAN) and Evolved Packet Core (EPC) as shown in the Fig. 1 [7]. In EUTRAN, various base stations (eNBs) connect with user equipments/mobile nodes (UE/MN). The 3GPP has recommended a new base station HeNB (Home eNB) to improve the indoor coverage for uninterrupted data services. Furthermore, EPC consists the Packet Data Network Gateway (PDN-GW), Serving Gateway (S-GW) and Memory Management Entity (MME) that communicates with the HSS. Mainly, EPC maintains the overall control on the UE and establishes the communication bearers [8–10]. Moreover, the MME establishes the signaling between the UE and the core network. The HSS consists of the UEs subscription data and maintains the information of PDNs. Whenever UE associates with EPC through EUTRAN, MME communicates to the HSS to obtain the respective authentication parameters to achieve mutual authentication with the UE. In EUTRAN, each eNB/HeNB communicates with another eNB/HeNB with X2 interface and with MMEs via S1 interface. There are three approaches by which HeNB can communicate in the network such as:

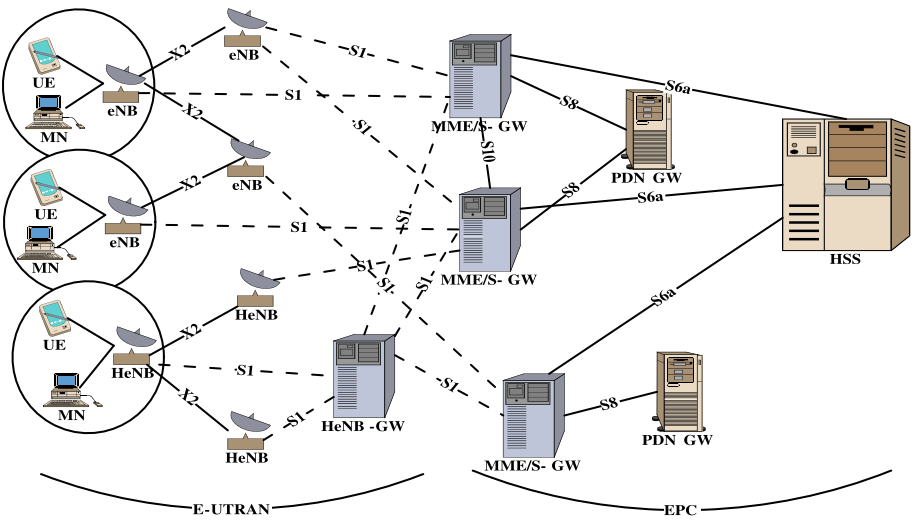

Fig. 1 The network architecture of LTE/LTE-A

(1) Closed Subscriber Group (CSG) approach (UE's present in CSG list); (2) Hybrid approach i.e each valid UE can communicate with HeNB but, those HeNBs in CSG list have the higher preference and (3) Open mode approach (same as eNB) [11].

The EUTRAN can setup a HeNB Gateway (HeNB-GW) to establish the S1 interface between the EPC and HeNB. Hence, the HeNB can communicate to the EPC via the S1 interface without any assistance of HeNB-GW. In the LTE/LTE-A architecture, the HenB and enB can't communicate directly to each other. Therefore, eNB needs to perform with MME to communicate the HeNB. Primarily, 3GPP has recommended four handover scenarios in the LTE/LTE-A network [8, 9]: LTE X2 based handover, S1 based intra/inter-MME handover and S1 based hybrid/CSG HeNB handover. In addition, two handover scenarios can be considered in LTE X2 based handover: (1) between eNBs and; (2) between a HeNB and open mode HeNB. In these handovers, it does not require to contact with the MME. In S1-based intra MME handover, same MME manages both the target and source base stations. Whenever, UE communicates to a CSG/hybrid HeNB, S1-based hybrid/CSG HeNB handover is operated. In addition, S1 based inter-MME handover is executed in the network when different MMEs manage the different eNBs [12].

The 3GPP has illustrated and analyzed all the above handover scenarios in their protocols [13, 14] but, still these protocols suffered from some vulnerabilities as: (1) numerous message exchange is required in the S1-based handover to contact the MME. Hence, the communication network delays the handover and degrades the transmission performance. In addition, a secure authentication medium is required between eNBs in LTE X2 based handover. But, the handover between HeNB and open mode HeNB may generate complexity due to its architecture. (2) 3GPP has recommended a new handover key derivation scheme in LTE/LTE-A networks that generates various eNB keys based on vertical/horizontal key management approach. Therefore, it increases the system complexity and suffers from key forward/backward secrecy [15].

Furthermore, researchers have proposed various handover authentication protocols to achieve the essential security demands in LTE/LTE-A networks [16–25]. These protocols can be divided into five categories: (1) Authentication, Authorizing and Accounting (AAA) server based protocol; (2) Security Information Transmission (SIT) based protocol; (3) Identity-Based Cryptography (IBC) protocol; (4) Bilinear pairing based protocol; and (5) Chameleon hash function based protocol. These protocols maintain the mutual authentication between the communication entities and basic security requirements but, fail to achieve the key forward/backward secrecy and vulnerable to various identified attacks. Moreover, the key escrow problem and high computation overhead are also observed in these protocols during the key operations. Therefore, these protocols are not well suited for secure handover authentication in LTE/LTE-A network.

Recently, the proxy signature based handover protocols [26–30] are also proposed to avoid all the above problems in LTE/LTE-A networks. In the proxy signature scheme, the HSS delegates its signing capability (proxy warrant) to the UE and eNB that allows them to obtain the proxy signature on behalf of the HSS [31, 32]. These protocols fulfill most of the security features and incur less bandwidth consumption compare to the above protocols during the handover but, vulnerable to various security issues such as key escrow, privacy preservation, redirection attack and revocation. The revocation is an important feature in proxy signature schemes. The original signers can revoke the delegation rights from the proxy signers whenever they compromised during the authentication process. Although, researchers have proposed the proxy signature based protocols with revocation [33, 34] but, these solutions for revocation don't suit to handover protocols in LTE/LTE-A

networks. Hence, it is require to propose a proxy signature based efficient and robust handover authentication protocol with revocation in the LTE/LTE-A networks.

1.1 Technical Contribution

In order to avoid the above identified problems and fulfill all the security requirements, we propose the efficient and robust proxy signature based handover authentication protocol with revocation. The main contributions of this paper are as follows.

1. In the proposed protocol, UE and new eNB achieve the secure mutual authentication during the handover process. Meanwhile, a shared secret key is established between UE and eNB. In addition, the protocol establishes the revocation property whenever the UE/eNB compromised during the handover authentication. Also, the protocol preserves the privacy of UE and eNB during the key distribution with the authentication entities.
2. The protocol is applicable in all the mobility scenarios and maintains the key forward/backward secrecy during the handover authentication process.
3. The proposed protocol is formally verified by BAN logic and simulated using the AVISPA tool. The analysis proves the correctness and represents that the protocol achieves all the security goals.
4. The security analysis of the protocol is presented with respect to various security parameters. The analysis shows that the protocol avoids all the identified attacks. Also, the proposed protocol resists from the key escrow problem.
5. The performance evaluation of the proposed handover protocol is carried out in terms of transmission overhead, storage overhead, message overhead and computation overhead with respect to existing protocols.

1.2 Organization of the Paper

The remaining sections of this paper are organized as follows. Section 2 illustrates the related work of various handover protocols. A preliminary overview is presented in Sect. 3. The proposed handover protocol is shown in Sect. 4. The formal analysis and verification of the proposed protocol are presented in Sect. 5 followed by its security analysis in Sect. 6. The performance evaluation of the proposed and existing protocols is compared in Sect. 7. Finally, Sect. 8 concludes the paper with future aspects.

2 Related Work

A lot of research has been carried out to propose the efficient and robust handover authentication protocol. Many AAA server, SIT, bilinear pairing, IBC, chameleon hash function and proxy signature based handover protocols have been proposed to enhance the security and reduce the bandwidth consumption of the communication network. In this section, we discuss and analyze these protocols on the basis of their characteristics.

A hash chaining based pre-authentication protocol is proposed by Hong et al. [17]. The hash functions are shared between the communication entities and performed the handover authentication. Unfortunately, the protocol suffers from heavy overload at the network. In addition, Bohák et al. [16] proposed a pre-authentication based approach that eliminates linear dependency between AP and AAA server. In order to establish such a framework, a

trust relationship is required to maintain among operating nodes. But, a high network traffic can be observed in the protocol which increases the complexity of the system. Hence, these approaches are not suited for handover authentication due to the connection failure between the communication entities and heavy burden at the AAA server.

To avoid the above problems, Zhang et al. [18] and Cai et al. [19] proposed the handover protocols based on SIT. In these schemes, the security information with corresponding parameters of UE is transmitted to the new base station from the current base station before UE handover. In addition, these schemes don't require the communication between AP and AAA server. Hence, the communication channel between the entities is free from authentication traffic. Although, a trust relationship between the communicating AP's is desirable but, it makes the overall system complex and over burdened in various handover scenarios.

Kim et al. [20] proposed the IBC based handover protocol that mitigates the problems of above explained protocols. The protocol doesn't communicate with AAA server and achieves the mutual authentication between UE/MN and new eNB/AP without pre-authentication or trust relationship. However, the protocol didn't obtain the key forward/backward untraceability (KFU/KBU) during the authentication process. Also, the protocol can't avoid the key escrow problem as private keys of UE or enB are obtained from the private key generator (PKG). Moreover, the protocol suffers from high computation overhead and bandwidth consumption because the computationally expensive bilinear pairing based operations. Further, Cao et al. [21] proposed the handover authentication protocol between E-UTRAN and non-3GPP to overcome all the issues of Kim's protocol. The protocol establishes the mutual authentication between the communication entities and achieves the KFU/KBU. Unfortunately, the protocol doesn't preserve the privacy of authentication entities and suffers from the key escrow problem. Hence, these protocols are not suitable for traditional handover authentication.

Zhang et al. [22] and Han et al. [24] proposed an identity-based handover protocol in wireless networks that defeat the various malicious attacks and maintain the KFU/KBU. Unfortunately, these protocols suffer from key escrow problem and high computation overhead due to time consuming pairing operations. Therefore, it is not possible to mandate this expensive infrastructure for handover protocols. Choi et al. [23] proposed the credentials based chameleon hashing handover protocol. In this protocol, credentials are generated from collision resistant hash functions that provide mutual authentication between MN and AP. But, the protocol is vulnerable to MiTM attack and can't achieve the KFU/KBU. Similarly, Zhang et al. [25] addressed the handover authentication protocol that avoids the key escrow problem from Han's scheme. But, the protocol doesn't preserve the privacy and suffers from the redirection attack. Specifically, the protocol incurs the high storage and message overhead due to certificate based key operations. Hence, these handover protocols are not suitable for secure communication in LTE/LTE-A networks.

Different from above explained handover protocols, researchers have proposed proxy signature based handover authentication protocols. Roh et al. [26] proposed a RSA-based proxy signature protocol where the authentication information of respective MN is transferred to the new AP from current AP. In addition, Jing et al. [27] addressed the EAP-based handover scheme for the wireless network. In this scheme, all the communicating APs maintain a trust relationship among them and keep the knowledge of their public keys. Moreover, MN communicates to the current AP to obtain the secure information for the verification of the new AP. These schemes require to generate a trust relationship among APs and the association of current AP. Hence, this framework makes the overall network complex.

Further, Cao et al. [28] proposed the handover authentication protocol in LTE/LTE-A networks based on proxy signature. The protocol defeats all the issues of above explained protocols, but suffers from high message overhead and computational consumption because it performs the computationally expensive modular exponentiation operations during the authentication process. Similarly, Cao et al. [29] proposed the handover protocol for various eNBs in LTE/LTE-A networks. The authentication process of the protocol is very similar to [28]. Hence, it carries the similar drawbacks in the authentication process. Recently, Qiu et al. [30] proposed a handover authentication protocol. The protocol avoids all the issues of existing protocols and free from high computational overhead. But, the revocation property is not maintained by the protocol whenever UE or eNB compromises their delegation rights. Although, the revocation property is maintained in various proxy signature based protocols, but the solutions for revocation incur security issues. Sun [33] proposed a time-stamp based proxy signature scheme that allows the verifier to verify the proxy signer. Further, Das et al. [34] pointed out that the Sun's scheme is insecure and proposed a trusted third party based proxy signature scheme. In real world applications, the trusted third party is a strong assumption. Hence, these solutions don't suit to accomplish revocation in the handover protocols.

From the literature survey, it can be concluded that the above explained handover protocols are not suitable for secure handover authentication in LTE/LTE-A network. These schemes suffered from various kinds of issues and drawbacks. Moreover, most of the protocols generate the heavy bandwidth consumption and computational complexities. Hence, researchers have proposed the proxy signature based handover protocols to overcome all the above mentioned issues but, none of them accomplish all the security features and requirements. In addition, these protocols didn't consider the revocation property. Therefore, considering the advantage of the protocol [35], we propose the proxy signature based handover authentication protocol with revocation for various mobility scenarios in LTE/LTE-A network. The proposed protocol establishes the mutual authentication between UE and new eNB. The protocol achieves all the security properties as data integrity, confidentiality, key secrecy and privacy preservation. Also, the protocol reduces the computational and storage overhead from the network.

3 Preliminary

In this section, we present the important specifications of the handover authentication protocol in LTE/LTE-A network. The brief overview of the Elliptic Curve Cryptography (ECC) is also described.

3.1 Requirement of Handover Authentication

The essential and basic requirement for handover authentication is to establish the mutual authentication between the communication entities. Moreover, it is also required to maintain a shared secret session key between the UE and target base station to assure the confidentiality of successive communication. The handover authentication protocol in LTE/LTE-A network should accomplish these requirements.

- The handover protocol should follow the KFU/KBU during the authentication process. Moreover, the protocol should establish the privacy preservation and freshness of session key in each connection.

- The proposed protocol should exhibit the vigorous security throughout the authentication process to defeat various kinds of attacks in the communication network.
- The UE is a resource constrained device and the communication channel has the limited bandwidth. Hence, the proposed handover protocol should be designed in such a way that the protocol could maintain the appropriate efficiency in terms of communication and computation overhead.
- From the efficiency point of view, the handover AKA protocol should keep the computation overhead within 20 ms to achieve the undisrupted and smooth traffic [25].
- In the handover authentication protocol, the UE/eNB must be revoked automatically if their delegation period expires. Moreover, the original signer must withdraw the delegation right from proxy signers whenever the proxy signers are compromised.

3.2 Elliptic Curve Cryptosystem

To authenticate the handover process between UE and target eNB/HeNB in LTE/LTE-A network, we are using the elliptic curve cryptosystem (ECC). The proposed handover scheme is based on the elliptic curve discrete logarithmic problem (ECDLP) [36]. It is observed that the computation of ECDLP is infeasible with the polynomial-time algorithm and the ECC key (160 bits) achieves the similar security as the RSA key (1024 bits). Moreover, the cryptographic operations such as addition, multiplication and point multiplication are faster than the modular exponentiation operated in the group.

Consider, n be a prime and $E(F_n)$ an elliptic curve over F_n having n elements. There are two elements x, y defined in E over F_n holding an equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_1, a_2, a_3, a_4, a_5, a_6 \in F_n$. Let P be a point of $E(F_n)$ with a prime order q, where $q|\#E(F_n)$. In addition, C be a cyclic group having the generator P. Z_q is the finite field of integers modulo prime q and Z_q^* is the multiplicative sub-group of Z_q.

- *Note-1* Given a group C of prime order q with P and an element $xP \in C$, where $x \in Z_q^*$. It is computationally hard to compute the x from P and xP (ECDLP).
- *Note-2* Given a group C of prime order q with P and an element $P, xP, yP \in C$, where $x, y \in Z_q^*$. It is computationally hard to generate the xyP with any polynomial time algorithm (Computational Diffie–Hellman problem).

4 Proposed Protocol

In this section, we propose a handover scheme to authenticate the communication entities in LTE/LTE-A network. The proposed protocol adopts the ECC with proxy signature methodology. In the proposed protocol, the cyclic group C is used for ECC with its order q (160 bits). Further, three cryptographic secure collision resistant one way hash functions are also selected as $H_i : \{0,1\}^* \times C \longrightarrow Z_q^*$, where $i = 1, 2, 3$.

The proposed protocol consists of two phases: (1) initial authentication phase and (2) handover authentication phase. In the initial authentication phase, UE and eNB/HeNB are verified at MME and obtains the proxy delegation from HSS. In the handover authentication phase, the authentication process is initiated whenever UE moves from one base station to another one. The protocol considers all the handover scenarios described in Sect. 1. In between the handover authentication process, the HSS verifies the UE or eNB and revoke the proxy delegation if the entities are compromised. The notations and definition of the proposed protocol are as listed in Table 1.

4.1 Initial Authentication Phase

In this phase, UE needs to authenticate at MME and HSS to communicate on the network. To obtain the mutual authentication between UE and HSS, UE executes the improved Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol [15]. During the verification process, some parameters such as warrant, delegation token and other information are enclosed in the message authentication response of EPS-AKA protocol. These newly added information in the EPS-AKA protocol do not degrade the performance of the network. In this protocol, after the successful verification of the UE from the MME, HSS delegates its signing power σ_{HSS-UE} to the UE through a secure channel K_{ASME}. We assume that the communication path between UE and HSS is secured by diameter protocol. HSS also transfers the delegation authority $\sigma_{HSS-eNB}$ to the eNB after the verification of eNB at MME. The path between enB and HSS is secured by Internet protocol security (IPsec). Moreover, each entity z selects a private key $x_z \in Z_q{}^*$ and computes the public key $PK_z = x_z \cdot P$ in the communication network. The pictorial presentation of the initial authentication phase is shown in Fig. 2 and step-wise description is as follows:

- *Step-1* Firstly, UE selects a random number $x_{UE} \in Z_q{}^*$ and generates $PK_{UE} = x_{UE} \cdot P$. UE transfers the request message (X') to the MME that consists the encrypted *IMSI* as $X' = \{\{IMSI\}_{x_{UE}}\}_{PK_{MME}}$.
- *Step-2* After receiving the X', MME decrypts it and generates the *IMSI*. Then, MME selects a random number $x_{MME} \in Z_q{}^*$ as its secret key and generates the public key $PK_{MME} = x_{MME} \cdot P$. Then, MME transfers a request authentication message (Y') to the HSS that consists the encrypted *IMSI* as $Y' = \{\{IMSI\}_{x_{MME}}\}_{PK_{HSS}}$.
- *Step-3* After receiving the Y', HSS decrypts it and stores the *IMSI*. HSS also generates the corresponding *AVs* for the UE that consists *XRES*, K_{ASME} and *AUTN*. Then, HSS chooses a random value $\kappa_{HSS-UE} \in Z_q$ and generates $K_{HSS-UE} = \kappa_{HSS-UE} \cdot P$. Further, HSS selects the PW_{UE} for the UE that defines validity of proxy delegation and consists $h(AVs||IMSI||ID_{HSS})$. Then, HSS computes the proxy delegation with warrant

Table 1 Notations and definition of the proposed protocol

Notation	Definition
IMSI	International mobile subscriber identity
RES / *XRES*	Response/expected response
K_{ASME}	Access security management entity key
AUTN	Authentication token
x_{UE} /x_{MME} /x_{HSS}	Private key of UE/MME/HSS
PK_{UE} /PK_{MME} /PK_{HSS}	Public key of UE/MME/HSS
x_z /PK_z	Private/ public key of z
σ_{HSS-z}	The delegation of HSS transfers to z
h_{HSS-z}	Delegation information token of z
D_z	Signing key of z
K_{HSS-z}	Delegation information of HSS to z
S_z	Proxy signed signature of z by D_z
PW_z	Proxy warrant of z
$info_z$	Authentication information of z

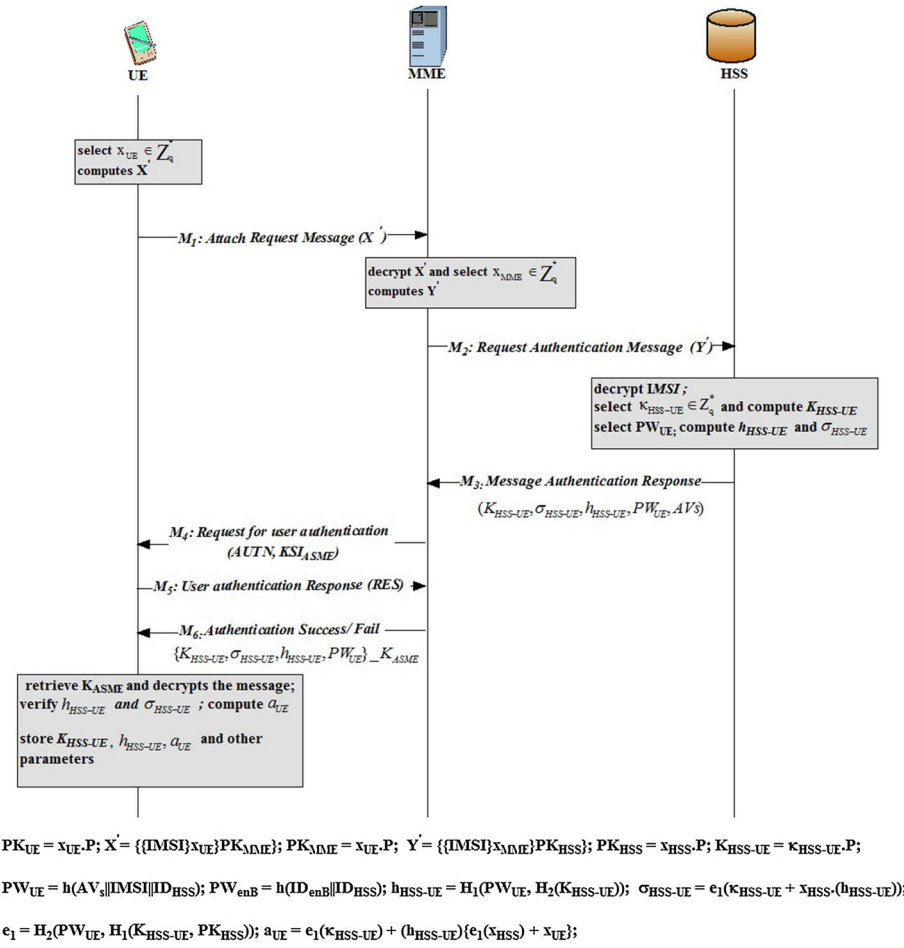

Fig. 2 The initial authentication phase

information as

$$\sigma_{HSS-UE} = (e_1(\kappa_{HSS-UE} + x_{HSS}(h_{HSS-UE}))) \tag{1}$$

where $h_{HSS-UE} = H_1(PW_{UE}, H_2(K_{HSS-UE}))$. In addition, $e_1 = H_2(PW_{UE}, H_1(K_{HSS-UE}, PK_{UE}))$. Finally, HSS transfers a message authentication response $(K_{HSS-UE}, \sigma_{HSS-UE}, h_{HSS-UE}, PW_{UE})$ with *AVs* (authentication vector) to the MME.

- *Step-4* MME receives the *AVs* from the HSS and stores the *XRES* and K_{ASME}. Further, it transfers the user authentication request *AUTN* and KSI_{ASME} (an index for K_{ASME}) to the UE.
- *Step-5* Then, UE computes the *AUTN* and compares it with received *AUTN* from MME. If they match, MME is authenticated at UE. Further, UE generates the corresponding *RES* and transfers to the MME.
- *Step-6* After receiving the authentication response from the UE, MME verifies whether $RES = XRES$ or not. If the verification fails, MME transfers an authentication decline message to the UE. On successful verification of the UE, MME retrieves the K_{ASME} and

encrypts the $(K_{HSS-UE}, \sigma_{HSS-UE}, h_{HSS-UE}, PW_{UE})$ with K_{ASME}. Then, MME sends this encrypted message to the UE.

Further, UE retrieves the K_{ASME} and decrypts the received message. Then, it verifies the σ_{HSS-UE} as

$$\sigma_{HSS-UE} \cdot P = (e_1(K_{HSS-UE} + PK_{HSS}(h_{HSS-UE}))) \tag{2}$$

If the verification is successful, UE acquires the legitimate proxy delegation σ_{HSS-UE} and keeps all these parameters. Moreover, UE generates its proxy private key and proxy public key from Eq. (2) as

$$\begin{aligned} a_{UE} &= \sigma_{HSS-UE} + (h_{HSS-UE})x_{UE} \\ &= e_1(\kappa_{HSS-UE}) + h_{HSS-UE}\{e_1(x_{HSS}) + x_{UE}\} \end{aligned} \tag{3}$$

$$\begin{aligned} A_{UE} &= a_{UE} \cdot P \\ &= (e_1(\kappa_{HSS-UE}) + h_{HSS-UE}\{e_1(x_{HSS}) + x_{UE}\}) \cdot P \\ &= e_1(K_{HSS-UE}) + h_{HSS-UE}\{e_1(PK_{HSS}) + PK_{UE}\} \end{aligned} \tag{4}$$

Otherwise, UE transfers an authentication failure message to the HSS. And; MME removes the $(K_{HSS-UE}, \sigma_{HSS-UE}, h_{HSS-UE}, PW_{UE})$. Furthermore, UE sends a request message to the HSS for a legitimate proxy delegation whenever the warrant expires.

Similar to above defined process, each eNB is also verified at MME using its identity ID_{eNB}. In addition, eNBs select the random number and generate the corresponding the public key. HSS selects the PW_{eNB} for eNB that defines the validity of proxy delegation and consists $h(ID_{eNB}||ID_{HSS})$ with related parameters. The CSG identity is also required if an eNB is hybrid or closed HeNB. eNB obtains the proxy delegation $K_{HSS-eNB}, \sigma_{HSS-eNB}, h_{HSS-eNB}, PW_{eNB}$ from the HSS through a secure channel. eNB also computes its proxy private key (a_{eNB}) and proxy public key (A_{eNB}) and keep it secure for the subsequent handover authentication. The proxy secret keys are updated by the HSS only after the authentication data requested by the MME.

4.2 Handover Authentication Phase

In the handover authentication phase, whenever the UE enters into the coverage area of another eNB (eNB_2) from the current base station (eNB_1), the mutual authentication and key compliance procedure is initiated between UE and eNB_2. Both the communication entities apply their proxy secret keys obtained in the initial authentication phase. In this section, we describe the handover scenarios such as LTE X2 based handover, S1 based intra/inter-MME handover and S1 based hybrid/CSG HeNB handover. The LTE X2 based handover and S1 based intra-MME handover follow the traditional handover authentication process. However, in the S1 based inter-MME handover where the source MME (MME_1) transfers the information of current UE to the target MME (MME_2). In S1 based hybrid/CSG HeNB handover, only MME_1 verifies the subscription of the UE to access the target HeNB. In these two handover scenarios, some additional steps are required with the traditional handover authentication process. Figure 3 depicts the handover authentication process in LTE/LTE-A network. The steps are illustrated as follows:

- *Step-1* Whenever, the UE moves into coverage area of new base stations, it has the public keys of neighbor *eNBs* and other information such as physical cell ID (PCI), public land mobile network-ID (PLMN-ID) and location area identity (LAI) of eNB_2 from eNB_1. Also, it may require the CSG_{ID} if the eNB_2 is hybrid/CSG HeNB. If it is, the UE verifies whether its CSG_{ID} in CSG whitelist. Then, UE selects a random number $m_{UE} \in Z_q^*$ and computes $M_{UE} = m_{UE} \cdot P$. Now, UE generates the signing key D_{UE} as

$$D_{UE} = (e_2(m_{UE} + x_{UE}(h_{UE}))) \tag{5}$$

where $h_{UE} = H_1(info_{UE}, H_2(M_{UE}))$. The $info_{UE}$ includes the corresponding parameters such as *IMSI* of UE, Globally Unique Temporary ID ($GUTI_{ID}$), $PLMN_{ID}$, MME_{ID} of MME_1, cell ID (*ECI*), *PCI*, target *LAI*, UE security capability algorithms (integrity key (*IK*) and cipher key (*CK*)) and optional CSG_{ID}. And, $e_2 = H_2(PW_{UE}, H_1(M_{UE}, PK_{eNB}))$.

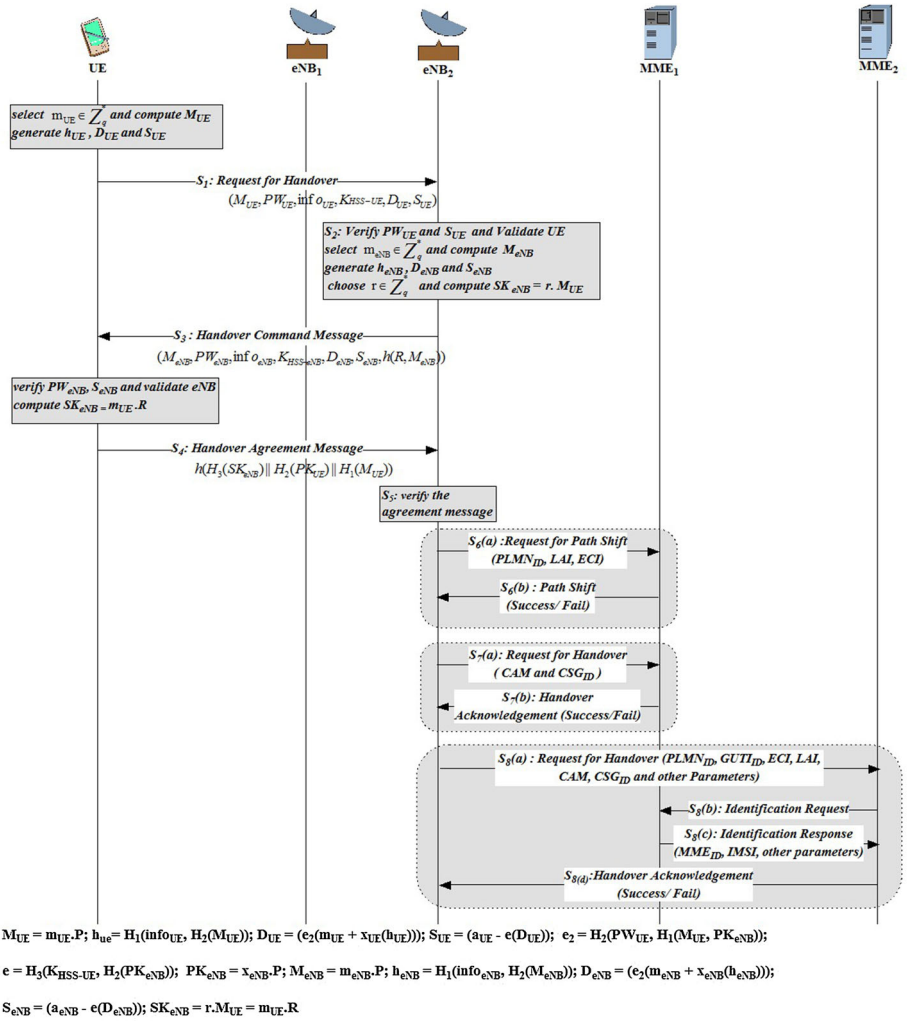

Fig. 3 The handover authentication phase

Finally, it computes the proxy signed signature S_{UE} from D_{UE} as

$$S_{UE} = (a_{UE} - e(D_{UE})) \tag{6}$$

where $e = H_3(K_{HSS-UE}, H_2(PK_{eNB}))$. Then, UE transfers the handover request message $(M_{UE}, PW_{UE}, info_{UE}, K_{HSS-UE}, D_{UE}, S_{UE})$ to the eNB_2.

- *Step-2* After receiving the handover request message, eNB_2 verifies the validity of PW_{UE} and finds whether its delegation time is expired or not. If the delegation time of PW_{UE} is expired, eNB_2 declines the handover request of the UE and UE inquires for a new proxy delegation from the HSS. Otherwise, eNB_2 verifies D_{UE} as

$$\begin{aligned} D_{UE} \cdot P &= (e_2(m_{UE} + x_{UE}(h_{UE}))) \cdot P \\ &= (e_2(M_{UE} + PK_{UE}(h_{UE}))) \end{aligned}$$

From Eq. (6), eNB_2 verifies the proxy signed signature as

$$\begin{aligned} S_{UE} \cdot P &= (a_{UE} - e(D_{UE})) \cdot P \\ S_{UE} \cdot P + e(D_{UE}) \cdot P &= a_{UE} \cdot P \end{aligned}$$

And, from Eqs. (3) and (5);

$$\begin{aligned} &S_{UE} \cdot P + e(e_2(M_{UE} + PK_{UE}(h_{UE}))) \\ &= (e_1(K_{HSS-UE}) + h_{HSS-UE}\{e_1(PK_{HSS}) + PK_{UE}\}) \\ &= a_{UE} \cdot P \end{aligned}$$

If it verifies, eNB_2 successfully authenticates the handover authentication request of UE otherwise eNB_2 transfers verification failure message.

- *Step-3* Further, eNB_2 selects a random number $m_{eNB} \in Z_q^*$ and computes $M_{eNB} = m_{eNB} \cdot P$. Then, it generates the signing key D_{eNB} as

$$D_{eNB} = (e_2(m_{eNB} + x_{eNB}(h_{eNB}))) \tag{7}$$

where $h_{eNB} = H_1(info_{eNB}, H_2(M_{eNB}))$. The $info_{eNB}$ includes the corresponding parameters such as $PLMN_{ID}$, $GUTI_{ID}$, MME_{ID} of MME_1, ECI, PCI, target LAI, enB security capability algorithms (IK and CK) and optional CSG_{ID}. And, $e_2 = H_2(PW_{eNB}, H_1(M_{eNB}, PK_{UE}))$. Finally, it computes the proxy signed signature S_{eNB} from D_{eNB} as

$$S_{eNB} = (a_{eNB} - e(D_{eNB})) \tag{8}$$

where $e = H_3(K_{HSS-eNB}, H_2(PK_{UE}))$. In addition, for the secure communication between eNB_2 and UE, eNB_2 generates the session key $SK_{eNB} = r \cdot M_{UE}$; where $r \in Z_q^*$ and $R = r \cdot P$. Finally, eNB_2 transfers the handover message $(M_{eNB}, PW_{eNB}, info_{eNB}, K_{HSS-eNB}, D_{eNB}, S_{eNB}, h(R, M_{eNB}))$ to the UE.

- *Step-4* UE receives the handover message and verifies the validity of PW_{eNB} and checks whether its delegation time is expired or not. If the delegation time of PW_{eNB} is expired, UE declines the handover command of eNB_2 and eNB_2 inquires for a new proxy delegation from the HSS. Otherwise, UE authenticates D_{eNB} as

$$\begin{aligned} D_{eNB} \cdot P &= (e_2(m_{eNB} + x_{eNB}(h_{eNB}))) \cdot P \\ &= (e_2(M_{eNB} + PK_{eNB}(h_{eNB}))) \end{aligned}$$

From Eq. (8), UE verifies the proxy signed signature as

$$\begin{aligned} S_{eNB} \cdot P &= (a_{eNB} - e(D_{eNB})) \cdot P \\ a_{eNB} \cdot P &= S_{eNB} \cdot P + e(e_2(M_{eNB} + PK_{eNB}(h_{eNB}))) \\ &= (e_1(K_{HSS-eNB}) + h_{HSS-eNB}\{e_1(PK_{HSS}) + PK_{eNB}\}) \\ &= a_{eNB} \cdot P \end{aligned}$$

If it verifies, UE successfully authenticates the handover command of eNB_2; otherwise UE transfers verification failure message. In addition, UE generates the session key $SK_{eNB} = m_{UE} \cdot R$. If the computed SK_{eNB} matches with the session key of eNB_2, then UE transfers a handover agreement message as $h(H_3(SK_{eNB}), H_2(PK_{UE}), H_1(M_{UE}))$.

- *Step-5* eNB_2 computes the $h(H_3(SK_{eNB}), H_2(PK_{UE}), H_1(M_{UE}))$ and verifies with the received handover agreement message. If the computed agreement matches with the received one, then handover process completed successfully. Hence, the eNB_2 provides the communication service to the UE after the completion of the traditional handover process.
- *Step-6* According to S1 based intra-MME mobility scenario, the eNB_2 communicates with MME_1. In this process, eNB_2 does not operate as hybrid/CSG HenB and MME_1 remains persistent. Therefore, it follows the same process from Step-1 to Step-5 and a request message of path shift is transferred from eNB_2 to the MME_1 that consists the $PLMN_{ID}$, *LAI* and *ECI*. Then, MME_1 approves the request message and transfers a positive response with path shift to the eNB_2.
- *Step-7* If eNB_2 is hybrid/CSG HeNB and MME_1 remains persistent, some additional steps are required by the traditional handover mechanism to mutually authenticate UE and HeNB followed by UE membership verification. The procedure is as follows:

  1. The verification of UE at eNB_2 (HeNB) follows the similar authentication from Step-1 to Step-2.
  2. Now, eNB_2 transfers a handover request that consists cell access mode (*CAM*) and CSG_{ID} to the MME_1.
  3. MME_1 verifies the *CAM* and CSG_{ID} of eNB_2. If it fails, MME_1 ends the handover authentication with a failure message. Now, MME_1 regulates the CSG membership of the UE in *CAM*. If the eNB_2 executes in *CAM*, establish the UE access control and set the priority of UE. Otherwise, MME_1 transfers a handover decline message to the UE. Further, MME_1 transfers the handover success message to the eNB_2 that includes priority status of UE and CSG_{ID}.
  4. After receiving the successful acknowledgment, eNB_2 proceeds from Step-3 to Step-5.

- *Step-8* If eNB_2 is not communicating with the MME_1, it selects a new MME (MME_2) in S1 based inter-MME handover. In addition, the membership of UE is verified after the completion of handover if eNB_2 is HeNB. The procedure is as follows:

  1. The mutual authentication of UE and eNB_2 is performed from Step-1 to Step-2.
  2. Then, eNB_2 transfers a handover request to the MME_2 with relative information that consists $PLMN_{ID}$, $GUTI_{ID}$, *ECI*, target *LAI*, optional CSG_{ID} and *CAM* of MME_2.

3. MME_2 receives the handover request and uses the $PLMN_{ID}$, ECI and $GUTI_{ID}$ to obtain the information of the MME_1. Then, it transfers the identification request to the MME_1.
4. MME_1 transfers the response message to the MME_2 that includes MME_{ID}, $IMSI$, network capability and security context algorithms of the UE.
5. Finally, MME_2 transfers the handover acknowledgement message to the eNB_2. If the eNB_2 is a hybrid/CSG HeNB, then MME_2 follows the similar process with MME_1 as shown in Step-7. Further, the handover authentication process proceeds with Step-3 to Step-5.

During the handover authentication process, the HSS delegates its signing capability to the UE or eNB_2 with proxy warrant PW_{UE} or PW_{eNB}. The delegation information must be aborted after the validity period expires. However, the HSS can terminate the proxy delegation authority from the UE or eNB_2 whenever these entities compromised during the handover process. We are assuming that the HSS have noticed about the exploitation of proxy delegation information by UE or eNB_2. Hence, the HSS wants to withdraw the proxy delegation power from UE or eNB_2. Therefore, HSS executes the following proxy revocation steps.

- *Step-1* HSS transfers a proxy revocation request $(PW_{UE}, M_r, \sigma_{HSS-UE}, PK_{HSS}, K_{HSS-UE})$ to the UE. M_r consists the reason of proxy revocation.
- *Step-2* UE receives the proxy revocation request. If the warrant time of PW_{UE} is expired, UE declines the delegation information. Otherwise, the HSS selects a random number $b \in Z_q^*$; $B = b \cdot P$ and transfers to UE through a secure channel. Then, HSS computes $c = h(K_{HSS-UE}||PK_{HSS}||B)$ and stores it.
- *Step-3* UE receives the random number and computes the validation function c as

$$c = h(K_{HSS-UE}||PK_{HSS}||B) \tag{9}$$

  Then, it computes $y = b - c(x_{UE})$ and sends to the HSS.
- *Step-4* HSS receives y and computes c' as

$$c' = h(K_{HSS-UE}||PK_{HSS}||(y + c(x_{UE})) \cdot P) \tag{10}$$

  Now, HSS verifies whether $c' = c$ or not. If it is an invalid match, HSS confirms that the UE is compromised. Then, the HSS withdraws the delegation power from the UE and transfers the compromised information of UE (PW_{UE}, K_{HSS-UE}) to the eNB_2. Hence, eNB_2 maintains a revocation list from the information of compromised UEs. If the UE has still the valid delegation period and eNB_2 doesn't find the K_{HSS-UE} of the UE in the revocation list, then UE is legitimate entity and maintains the mutual authentication with eNB_2. In another scenario, the UE has the valid delegation period but, eNB_2 finds the K_{HSS-UE} of the UE in revocation list. In this case, eNB_2 will no longer communicate to the compromised UE. In addition, K_{HSS-UE} from the revocation list is eliminated whenever the proxy delegation (PW_{UE}, K_{HSS-UE}) is expired. Therefore, the size of the revocation list will not increase.

Similarly, eNB_2 follows the above proxy revocation steps with HSS if it is compromised in the handover authentication process.

The proposed handover authentication protocol follows the 3GPP standard during the communication process. Although, some additional steps are added in signaling messages

but, it doesn't generate the computational complexity. Moreover, the protocol achieves all the mobility scenarios with revocation without generating complex key mechanism.

5 Formal Analysis and Verification of the Proposed Protocol

To analyze the authenticity of the proposed protocol, we use the BAN logic model [37] and AVISPA tool [38]. BAN logic rigorously verifies the cryptographic protocols and prove the correctness of the scheme. In this section, the proposed protocol is also simulated by the AVISPA tool. The analysis represents that the protocol is free from all the malicious attacks.

5.1 Formal Verification Using BAN Logic

This subsection illustrates the basic syntax, notations, symbols, inference rules of the logic model. In addition, the correctness and verification of the protocol is proved by achieving the adequate security goals. In the BAN logic model, there are several entities such as principals, encryption keys and statements. The principals are S and T; X and Y are the statements; K_s and K_t are represented as public keys and ${K_s}^{-1}$, and ${K_t}^{-1}$ are the private keys.

5.1.1 Basic Syntax and Definitions

The basic notations and symbols with their semantics in the BAN logic model are as follows.

(D1) $S| \equiv X$: S believes that X is true; in other words, S is designated to believe X.
(D2) $S| \sim X$: S transfers a message including X at some time, but it is true that S believes X.
(D3) $S \triangleleft X$: S reads and receives the message X; or say, message X is transmitted to S.
(D4) $S| \Rightarrow X$: S contains authority over X; or say, S regulates to X.
(D5) $\#(X)$: X has not transfer the message before executing the protocol.
(D6) $\{X\}_K$: X is encrypted by key K.
(D7) $\xrightarrow[S]{K_s}$: K_s is the public key of S and the private key ${K_s}^{-1}$ will never be compromised other than S.
(D8) $S \xleftrightarrow{K} T$: K is the shared key between S and T. Other than S and T, no one can know about it.
(D9) $\langle X \rangle_Y$: X is combined with Y.
(D10) $S \overset{X}{\Leftrightarrow} T$: X is secretly known only to S and T; only possible principals trusted by them.

5.1.2 Inference Rules of BAN Logic

The inference rules of BAN logic are stated as follows.

- Rule-1. *Message Meaning Rule* (*a*) $\frac{S|S \equiv \xrightarrow[T]{K_t}, S \triangleleft \{X\}_{K_t}^{-1}}{S| \equiv T| \sim X}$; (*b*) $\frac{S|S \equiv \xleftrightarrow{K} T, S \triangleleft \{X\}_K}{S| \equiv T| \sim X}$ and

(*c*) $\frac{S|\equiv S \overset{Y}{\Leftrightarrow} T, S \triangleleft \langle X \rangle_Y}{S|\equiv T|\sim X}$

- Rule-2. *Jurisdiction Rule* $\frac{S|\equiv T|\Rightarrow X, S|\equiv T|\equiv X}{S|\equiv X}$
- Rule-3. *Nonce Verification Rule* $\frac{S|\equiv \#(X), S|\equiv T|\sim X}{S|\equiv T|\equiv X}$
- Rule-4. *Belief Rule* $\frac{S|\equiv Y, S|\equiv X}{S|\equiv (Y,X)}$ or $\frac{S|\equiv (Y,X)}{S|\equiv (Y)}$
- Rule-5. *Freshness Rule* $\frac{S|\equiv \#(X)}{S|\equiv \#(X,Y)}$

5.1.3 Security Goals of the Protocol

The proposed handover protocol must fulfill the following security goals to achieve the authentication between the communication entities. For simplicity, UE, eNB, MME and HSS are represented as *U*, *E*, *M* and *H* respectively. Hence, the security goals of the proposed handover authentication protocols are as follows.

Goal 1 $M| \equiv U| \equiv IMSI$; *Goal 2:* $H| \equiv M| \equiv IMSI$; *Goal 3* $H| \equiv H \overset{K_{ASME}}{\longleftrightarrow} M$; *Goal 4* $M| \equiv M \overset{K_{ASME}}{\longleftrightarrow} U$; *Goal 5* $U| \equiv E| \equiv U \overset{SK}{\longleftrightarrow} E$; *Goal 6* $U| \equiv U \overset{SK}{\longleftrightarrow} E$; *Goal 7* $E| \equiv U| \equiv U \overset{SK}{\longleftrightarrow} E$; *Goal 8* $E| \equiv U \overset{SK}{\longleftrightarrow} E$; *Goal 9* $H| \equiv U \overset{c}{\Leftrightarrow} H$.

5.1.4 Formal Messages of the Proposed Protocol

The conventional messages of the handover authentication protocol are as follows.

- M_1: $U \rightarrow M$: $IMSI, \langle \{IMSI\}_{x_U} \rangle_{PK_M}$
- M_2: $M \rightarrow H$: $IMSI, \langle \{IMSI\}_{x_M} \rangle_{PK_H}$
- M_3: $H \rightarrow M$: $K_{H-U} = \kappa_{H-U} P,\ PK_H = x_H P,\ PK_U = x_U P,\ \{(\kappa_{H-U}, x_H h_{H-U}), K_{H-U}, h_{H-U}, PW_U, AV\}_{K_{ASME}}$
- M_4: $M \rightarrow U$: $\langle AUTN \rangle_{K_{ASME}}$
- M_5: $U \rightarrow M$: $\langle RES \rangle_{K_{ASME}}$
- M_6: $M \rightarrow U$: $\langle K_{H-U}, \sigma_{H-U}, h_{H-U} \rangle_{K_{ASME}}$
- S_1: $U \rightarrow E$: $M_U = m_U P,\ PK_U = x_U P,$ $\langle PW_U, info_U, S_U, D_U, M_U, K_{H-U} \rangle_{PK_E}$
- S_2: $E \rightarrow U$: $M_E = m_E P,\ PK_E = x_E P,\ R = rP,$ $\langle PW_E, info_E, S_E, M_E, K_{H-E}, D_E, PK_E, SK, h(R, M_E) \rangle_{K_E}$
- S_3: $U \rightarrow E$: $\langle R, PK_U, M_U, SK \rangle_{K_E}$
- R_1: $H \rightarrow U$: $B = bP$ $\langle PW_U, M_r, \sigma_{H-U}, PK_H, K_{H-U} \rangle_{K_{ASME}}$; $\langle B, PK_U \rangle_{K_{ASME}}$
- R_2: $U \rightarrow H$: $\langle PK_H, y, h(K_{H-U}, PK_H, B) \rangle_{K_{ASME}}$

5.1.5 Transformation into Idealized Logical Form

The transformation of the formal messages into idealized logic form is as follows.

- *Message* $M_1 : U \rightarrow M$: $\langle IMSI \rangle_{U \overset{PK_M}{\longrightarrow} M}$
- *Message* $M_2 : M \rightarrow H$: $\langle IMSI \rangle_{M \overset{PK_H}{\longrightarrow} H}$

- *Message* $M_3 : H \rightarrow M : \langle (\kappa_{H-U}, x_H h_{H-U}), \kappa_{H-U} P, h_{H-U}, PW_U, AV, H \overset{K_{ASME}}{\longleftrightarrow} M \rangle_{H \overset{\kappa_{ASME}}{\longleftrightarrow} M}$
- *Message* $M_4 : M \rightarrow U$: $\langle AUTN, M \overset{K_{ASME}}{\longleftrightarrow} U \rangle_{M \overset{\kappa_{ASME}}{\longleftrightarrow} U}$
- *Message* $M_5 : U \rightarrow M$: $\langle RES, M \overset{K_{ASME}}{\longleftrightarrow} U \rangle_{M \overset{\kappa_{ASME}}{\longleftrightarrow} U}$
- *Message* $M_6 : M \rightarrow U$: $\langle K_{H-U}, \sigma_{H-U}, U \overset{h_{H-U}}{\Leftrightarrow} H \rangle_{M \overset{\kappa_{ASME}}{\longleftrightarrow} U}$
- *Message* $S_1 : U \rightarrow E$: $\langle M_U, PW_U, info_U, S_U, D_U, K_{H-U} \rangle_{U \overset{PK_E}{\longrightarrow} E}$
- *Message* $S_2 : E \rightarrow U : \langle M_E, PW_E, info_E, S_E, D_E, K_{H-E}, h(R, M_E), U \overset{SK}{\longleftrightarrow} E \rangle_{U \overset{\kappa_E}{\Leftrightarrow} E}$
- *Message* $S_3 : U \rightarrow E$: $\langle R, PK_U, M_U, U \overset{SK}{\longleftrightarrow} E \rangle_{U \overset{\kappa_E}{\Leftrightarrow} E}$
- *Message* $R_1 : H \rightarrow U$: $\langle PW_U, M_r, \sigma_{H-U}, PK_H, K_{H-U}, B, H \overset{K_{ASME}}{\longleftrightarrow} U \rangle_{H \overset{\kappa_{ASME}}{\longleftrightarrow} U}$
- *Message* $R_2 : U \rightarrow H$: $\langle PK_H, y, U \overset{c}{\Leftrightarrow} H \rangle_{H \overset{\kappa_{ASME}}{\longleftrightarrow} U}$

5.1.6 Basic Assumptions

To analyze the protocol, following assumptions are considered.

$(P1): \ U\| \equiv U \overset{PK_M}{\longrightarrow} M$	$(P2): \ M\| \equiv \#IMSI$	$(P3): \ M\| \equiv M \overset{PK_H}{\longrightarrow} H$
$(P4): \ U\| \equiv \#(\kappa_{H-U} P)$	$(P5): \ U\| \equiv \#(x_U P)$	$(P6): \ H\| \equiv \#(x_H P)$
$(P7): \ M\| \equiv M \overset{K_{ASME}}{\longleftrightarrow} U$	$(P8): \ M\| \equiv \#(x_M P)$	$(P9): \ U\| \equiv U \overset{PK_E}{\longrightarrow} E$
$(P10): \ U\| \equiv U \overset{K_E}{\Leftrightarrow} E$	$(P11): \ E\| \equiv \#(\kappa_{H-E} P)$	$(P12): \ E\| \equiv \#(x_E P)$
$(P13): \ E\| \equiv \#(m_E P)$	$(P14): \ E\| \equiv U\| \Longrightarrow U \overset{SK}{\longleftrightarrow} E$	$(P15): \ H\| \equiv H \overset{K_{ASME}}{\longleftrightarrow} U$
$(P16): \ H\| \equiv \#(bP)$	$(P17): \ H\| \equiv U\| \Longrightarrow U \overset{c}{\longleftrightarrow} H$	

5.1.7 Protocol Verification

This section uses the inference logic, assumptions and idealized form to verify the correctness of the security goals in the proposed protocol. The goals of the proposed protocol are formally verified as follows.

- (V_1) : from M_1: $M \triangleleft \langle IMSI \rangle_{U \overset{PK_M}{\longrightarrow} M}$; and From Rule-1 and $(P1)$, it can deduce that $M\| \equiv U\| \sim \langle IMSI \rangle$. From $(P2)$ and Rule-3, it is concluded that $M\| \equiv U\| \equiv IMSI$. It means *Goal 1* is achieved. Similarly, *Goal 2* can be achieved from message M_2.
- (V_2) : from M_3: $M \triangleleft \langle (\kappa_{H-U}, x_H h_{H-U}), \kappa_{H-U} P, h_{H-U}, PW_U, AV, H \overset{K_{ASME}}{\longleftrightarrow} M \rangle_{H \overset{\kappa_{ASME}}{\longleftrightarrow} M}$. From Rule-1 and $(P3)$, it is said that $M\| \equiv H\| \sim \langle (\kappa_{H-U}, x_H h_{H-U}), \kappa_{H-U} P, h_{H-U}, AV, H \overset{K_{ASME}}{\longleftrightarrow} M \rangle$. From Rule-3, Rule-5, $(P4)$, $(P5)$ and $(P6)$; it is said that $H\| \equiv H \overset{K_{ASME}}{\longleftrightarrow} M$. It means *Goal 3* is achieved.

- (V_3) : from M_4: $U \triangleleft \langle AUTN, M \overset{K_{ASME}}{\longleftrightarrow} U \rangle_{M \overset{K_{ASME}}{\longleftrightarrow} U}$; From Rule-1 and $(P7)$, it can deduce that $U| \equiv M| \sim \langle AUTN, M \overset{K_{ASME}}{\longleftrightarrow} U \rangle$. From Rule-3, Rule-5 and $(P8)$; it is said that $M| \equiv M \overset{K_{ASME}}{\longleftrightarrow} U$. It means *Goal 4* is achieved. Similarly, the *Message* M_5 and *Message* M_6 can be verified.
- (V_4) : from S_1: $E \triangleleft \langle M_U, PW_U, info_U, S_U, D_U, K_{H-U} \rangle_{U \overset{PK_E}{\longrightarrow} E}$; and From Rule-1 and $(P9)$, it can deduce that $E| \equiv U| \sim \langle M_U, PW_U, info_U, S_U, D_U, K_{H-U} \rangle$.
- (V_5) : from S_2: $U \triangleleft \langle M_E, PW_E, info_E, S_E, D_E, K_{H-E}, h(R, M_E), U \overset{SK}{\longleftrightarrow} E \rangle_{U \overset{K_E}{\Leftrightarrow} E}$. From Rule-1 and $(P10)$, it can deduce that $U| \equiv E| \sim \langle M_E, PW_E, info_E, S_E, D_E, K_{H-E}, h(R, M_E), U \overset{SK}{\longleftrightarrow} E \rangle$. From Rule-3, Rule-5, $(P11)$, $(P12)$ and $(P13)$; it is said that $U| \equiv E| \equiv U \overset{SK}{\longleftrightarrow} E$. Hence, *Goal 5* is achieved. From $(P14)$, *Goal 5* and Rule-2, it is concluded that $U| \equiv U \overset{SK}{\longleftrightarrow} E$. It means *Goal 6* is achieved. Similarly, *Goal 7* and *Goal 8* can be achieved from message S_3.
- (V_6) : from R_1: $U \triangleleft : \langle PW_U, M_r, \sigma_{H-U}, PK_H, K_{H-U}, B, H \overset{K_{ASME}}{\longleftrightarrow} U \rangle_{H \overset{K_{ASME}}{\longleftrightarrow} U}$ From Rule-1 and $(P15)$, it is said that $U| \equiv H| \sim \langle PW_U, M_r, \sigma_{H-U}, PK_H, K_{H-U}, H \overset{K_{ASME}}{\longleftrightarrow} U \rangle$.
- (V_7) : from R_2: $H \triangleleft \langle PK_H, y, U \overset{c}{\Leftrightarrow} H \rangle_{H \overset{K_{ASME}}{\longleftrightarrow} U}$; and From Rule-1 and $(P15)$, it can be deduce that $H| \equiv U| \sim \langle PK_H, y, U \overset{c}{\Leftrightarrow} H \rangle$. From Rule-3, Rule-5, $(P6)$ and $(P16)$; it is said that $H| \equiv U| \equiv U \overset{c}{\Leftrightarrow} H$. From $(P17)$ and Rule-2, it is concluded that $H| \equiv U \overset{c}{\Leftrightarrow} H$. It means *Goal 9* is achieved.

5.2 Formal Analysis Using AVISPA Tool

In this subsection, the proposed protocol is simulated using AVISPA tool to validate the data integrity, confidentiality, mutual authentication and key secrecy. The protocol is coded in High-Level Protocol Specification Language (HLPSL) to specify the characteristics. It simulates the protocol in various back-ends such as On-the-Fly Model Checker (OFMC), CL-based Attack Searcher (CL-ATSE) and SAT-based Model Checker (SAT-MC).

In the proposed handover protocol, EPS-AKA is applied in the initial authentication phase. As the EPS-AKA protocol simulated by AVISPA is secure [39]. Hence, we have not modeled the initial authentication process by AVISPA. In the handover authentication process, there are two participants named UE and enB which mutually authenticate to each other. We have simulated the handover process by HLPSL with their basic roles. In this paper, we present the basic roles of both the communication entities in Figs. 4 and 5. The security properties of the protocol are analyzed in the goal section as shown in Fig. 6.

The simulation is carried out using the OFMC backend of the AVISPA tool. The output of the OFMC model result is presented in Fig. 7. The SAFE keyword in the output shows the correctness of the protocol. In this model, an adversary obtains some information in between the sessions but, he/she can't launch any attacks. Hence, we conclude that the proposed handover protocol achieves the security properties and defeats all the identified attacks from the communication network.

```
   role ue (U, E:agent,
       SND, RCV: channel(dy), U_AUE, E_AENB: public_key,
       P, U_aue1, E_aenb1: text,  H1,H2,H3,H : hash_func)
played_by U  def=
local  State                                    : nat,
      K_h_e, K_h_u,M_ue,M_enb                   : text,
      X_ue,X_enb,X_hss,R,Sue,Due,Senb,Denb      : text,
      Pwue,Infoue,Pwenb,Infoenb                 : text,
      Eue0,Eenb0                                : hash((text.text).hash(text.text)),
      Eue1,Eenb1                                : hash((text).hash((text.text).(text.text))),
      Eue2,Eenb2                                : hash((text).hash((text.text).(text.text))),
      Kenb                                      : text.text.text
const
      sec_u_aue, sec_e_aenb,sec_kenb, ue_enb, enb_ue : protocol_id,
      add,minus   : hash_func, success          : text
init  State := 0
transition
1.  State = 0    /\ RCV(start) =|>
      State':= 1 /\ M_ue'       := new()
                 /\ Eue0'       := H3((K_h_u.P).H2(X_enb.P))
                 /\ Eue1'       := H2((Pwue).H1((X_ue.P).(K_h_u.P)))
                 /\ Eue2'       := H2((Pwue).H1((M_ue'.P).(X_enb.P)))
                 /\ Due'        := add ((Eue2'(M_ue')), (Eue2'(X_ue.(H1(Infoue.H2(M_ue'.P))))))
                 /\ Sue'        := minus (U_aue1, Eue0'(Due'))
                 /\ SND({M_ue'.P.Pwue.Infoue.K_h_u.P.Due'.Sue'}_(inv(U_AUE)))
                 /\ secret(M_ue',sec_u_aue,{U,E})
                 /\ witness(E, K_h_u, ue_enb,U_aue1)
 2. State   = 1  /\ RCV (({M_enb'.P.Pwenb.Infoenb.K_h_e.P.Denb'.Senb'}_(inv(E_AENB))). H(R.M_enb'.P))
                 /\ Kenb' = (M_ue'.R.P)=|>
   State' := 2
                 /\ Kenb' := (M_ue'.P.R)
                 /\ SND (H(H3(Kenb').H2(X_ue.P).H1(M_ue'.P)))
                 /\ secret(Kenb', sec_e_aenb,{U,E})
                 /\ secret(M_ue', sec_kenb,{U,E})
                 /\ witness(E, U, enb_ue, M_enb')
 3. State   = 2  /\ RCV(success) =|>
    State' := 3
end role
```

Fig. 4 The basic role of UE in handover authentication phase

6 Security Analysis

To present the correctness and secrecy of the proposed handover protocol, the security analysis is carried out in the form of privacy properties and security against various attacks.

- *Confidentiality* The original signer HSS delegates its signing authority to the proxy signers UE and eNB in the handover authentication process. No other device/entity can perform as the proxy signer. In the proposed protocol, HSS transfers the proxy keys to the UE and eNB through a secure channel. Hence, the signed signature is sent by one of the proxy signers and other one can be a legitimate verifier in the authentication process.
- *Unforgeability* The legitimate proxy private key and public key can be computed through respective σ_{HSS-UE} / $\sigma_{HSS-eNB}$ by designated UE/eNB only. The computation of σ_{HSS-UE} or $\sigma_{HSS-eNB}$ is based on ECDLP; hence an adversary $\mathcal{A}$ can't compute the valid proxy delegation.
- *Undeniability* During the handover process of the proposed protocol, the HSS can't refuse its signature transfer to the UE and eNB_2 when the S_{UE} and S_{eNB} are verified respectively.

Theorem 1 *Under the chosen message attack, the proposed protocol is secure if $\mathcal{A}$ can achieve only non-negligible advantage from encrypted messages. Then, the ECDLP is solvable in subgroups in polynomial time.*

Argument In the proposed protocol, suppose an adversary $\mathcal{A}$ computes the keys (K_{HSS-UE}, σ'_{HSS-UE}) by making several attempts on hash functions; where $h_{hss-UE} \neq h'_{hss-UE}$ and $\sigma'_{HSS-UE} \neq \sigma_{HSS-UE}$. It is considered that

$$Pr[\mathcal{A}(m_1) = 1] - Pr[\mathcal{A}(m_2) = 1] \leq \epsilon \tag{11}$$

```
role enb (E, U:agent,
      SND, RCV: channel(dy), U_AUE, E_AENB: public_key,
      P, U_aue1, E_aenb1: text,  H1,H2,H3,H : hash_func)
played_by U  def=
local   State                                  : nat,
      K_h_e, K_h_u,M_ue,M_enb                  : text,
      X_ue,X_enb,X_hss,R                       : text,
      Pwue,Infoue,Pwenb,Infoenb                : text,
      Sue,Due,Senb,Denb                        : text,
      Eue0,Eenb0                               : hash((text.text).hash(text.text)),
      Eue1,Eenb1                               : hash((text).hash((text.text).(text.text))),
      Eue2,Eenb2                               : hash((text).hash((text.text).(text.text))),
      Kenb                                     : text.text.text
const
      sec_u_aue, sec_e_aenb,sec_kenb, ue_enb, enb_ue : protocol_id,
      add,minus   : hash_func,
      success     : text
init  State := 0
transition
1.  State = 0 /\ RCV ({M_ue'.P.Pwue.Infoue.K_h_u.P.Due'.Sue'}_(inv(U_AUE)))
              /\ Due'          = add ((Eue2'(M_ue')), (Eue2'(X_ue.(H1(Infoue.H2(M_ue'.P))))))
              /\ Sue'          = minus (U_aue1, Eue0'(Due'))  =|>
  State':= 1  /\ M_enb'          := new()
              /\ Eenb0'          := H3((K_h_e.P).H2(X_ue.P))
              /\ Eenb1'          := H2((Pwenb).H1((X_enb.P).(K_h_u.P)))
              /\ Eenb2'          := H2((Pwenb).H1((M_enb'.P).(X_ue.P)))
              /\ Denb'           := add ((Eenb2'(M_enb')), (Eenb2'(X_enb.(H1(Infoenb.H2(M_enb'.P))))))
              /\ Senb'           := minus (E_aenb1, Eenb0'(Denb'))
              /\ Kenb'           := (R.M_ue'.P)
              /\ SND ({M_enb'.P.Pwenb.Infoenb.K_h_e.P.Denb'.Senb'}_(inv(E_AENB))). H(R.M_enb'.P))
              /\ secret(Kenb', sec_e_aenb,{E,U})
              /\ secret(M_enb', sec_kenb,{E,U})
              /\ witness(E, U, ue_enb, E_aenb1)
2. State  = 1 /\ RCV (H(H3(Kenb').H2(X_ue.P).H1(M_ue'.P))) =|>
  State' := 2 /\ SND(success)
              /\ request(E,U,enb_ue,M_ue')
end role
```

Fig. 5 The basic role of eNB in handover authentication phase

Fig. 6 Goals of the proposed protocol

```
goal

secrecy_of sec_u_aue, sec_e_aenb,sec_kenb
authentication_on ue_enb
authentication_on enb_ue

end goal
```

where m_1 and m_2 are the messages in the protocol [40]. Hence, we obtain from the Eq. (1)

$$\sigma'_{HSS-UE} = (e_1(\kappa_{HSS-UE} + x_{HSS}(h'_{HSS-UE}))) \tag{12}$$

From Eqs. (1), (11) and (12), the private key computed as:

$x_{HSS} = \frac{\sigma_{HSS-UE} - \sigma'_{HSS-UE}}{e_1(h_{HSS-UE} - h'_{HSS-UE})}$ Hence, the σ_{HSS-UE} is secure and proxy key can't be computed by an adversary. Further, UE and eNB_2 compute corresponding proxy private and public key.

Theorem 2 *If the computation of Diffie–Hellman problem (CDHP) is hard, $\mathcal{A}$ can compute the signed signature with only negligible advantage $\frac{1}{q-1}$.*

Argument Suppose, an adversary $\mathcal{A}$ attempt to compute the S_{UE} or S_{eNB} from M_{UE}, PK_{UE} or PK_{eNB}. But, the $\mathcal{A}$ can't compute these values because he/she will never generate the legitimate private keys as CDHP is hard. Hence, $\mathcal{A}$ can generate the legitimate S_{UE} or S_{eNB} with the negligible advantage $\frac{1}{q-1}$.

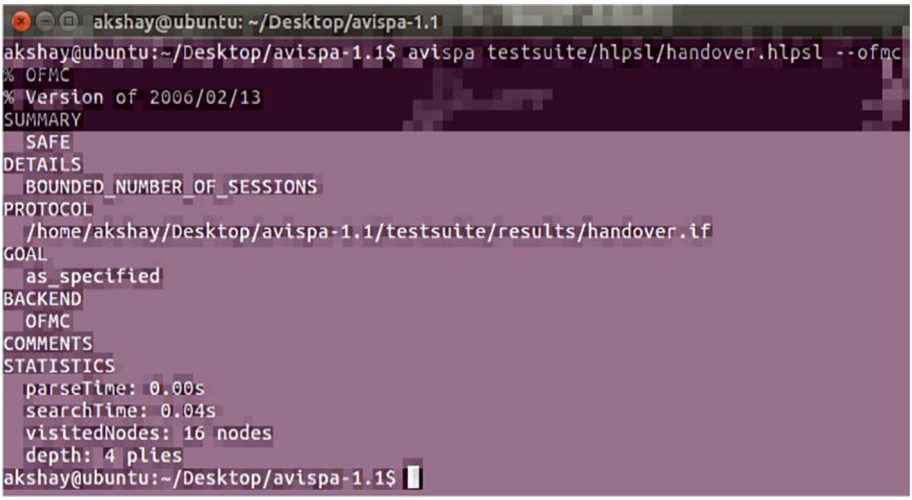

Fig. 7 Results summary of OFMC back-end

- *Identifiability* In the proposed protocol, the PK_{HSS} is used to validate the signature. Therefore, the UE and eNB_2 as a verifier have the knowledge of the legitimate signature of the signer after the authentication of signature. In addition, the HSS can identify UE and eNB_2 from the S_{UE} and S_{eNB}.
- *Mutual Authentication* In the proposed protocol, the security goals (*Goal 5* to *Goal 8*) are achieved in Sect. 5.1. From these security goals, it is proved that the protocol maintains the mutual authentication between UE and enB_2. These entities verify the session key at other side and authenticate to each other as follows:

$$SK_{enB} = r \cdot M_{UE} \Rightarrow r \cdot m_{UE} \cdot P \Rightarrow m_{UE} \cdot R$$
$$SK_{eNB} = m_{UE} \cdot R \Rightarrow m_{UE} \cdot P \cdot r \Rightarrow r \cdot M_{UE}$$

  Hence, only valid UE and eNB_2 can generate the legitimate session key.
- *Forward and Backward Untraceability* In the forward and backward untraceability, the secret key will not disclose the following and preceding session keys if it is compromised at any time. In the proposed handover scheme, the HSS transfers the long term secret keys (σ_{HSS-UE} and $\sigma_{HSS-eNB}$) to UE and eNB_2 respectively in a secure manner. Hence, $\mathcal{A}$ can't trace these keys. Suppose, $\mathcal{A}$ successfully generate the σ_{HSS-UE} or $\sigma_{HSS-eNB}$, then he/she can generate a_{UE} or a_{eNB}. Further, $\mathcal{A}$ attempts to deduce the D_{UE} to compute the proxy signed signature. But, it is merely impossible for $\mathcal{A}$ to generate D_{UE} because the m_{UE} and x_{UE} are selected randomly in each handover authentication process. To obtain the following and preceding session keys of SK_{eNB}, $\mathcal{A}$ needs the knowledge about random numbers such as m_{UE} and r. As the computation of ECDLP is hard; hence, an adversary will never compute these secret random numbers. Moreover, the proposed protocol does not adopt the key chain framework and association of eNB_1. Therefore, $\mathcal{A}$ will never know the successive session/secret keys.
- *Identity Privacy Preservation* The security goals (*Goal 1* and *Goal 2*) are proved in Sect. 5.1. Therefore, it can be deduced that the proposed protocol achieves the identity privacy preservation of UE and eNB_2. According to the ECDLP, $\mathcal{A}$ can't obtain the selected private keys x_{UE}, x_{MME}. Hence, the only legitimate UE can transfer the *IMSI* to

the HSS followed by MME. The transmitted message can be forged by $\mathcal{A}$ when the communication channel is not secure. Hence, the HSS transfers the delegation information and other relevant information to the UE by encrypting with K_{ASME}. Similarly, eNB_2 sends ID_{eNB} to the HSS and receives the proxy warrant through a secure channel encrypted with IPsec from the HSS.

- *Key Escrow Problem* The UE or eNB_2 generate the private keys by selected random numbers in the proposed handover authentication protocol. There is no involvement of the third party in generating the secret keys. Hence, the selected keys remain secret throughout the authentication process. Therefore, the protocol resists from the key escrow problem.
- *Revocation* Suppose, in the proposed protocol, $\mathcal{A}$ successfully generates the valid proxy delegation of UE or eNB_2 and attempts to establish the mutual authentication between them. But, *Goal 9* proves that the $c = h(K_{HSS-UE}||PK_{HSS}||B)$ is computed only by the UE and HSS. We also consider that the $\mathcal{A}$ will never obtain the secret/random number to generate the legitimate public keys followed by proxy signatures as ECDLP is hard to solve in polynomial time.
  Whenever UE is compromised, eNB_2 generates the revocation list of the compromised UEs and prevents the $\mathcal{A}$ from transferring a forged message in future. By these security assumptions, we consider that at most 1% UEs may be compromised and send a forged message during the handover authentication [41, 42]. For instance, there are 10,000 UEs are registered in the initial authentication phase and $10,000 \times 1\% = 100$ UEs are compromised (one at a time). Moreover, K_{HSS-UE} from the revocation list is eliminated once the proxy delegation is expired. Therefore, the size of the revocation list will be very limited and doesn't expand infinitely in eNB_2.

– *Attack analysis*
  The proposed handover protocol defeats the MiTM attack, replay attack, impersonation attack and redirection attack between the communication entities. The brief description of attack analysis is described as follows.

- *Man in-the Middle (MiTM) Attack* It is not possible for an adversary $\mathcal{A}$ to launch the MiTM attack during the authentication process of the proposed protocol. It is confirmed by the fact that SK_{eNB} is successfully authenticated with ECDLP parameters at UE and eNB_2. For instance, $\mathcal{A}$ tampers the M_{UE} and R. Then, it computes M_{UEadv} and R_{adv}, where M_{UEadv}=$m_{UEadv} \cdot P$ and $R_{adv} = r_{adv} \cdot P$. Hence, $\mathcal{A}$ successfully computes the M_{UEadv} at eNB_2 but, the SK_{eNBadv} is not computed correctly as SK_{eNBadv}= $r.M_{UEadv}$. Similarly, $\mathcal{A}$ computes the R_{adv} at UE but, the SK'_{eNBadv} is not computed correctly as $SK'_{eNBadv} = m_{UE} \cdot R_{adv}$. Moreover, eNB_2 will not accept M_{UEadv} as the signed signature is not authenticated correctly. Also, the $\mathcal{A}$ doesn't know the information of proxy private key of UE, so it is merely impossible for him/her to generate the legitimate proxy signed signature by M_{UEadv}. In addition, the UE will not acknowledge R_{adv} as UE computes $h(H_3(SK_{eNBadv}), H_2(PK_{UE}), H_1(M_{UEadv}))$ and sends it to the eNB_2. eNB_2 matches this received value with $h(H_3(SK_{eNB}), H_2(PK_{UE}), H_1(M_{UE}))$ and finds an unsuccessful match. Since, $\mathcal{A}$ can't compute the respective private keys and it is impossible for him/her to generate the valid handover agreement message. Therefore, the proposed protocol defeats the MiTM attack.

- *Replay Attack* During the authentication process of the proposed protocol, replay attack can't be executed as each handshake consists of selected private keys. Suppose, $\mathcal{A}$ sends the replayed message to UE or eNB_2. Then, the communication entities easily notice that the message is already received by them because the random numbers are distinct in each connection. Moreover, $\mathcal{A}$ can't generate the valid session key SK_{eNB}. Hence, the protocol is free from the replay attack.
- *Impersonation Attack* By achieving the *Goal 3* and *Goal 4*, the proposed protocol is free from the impersonation attack. Suppose, $\mathcal{A}$ impersonate the legitimate UE and eNB_2 by the malicious communication entities. The malicious UE may compute the MAC from valid UE and attempts to impersonate it in handover authentication process. Although, $\mathcal{A}$ will never compute the session key $SK_{eNB} = r \cdot M_{UE}$ by a malicious eNB_2 because the selected secret key r. Hence, the proposed protocol defeats the impersonation attack.
- *Redirection Attack* An adversary $\mathcal{A}$ can launch the redirection attack if he/she successfully impersonates the UE or generates the bogus eNB. The proposed handover protocol achieves the *Goal 1* and *Goal 2* as shown in Sect. 5.1. Hence, $\mathcal{A}$ can't obtain the actual identity and fails to impersonate the UE. Similarly, $\mathcal{A}$ can't obtain the identity of the legitimate eNB_2 as eNB_2 transmits the encrypted ID_{eNB} to the HSS. Moreover, the eNB_1 transmits the LAI to eNB_2 securely whenever UE moves into coverage area of eNB_2. Therefore, the redirection attack can't be carried out by $\mathcal{A}$ in the proposed protocol.

The comparative analysis of the existing and proposed handover protocols is shown in Table 2 on the basis of various security parameters. It can be observed that each handover protocol maintains the mutual authentication and key agreement between the communication entities during the authentication process. The proxy signature based Qiu's scheme [30], Cao's scheme_1 [29] and Cao's scheme_2 [28] achieve all the security features but, fails to preserve the privacy of UE or eNB and don't establish the revocation property. The chameleon hash function based Zhang's scheme_1 [25] doesn't preserve the privacy and vulnerable to redirection attack. Although, the Han' scheme [24] maintains all the security parameters but, defeats from key escrow problem due to untrusted third party and carries the high computational overhead due to time consuming bilinear pairing operations. Furthermore, Cao's scheme_3 [21] doesn't maintain the privacy preservation and vulnerable to the key escrow problem. Similar to the above protocols, Zhang's scheme_2 [22] can't avoid the key escrow problem and carries huge bandwidth consumption during the authentication process. In addition, the Choi's scheme [23] doesn't achieve the privacy preservation and key forward/ backward untraceability. Apart from this, the protocol can't avoid the MiTM and redirection attack. Further, the Kim's scheme [20] can't maintain the key secrecy and suffers from the key escrow problem.

Different from above existing protocols, the proposed proxy signature based handover authentication protocol performs the revocation property during the authentication process. The protocol achieves the key forward/ backward untraceability during the authentication. Also, the protocol preserves the privacy of communication entities and solves the problem of key escrow. In addition, the protocol resists from all the identified attacks. Hence, the proposed protocol is comparatively superior to existing protocols as it achieves all the essential security parameters in the handover authentication process.

Table 2 Comparative analysis of handover protocols on the basis of various security parameters

Security Parameters	Qiu's Scheme [30]	Zhang's Scheme_1 [25]	Cao's Scheme_1 [29]	Han's Scheme [24]	Cao's Scheme_2 [28]	Cao's Scheme_3 [21]	Zhang's Scheme_2 [22]	Choi's Scheme [23]	Kim's Scheme [20]	Proposed Scheme
SP_1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SP_2	✔	✔	✔	✔	✔	✔	✔	✗	✗	✔
SP_3	✗	✗	✗	✔	✗	✗	✔	✗	✔	✔
SP_4	✔	✔	✔	✗	✔	✗	✗	✔	✗	✔
SP_5	✗	–	✗	–	✗	–	–	–	–	✔
SP_6	✔	✔	✔	✔	✔	✔	✔	✗	✗	✔
SP_7	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SP_8	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SP_9	✗	✗	✗	✔	✗	✗	✔	✗	✔	✔

SP_1: mutual authentication in handover phase; SP_2: achieve forward and backward untraceability; SP_3: identity protection in authentication process; SP_4: resistance form key escrow problem due to untrusted private key generator (third party); SP_5: revocation of delegation power from proxy signers; SP_6: resistance from MiTM attack; SP_7: resistance from replay attack; SP_8: resistance from impersonation attack; SP_9: resistance from redirection attack

7 Performance Evaluation of the Proposed Protocol

In this section, the performance of the proposed protocol is evaluated by comparing with existing handover protocols in terms of transmission overhead, communication cost, storage overhead, message authentication overhead and computation cost. The comparative analysis shows that the proposed protocol achieves the desired goals and efficiency.

7.1 Transmission Overhead

To compute the transmission overhead of the existing and proposed handover protocols, it is assumed that the expected cost of message verification between (1) eNB and MME/AAA is α unit; (2) UE and eNB is β unit; (3) eNB and eNB is γ unit; (4) MME and MME is Δ unit. It is pointed out that the eNB lies very far from the MME/AAA server; hence the cost of β unit has the range as $0 < \beta < \alpha$. In addition, the cost of the α is higher than the cost of γ and Δ. Table 3 represents the transmission overhead of the proposed and existing handover protocols. We present the transmission overhead of those handover protocols only that exhibit most of the mobility scenarios as discussed in Sect. 4.2. From Table 3, it is observed that the transmission overhead of the proposed handover protocol is lower than other handover protocols. Although, Qiu's scheme shows less transmission overhead compare to the proposed protocol because it does not consider the S1-based intra-MME handover scenario.

Further, a comparative analysis is also presented in Table 4 that consists the communication cost of proposed and existing handover protocols. These protocols discuss the traditional handover scenario between UE/MN and eNB_2/AP_2. Similar to the existing handover protocols, the proposed protocol needs three messages handshake between the UE and eNB_2. Although, only two messages are sufficient to mutually authenticate UE and eNB_2 in the handover process of the proposed protocol. The third message is just transmitted to confirm the handover key agreement between UE and eNB_2. Further, we compare the existing protocols with our protocol in terms of various parameters.

To evaluate the performance of the proposed protocol in terms of storage overhead and message overhead, we set $|q| = 160$ and $|p| = 1024$ as ECC key exhibits similar security as

Table 3 Comparative analysis of handover protocols in terms of transmission overhead

	Qiu's Scheme [30]	Cao's Scheme_2 [28]	LTE Scheme [11]	Proposed Scheme
TO_{eNB_2-MME}[a]	4α	6α	12α	6α
TO_{UE-eNB_2}[b]	3β	3β	3β	3β
$TO_{eNB_2-eNB_2}$[c]	0	0	2γ	0
$TO_{MME-MME}$[d]	2Δ	2Δ	2Δ	2Δ
TO_{Total}[e]	$4\alpha + 3\beta + 2\Delta$	$6\alpha + 3\beta + 2\Delta$	$12\alpha + 3\beta + 2\gamma + 2\Delta$	$6\alpha + 3\beta + 2\Delta$

[a]Transmission overhead of messages between eNB_2 and MME

[b]Transmission overhead of messages between UE and eNB_2

[c]Transmission overhead of messages between eNB_2 and eNB_2

[d]Transmission overhead of messages between MME and MME

[e]Total transmission overhead

Table 4 Comparative analysis of handover protocols in terms of communication cost

	Zhang's Scheme_1 [25]	Cao's Scheme_1 [29]	Han's Scheme [24]	Cao's Scheme_3 [21]	Zhang's Scheme_2 [22]	Qi's Scheme [27]	Choi's Scheme [23]	Cai's Scheme [19]	Kim's Scheme [20]	Proposed Scheme
Communication cost	3β	3β	3β	3β	3β	5β	3β	4β	3β	3β

Table 5 Comparative analysis of handover protocols in terms of UE's storage overhead

	Qiu's Scheme [30]	Zhang's Scheme_1 [25]	Cao's Scheme_1 [29]	Han's Scheme [24]	Cao's Scheme_2 [28]	Cao's Scheme_3 [21]	Zhang's Scheme_2 [22]	Choi's Scheme [23]	Kim's Scheme [20]	Proposed Scheme
Storage overhead	$\|q\| + \|n\| + l_{hash}$	$2\|q\| + 3\|n\|$	$2\|q\| + 2\|p\| + 2l_{hash}$	$3\|q\| + \|n\|$	$\|q\| + \|p\| + l_{hash}$	$2\|q\| + \|n\| + l_{hash}$	$3\|q\| + 5\|n\|$	$3\|q\| + \|p\|$	$2\|q\| + 4\|n\|$	$\|q\| + \|n\| + l_{hash}$

1024-bit RSA key. The elliptic curve $E(F_n) : \#E(F_n) = 160$ bits prime q. Moreover, $|n| = |\#E(F_n)| = 160$.

7.2 Storage Overhead

In the proposed protocol, UE and eNB store the relevant information (proxy secret keys, HSS/AAA parameters and delegation) in the initial authentication phase. Both the entities have same storage overhead. Primarily, we compute the storage overhead at the UE of the proposed and existing handover protocols. The computed storage overhead of the protocols is shown in Table 5. From Table 5, it is analyzed that the protocols [20–22, 24, 25] execute additional point multiplication operations that increase the storage overload at UE. Moreover, the Cao' scheme_1, Cao' scheme_2 and Choi's scheme perform modular exponentiation operations that generate high storage overhead. Furthermore, the storage overhead at UE (60 bytes) in the proposed protocol is similar to the Qiu's scheme [30]. The graph is also plotted to compare the storage overhead of handover protocols as shown in Fig. 8. It can be considered that the storage overhead at UE in the proposed protocol is quite competitive compared to the existing protocols.

7.3 Message Overhead

During the handover process of the proposed protocol, UE communicates to the eNB_2 in 3-way message handshake to mutually authenticate each other and verify the handover agreement message. To compute the message overhead of the proposed and existing handover protocols, we consider that the identity is of 4 bytes, time-stamp is of 4 bytes and hash (SHA-1) is of 20 bytes. The message overhead of the handover protocols is analyzed in Table 6. In the Qiu's scheme and Zhang's scheme_1, UE and eNB_2 execute extra point multiplication operations that generate the high message overhead. The Cao's scheme_1, Cao's scheme_2 and Choi's scheme adopt the modular exponential operations during the handover process that increase the message overhead.

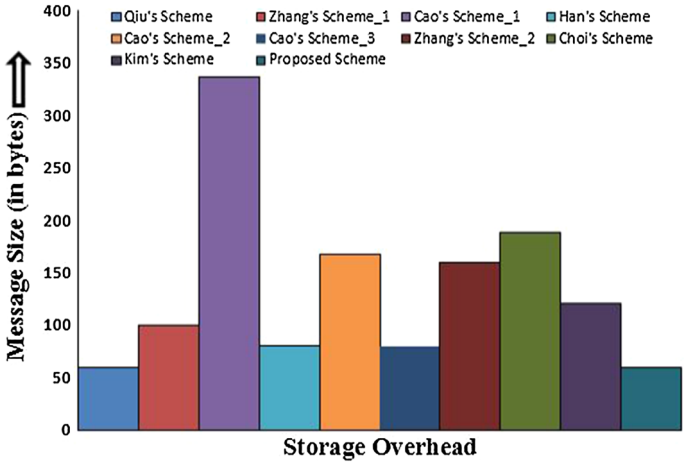

Fig. 8 Comparison of the UE's storage overhead

Table 6 Comparative analysis of handover protocols in terms of message overhead

	Message 1[a]	Message 2[b]	Message 3[c]	Total (in bytes)
Qiu's Scheme [30]	$\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	$2\|q\| + 3\|n\| + 2t_{time} + i_{id} + 2l_{hash}$	l_{hash}	$3\|q\| + 5\|n\| + 4t_{time} + 2i_{id} + 4l_{hash}$
Zhang's Scheme_1 [25]	$4\|q\| + 2\|n\| + 2t_{time} + i_{id}$	$4\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	l_{hash}	$8\|q\| + 4\|n\| + 4t_{time} + 2i_{id} + 2l_{hash}$
Cao's Scheme_1 [29]	$\|q\| + 2\|p\| + 2t_{time} + i_{id} + l_{hash}$	$\|q\| + 2\|p\| + 2t_{time} + i_{id} + 2l_{hash}$	$2l_{hash}$	$2\|q\| + 4\|p\| + 4t_{time} + 2i_{id} + 5l_{hash}$
Han's Scheme [24]	$4\|q\| + 2\|n\| + 2t_{time} + i_{id}$	$4\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	l_{hash}	$8\|q\| + 4\|n\| + 4t_{time} + 2i_{id} + 2l_{hash}$
Cao's Scheme_2 [28]	$\|q\| + 2\|p\| + 2t_{time} + i_{id} + l_{hash}$	$\|q\| + 2\|p\| + 2t_{time} + i_{id} + 2l_{hash}$	l_{hash}	$2\|q\| + 4\|p\| + 4t_{time} + 2i_{id} + 5l_{hash}$
Cao's Scheme_3 [21]	$2\|q\| + 2\|n\| + i_{id}$	$2\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	l_{hash}	$4\|q\| + 4\|n\| + 2t_{time} + 2i_{id} + 2l_{hash}$
Zhang's Scheme_2 [22]	$\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	$\|q\| + 2\|n\| + 2t_{time} + i_{id} + 2l_{hash}$	l_{hash}	$2\|q\| + 4\|n\| + 4t_{time} + 2i_{id} + 4l_{hash}$
Choi's Scheme [23]	$\|q\| + 2\|p\| + 2t_{time} + i_{id}$	$\|q\| + 2\|p\| + 2t_{time} + i_{id} + 2l_{hash}$	l_{hash}	$2\|q\| + 4\|p\| + 4t_{time} + 2i_{id} + 3l_{hash}$
Kim's Scheme [20]	$\|q\| + \|n\| + 2t_{time} + l_{hash}$	$\|q\| + \|n\|$	l_{hash}	$2\|q\| + 2\|n\| + 2t_{time} + 2l_{hash}$
Proposed Scheme	$\|q\| + 2\|n\| + 2t_{time} + i_{id} + l_{hash}$	$2\|q\| + 2\|n\| + 2t_{time} + i_{id} + 2l_{hash}$	l_{hash}	$3\|q\| + 4\|n\| + 4t_{time} + 2i_{id} + 4l_{hash}$

[a]Transmitted message (S_1) in handover authentication process

[b]Transmitted message (S_2) in handover authentication process

[c]Transmitted message (S_3) in handover authentication process

t_{time}: represents the current and expiry time (32 bits); i_{id}: represents the identity of the communication entity (32 bits); l_{hash}: represents the length of SHA-1 (160 bits)

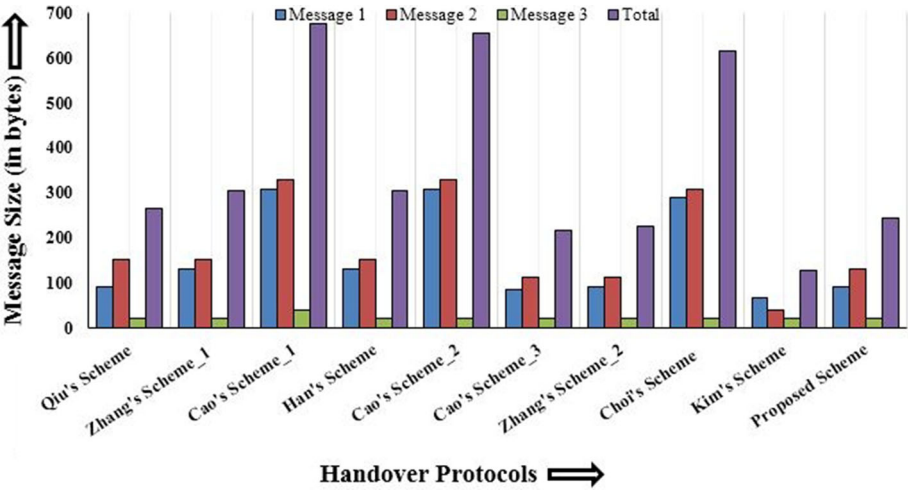

Fig. 9 Comparison of the message overhead

The graph is also plotted to compare the message overhead of the handover protocols as shown in Fig. 9. Although, the message overhead of the Kim's scheme, Zhang's scheme_2 and Cao's scheme_3 is very much competitive to the proposed handover protocol. But, these protocols suffer from the key escrow problem. Different from the existing schemes, the proposed scheme operates the point multiplication and hash functions efficiently in the handover process. Hence, the message overhead of the proposed protocol is comparatively superior to the existing protocols.

In addition, we compute the message overhead of the revocation verification and complete cost in revocation phase separately. Hence, the revocation verification cost is l_{hash} and total cost is $|q| + 2|n| + 2l_{hash}$.

7.4 Computation Overhead

The proposed handover protocol is compared with existing protocols to evaluate computation overhead. We set the elapsed time of the cryptographic operations in Table 7 [25]. The computational overhead of the existing and proposed protocols is analyzed in Table 8. In each handover protocol, the computation overhead of UE is similar to eNB_2. The Han's scheme, Zhang's scheme_2 and Kim's scheme execute the key operations in their protocol using time consuming bilinear operations which is very expensive in real time applications. In the Cao's scheme_1 and Cao's scheme_2, two extra modular exponentiation operations are used in the handover process that generate the high computational consumption. In the Choi's scheme, one additional RSA verification and two modular exponentiation operations are used that increase the computational overhead of the protocols.

The graph is also plotted to compare the computational consumption of the handover protocols as shown in Fig. 10. However, the computation overhead of the Qiu's scheme and Cao's scheme_3 is less than the proposed scheme. But, the Qiu's scheme doesn't establish the revocation property. The proposed protocol uses one extra additional point multiplication operation in the initial and handover authentication phases compared to Qiu's scheme. In addition, the Cao's scheme_3 suffers from the key escrow problem and the computation overhead of Zhang' scheme_1 is very competitive to the

Table 7 Elapsed time of various cryptographic operations

	T_{BP}[a]	T_{PM}[b]	T_{ME}[c]	T_{SM}[d]	T_{EV}[e]	T_{RV}[f]	T_{hash}[g]	T_{mul}[h]	T_{AO}[i]
UE	38.376	1.537	1.698	1.799	1.875	0.957	.0356	0.0132	0.0094
enB	16.322	0.475	0.525	0.556	0.581	0.301	0.0121	0.0042	0.0033

[a]Bilinear pairing operation

[b]Point multiplication operation

[c]Modular exponentiation operation

[d]Simultaneous point multiplication operation (T_{SM}=1.17 T_{PM})

[e]Verification of ECDSA ($T_{EV} = T_{SM} + 3T_{mul} + T_{hash}$)

[f]Verification of RSA

[g]SHA-1 hash function

[h]Multiplication operation

[i]Arithmetic operation

proposed protocol. Different from the existing protocols, the proposed protocol execute the cost effective point multiplication operations during the key operations and exhibits all the handover scenarios with revocation. Hence, the computational overhead of the proposed protocol is comparatively better than the existing protocols.

We observed that the computation complexity of the proposed protocol is less than 20 ms (the critical threshold for uninterrupted handover) that suits the standard handover scenario. Additionally, the computation overhead in revocation for the UE is $T_{PM} + 2T_{hash} + T_{mul} + 2T_{AO} = 1.640$ ms; and for the eNB is 0.509 ms.

8 Conclusion

In this paper, we proposed the proxy signature based efficient and robust handover authentication protocol with the revocation property in LTE/LTE-A network. In this protocol, a secure mutual authentication is achieved between the UE and eNB by obtaining the proxy delegation from HSS. In the meantime, a shared secret key is also maintained between communication entities. The protocol solves the problem of key escrow and achieves key forward/backward secrecy. Furthermore, the formal verification of the protocol is carried out by BAN logic and simulated using the AVISPA tool. In addition, the security analysis of the protocol is also presented with respect to various security parameters. The analysis proves the correctness of the protocol and security against various identified attacks. The performance analysis shows that the proposed protocol is more efficient than the existing handover protocols in terms of storage, transmission, communication and computation overhead. It is also expected that the proposed protocol will strengthen the security of LTE/LTE-A network in various handover scenarios. Further, the expansion of the proposed handover protocol could be useful in group based communication when the mass Machine Type Communication (MTC) devices are simultaneously authenticated by new eNBs.

Table 8 Comparative analysis of handover protocols in terms of computation overhead

	$CO_{UE-initial}$[a]	$CO_{eNB_2-initial}$[b]	CO_{UE}[c]	CO_{eNB_2}[d]	Total (in ms)
Qiu's Scheme [30]	$2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$3T_{PM} + 2T_{hash} + 3T_{mul} + T_{AO}$	$3T_{PM} + 2T_{hash} + 3T_{mul} + T_{AO}$	10.275
Zhang's Scheme_1 [25]	$2T_{PM} + 3T_{mul} + T_{AO}$	$2T_{PM} + 3T_{mul} + T_{AO}$	$T_{PM} + T_{SM} + T_{EV} + 3T_{hash} + 2T_{AO}$	$T_{PM} + T_{SM} + T_{EV} + 3T_{hash} + 2T_{AO}$	11.079
Cao's Scheme_1 [29]	$3T_{ME} + 2T_{hash} + T_{mul} + T_{AO}$	$3T_{ME} + 2T_{hash} + T_{mul} + T_{AO}$	$5T_{ME} + 3T_{hash} + 3T_{mul} + 2T_{AO}$	$5T_{ME} + 3T_{hash} + 3T_{mul} + 2T_{AO}$	18.128
Han's Scheme [24]	$T_{BP} + 2T_{PM} + 3T_{hash} + 2T_{mul}$	$T_{BP} + 2T_{PM} + 3T_{hash} + 2T_{mul}$	$T_{PM} + 2T_{SM} + T_{EV} + 3T_{hash} + T_{mul} + 2T_{AO}$	$T_{PM} + 2T_{SM} + T_{EV} + 3T_{hash} + T_{mul} + 2T_{AO}$	68.262
Cao's Scheme_2 [28]	$2T_{ME} + T_{hash} + T_{mul} + T_{AO}$	$2T_{ME} + T_{hash} + T_{mul} + T_{AO}$	$5T_{ME} + 2T_{hash} + 3T_{mul} + T_{AO}$	$5T_{ME} + 2T_{hash} + 3T_{mul} + T_{AO}$	15.773
Cao's Scheme_3 [21]	$2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$2T_{PM} + 3T_{hash} + 3T_{mul} + T_{AO}$	$2T_{PM} + 3T_{hash} + 3T_{mul} + T_{AO}$	8.340
Zhang's Scheme_2 [22]	$T_{BP} + 2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$T_{BP} + 2T_{PM} + T_{hash} + T_{mul} + T_{AO}$	$T_{BP} + 2T_{PM} + 4T_{hash} + 2T_{mul} + 2T_{AO}$	$T_{BP} + 2T_{PM} + 4T_{hash} + 2T_{mul} + 2T_{AO}$	117.771
Choi's Scheme [23]	$3T_{ME} + T_{RV} + T_{hash}$	$3T_{ME} + T_{RV} + T_{hash}$	$4T_{ME} + T_{RV} + 3T_{hash} + 4T_{mul} + 2T_{AO}$	$4T_{ME} + T_{RV} + 3T_{hash} + 4T_{mul} + 2T_{AO}$	18.360
Kim's Scheme [20]	T_{BP}	$2T_{BP}$	$2T_{BP} + T_{PM} + 2T_{hash}$	$2T_{BP} + T_{PM} + 2T_{hash}$	182.523
Proposed Scheme	$3T_{PM} + 2T_{hash} + 3T_{mul} + 2T_{AO}$	$3T_{PM} + 2T_{hash} + 3T_{mul} + 2T_{AO}$	$3T_{PM} + 4T_{hash} + 2T_{mul} + 2T_{AO}$	$3T_{PM} + 4T_{hash} + 2T_{mul} + 2T_{AO}$	12.494

[a]Computation cost of UE in initial authentication process

[b]Computation cost of eNB in initial authentication process

[c]Computation cost of UE in the handover authentication process

[d]Computation cost of eNB in the handover authentication process

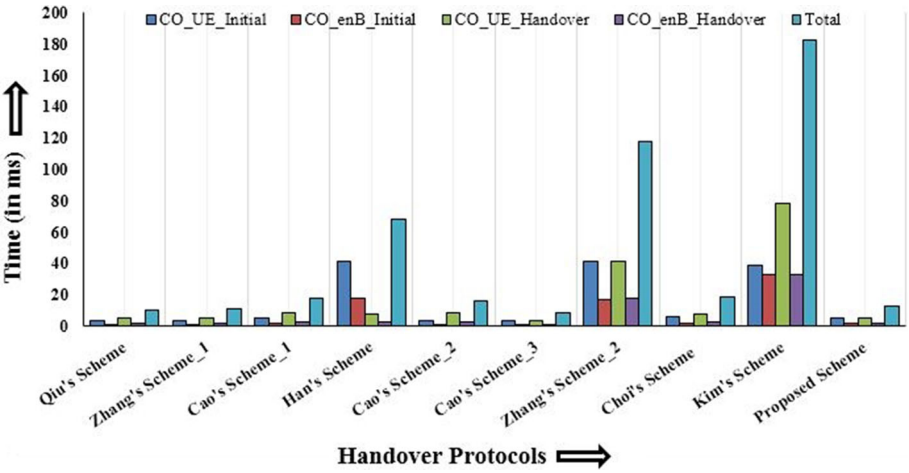

Fig. 10 Comparison of the computational consumption

References

1. Network EUTRA. (2011). 3rd generation partnership project. Technical specification group services and system aspects. *General packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRA) access*.
2. Li, G., Jiang, Q., Wei, F., & Ma, C. (2015). A new privacy-aware handover authentication scheme for wireless networks. *Wireless Personal Communications*, *80*(2), 581–589.
3. Astély, D., Dahlman, E., Furuskär, A., Jading, Y., Lindström, M., & Parkvall, S. (2009). LTE: The evolution of mobile broadband. *IEEE Communications Magazine*, *47*(4), 44–51.
4. Sankaran, C. (2009). Network access security in next-generation 3GPP systems: A tutorial. *IEEE Communications Magazine*, *47*(2), 84–91.
5. Oh, H., Yoo, K., Na, J., & Ck, Kim. (2010). A robust seamless handover scheme for the support of multimedia services in heterogeneous emerging wireless networks. *Wireless Personal Communications*, *52*(3), 593–613.
6. Xie, Y., Wu, L., Kumar, N., & Shen, J. (2017). Analysis and improvement of a privacy-aware handover authentication scheme for wireless network. *Wireless Personal Communications*, *93*(2), 523–541.
7. 3GPP. (Jun 2012). Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (EUTRAN), overall description. Sophia-Antipolis Cedex, France, 3GPP TS 36300 V1120.
8. 3GPP. (June 2012). 3rd generation partnership project; technical specification group services and system aspects; service requirements for the evolved packet system (EPS) (Rel 12). 3GPP TS 22278 V1210.
9. 3GPP. (Sepember 2012). 3rd generation partnership project; technical specification group core network and terminals; access to the 3GPP evolved packet core (EPC) via non-3GPP access networks (Rel 11). 3GPP TS 24302 V1140.
10. Lucent, A. (2009). The LTE network architecturea comprehensive tutorial. Strategic Whitepaper.
11. 3GPP. (September 2011). 3rd generation partnership project; technical specification group services and system aspects. *General packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access*. (Rel 10). 3GPP TS 23401 V1050.
12. 3GPP. (June 2011). 3rd generation partnership project; technical specification group radio access network. *Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRA). Overall description* (Rel 10). 3GPP TS 36300 V1040.
13. Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for lte and lTE—A networks. *IEEE Communications Surveys & Tutorials*, *16*(1), 283–302.
14. Forsberg, D. (2010). LTE key management analysis with session keys context. *Computer Communications*, *33*(16), 1907–1915.

15. 3GPP. (June 2011). 3rd generation partnership project; technical specification group service and system aspects. *3GPP system architecture evolution (SAE). Security architecture*. (Rel 11). 3GPP TS 33401 V1101.
16. Bohák, A., Buttyán, L., & Dóra, L. (2007). An authentication scheme for fast handover between wifi access points. In *Proceedings of ACM wireless internet conference (WICON)*.
17. Hong, K., Jung, S., & Wu, S. F. (2005). A hash-chain based authentication scheme for fast handover in wireless network. In *International workshop on information security applications* (pp. 96–107). Springer.
18. Zhang, C., Lu, R., Ho, P. H., & Chen, A. (2008). A location privacy preserving authentication scheme in vehicular networks. In *Wireless communications and networking conference, 2008. WCNC 2008, IEEE* (pp. 2543–2548). IEEE.
19. Cai, L., Machiraju, S., & Chen, H. (2010). Capauth: a capability-based handover scheme. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1–5). IEEE.
20. Kim, Y., Ren, W., Jo, J. Y., Jiang, Y., & Zheng, J. (2007). SFRIC: A secure fast roaming scheme in wireless LAN using ID-based cryptography. In: *IEEE international conference on communications, 2007. ICC'07* (pp. 1570–1575). IEEE.
21. Cao, J., Ma, M., & Li, H. (2012). An uniform handover authentication between E-UTRAN and non-3GPP access networks. *IEEE Transactions on Wireless Communications*, *11*(10), 3644–3650.
22. Zhang, Y., Chen, X., Li, H., & Cao, J. (2012). Identity-based construction for secure and efficient handoff authentication schemes in wireless networks. *Security and Communication Networks*, *5*(10), 1121–1130.
23. Choi, J., & Jung, S. (2010). A handover authentication using credentials based on chameleon hashing. *IEEE Communications Letters*, *14*(1), 54–56.
24. Han, Q., Zhang, Y., Chen, X., Li, H., & Quan, J. (2014). Efficient and robust identity-based handoff authentication for EAP-based wireless networks. *Concurrency and Computation: Practice and Experience*, *26*(8), 1561–1573.
25. Zhang, Y., Chen, X., Li, J., & Li, H. (2014). Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. *Computer Networks*, *75*, 192–211.
26. Hs, R. O. H., & Sh, J. U. N. G. (2010). RSA-based proxy signature for media independent handover. *Journal of Measurement Science and Instrumentation*, *26*(4), 122–127.
27. Jing, Q., Zhang, Y., Fu, A., & Liu, X. (2011). A privacy preserving handover authentication scheme for EAP-based wireless networks. In *Global telecommunications conference (GLOBECOM 2011), 2011 IEEE* (pp. 1–6). IEEE.
28. Cao, J., Li, H., Ma, M., Zhang, Y., & Lai, C. (2012). A simple and robust handover authentication between HeNB and eNB in LTE networks. *Computer Networks*, *56*(8), 2119–2131.
29. Jin, C., & Hui, L. (2013). Handover authentication between different types of eNBs in LTE networks. *The Journal of China Universities of Posts and Telecommunications*, *20*(2), 106–112.
30. Qiu, Y., Ma, M., & Wang, X. (2017). A proxy signature-based handover authentication scheme for LTE wireless networks. *Journal of Network and Computer Applications*, *83*, 63–71.
31. Mambo, M., Usuda, K., & Okamoto, E. (1996). Proxy signatures: Delegation of the power to sign messages. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *79*(9), 1338–1354.
32. Lu, R., & Cao, Z. (2005). Designated verifier proxy signature scheme with message recovery. *Applied Mathematics and Computation*, *169*(2), 1237–1246.
33. Sun, H. M. (2000). Design of time-stamped proxy signatures with traceable receivers. *IEE Proceedings-Computers and Digital Techniques*, *147*(6), 462–466.
34. Das, M. L., Saxena, A., & Gulati, V. P. (2004). An efficient proxy signature scheme with revocation. *Informatica*, *15*(4), 455–464.
35. Ma, C., Xue, K., & Hong, P. (2013). A proxy signature based re-authentication scheme for secure fast handoff in wireless mesh networks. *IJ Network Security*, *15*(2), 122–132.
36. Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417–426). Springer.
37. Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, The Royal Society*, *426*, 233–271.
38. Avispa (2005) Automated validation of internet security protocols. http://www.avispa-project.org. Accessed 29 July 2018.
39. AVISPA. (2004). EAP: Extensible authentication protocol. http://www.avispa-project.org/library/EAP_AKA.html. Online; Accessed April 19, 2017.

40. Saxena, N., Grijalva, S., & Chaudhari, N. S. (2016). Authentication protocol for an IoT-enabled LTE network. *ACM Transactions on Internet Technology (TOIT)*, *16*(4), 25.
41. Huang, J. L., Yeh, L. Y., & Chien, H. Y. (2011). ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *60*(1), 248–262.
42. Lai, C., Lu, R., Zheng, D., Li, H., & Shen, X. S. (2016). GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Computer Networks*, *99*, 66–81.

Shubham Gupta received his B.Tech. in information technology and M.Tech in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, and University College of Engineering, RTU, Kota, India respectively. Currently, he is pursuing his Ph.D. in Computer Science and Engineering from Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India. His research interest includes security in cellular networks, machine type communication, wireless communication networks and mobile computing.

Balu L. Parne has done his under graduation from Shri Sant Gajanan Maharaj College of Engineering (SSGMCE), Shegaon that is affiliated to Sant Gadge Baba Amravati University (SGBAU), Amravati, Maharashtra, India and post-graduation from National Institute of Technology (NIT), Rourkela, Orissa, India. He is currently a Ph.D. student in the Department of Computer Science and Engineering at Visvesvaraya National Institute of Technology (VNIT), Nagpur-440010, Maharashtra, India. His current area of research is Wireless Communication, Network security, Internet of Things, Mobile computing and its applications.

Narendra S. Chaudhari completed his undergraduate, postgraduate and doctoral studies at Indian Institute of Technology (IIT), Mumbai, Maharashtra, India, in 1981, 1983, and 1988 respectively. He has successfully completed 08 R&D Projects funded by DST, UGC, AICTE, MHRD, etc. He has done significant research work on game AI, novel neural network models like binary neural nets and bidirectional nets, graph isomorphism problem, security of the wireless mobile communication, mobile computing and Internet of Things. He has been referee and reviewer for a number of premier conferences and Journals including IEEE Transaction, Neurocomputing, etc. He is fellow and recipient of Eminent Engineer award (Computer Engineering) of the Institution of Engineers, India (IE-India), Bharat Vidya Shiromani Award (with gold medal), as well as fellow of the Institution of Electronics and Telecommunication Engineers (IETE) (India), senior member of Computer Society of India, senior member of IEEE, USA, member of Indian Mathematical Society (IMS), Cryptology Research Society of India (CRSI) and many other professional societies.